periodica polytechnica

Transportation Engineering
36/1-2 (2008) 51–56
doi: 10.3311/pp.tr.2008-1-2.10
web: http://www.pp.bme.hu/tr
© *Periodica Polytechnica 2008*

RESEARCH ARTICLE

On qualitative and operational reliability of electronic brake systems for heavy duty vehicles

Timea Fülep / *László* Palkovics / *László* Nádai

Received 2007-03-03

Abstract

The development of the safety critical systems of future commercial vehicles is mainly driven by the social demand, that the societies want to see safer, more reliable vehicles on the roads, which can also handle more complex situations than human driver can. It is questioned whether the approaches of the classical reliability theory are appropriate for redundant electronic systems, especially if they have a safety-critical nature, such as the electronic brake system, which has been used in commercial vehicles in Europe for almost a decade.

Keywords

electronic brake system · redundancy level · reliability analysis

Acknowledgement

This research has been partially sponsored by the Pázmány Péter Program of the National Office for Research and Technology through the Advanced Vehicles and Vehicle Control Knowledge Center.

Timea Fülep
Department of Automobiles, BME, 6 Stoczek St, 1111 Budapest, Hungary
e-mail: fulep.timea@auto.bme.hu

László Palkovics
László Nádai
Department of Automobiles, BME, 6 Stoczek St, 1111 Budapest, Hungary

1 Introduction

Reliability theory has become one of the important areas in Systems Engineering. Any system analysis, in order to be complete, must give due consideration to system reliability and availability. A system designer is often faced by 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 [1, 2].

Reliability is mainly determined according 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 of vehicle designers and automotive industry in general [3].

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. By the integration of modern electronic technologies and a well-implemented chassis control (Referring to Péter [4, 5]) into an intelligent system, a fully electronically controlled power train, the overall traffic safety and traffic efficiency for heavy goods vehicles can be improved [6]. The by-wire technologies offer functional as well as design benefits, but their application in safety-critical systems, such as brake and steering requires special care during the design and release process.

2 Brake System Architectures of HGV Today

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 (see below), but in the full pneumatic back-up mode several functions

are not available. Such a system is called 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 (part of TCM - Trailer Control Module) or from the rear axle can be cancelled or from both. The table below, Fig. 1 shows most of the possible layouts for 1E+2P (but no back-up on the rear axle or in the trailer control valve) with two-circuit pneumatic foot brake valve (part of FBM - Foot Brake Module), and also the 1E+1P layouts, where the foot brake valve has only a single circuit.

The 2 1E+1P layouts fulfil the legislative requirements keeping the fail-safe nature of the basic brake system of the vehicle (this means that the system will provide the in 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 is neither fail-tolerant nor fail-safe. In order to handle the problem of the automatic drive (or so called platooning) problem, a fully fail-tolerant, redundant brake system has been developed in the framework of the EU supported Chauffeur-2 project. Although the system is fully fail-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 deducted from that.

Although the 2E brake system architecture of PEIT (EU project, 5th Frame Program) is not fully fail-tolerant (at least in the classical sense – all functions are provided without any performance reduction in case of a single failure), but this architecture provides several features, which result in enhanced system performance even if – as a consequence of a single failure – one of the circuits is not intact, and as such, provides enhanced safety in comparison to the 2P, 1E+2P and 1E+1P systems [6].

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 extra functions, since the typical brake functions (load sensing, coupling force control, ABS, ESP, slip control, but the basic brake function remains) are realized only electronically. The 2E architecture – where all functions are being computed in both ECUs – 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 the rear axle control circuit failure the front axle brake control can realize functions, which are in pneumatic mode not available, such as tilt, 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 – Coupling Force Control, 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.

3 Structural Reliability Analysis of Brake Systems

Several evidences show that the occurrence probability of single and multiple vehicle accidents has improved with the introduction of active safety functions such as antilock braking, traction control and electronic stability programs. These encouraging results have created expectations that in the future new active safety functions will result in further safety improvements in vehicle technology. At the same time, though, there is a growing recognition that any new technologies are likely to introduce new risks which therefore need to be identified, analysed and effectively contained.

Active safety systems address known safety problems but also introduce new classes of potentially hazardous failure modes. In a traditional design, 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 electronic control of wheel brakes. Active safety functions that control such brakes are of course carefully designed to fail-silent in case of detected malfunctions. 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.

Understandably, such radical design changes raise serious safety concerns and demand the thorough safety evaluation of any new design concepts. Potential failure modes must be identified and the effects of them in the provision of sensitive active safety functions must be established [7].

3.1 Reliability Design

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 [1].

Reliability design in the concept design phase is primarily oriented towards defining of reliability specification and selecting of the most acceptable solution from the point of view of

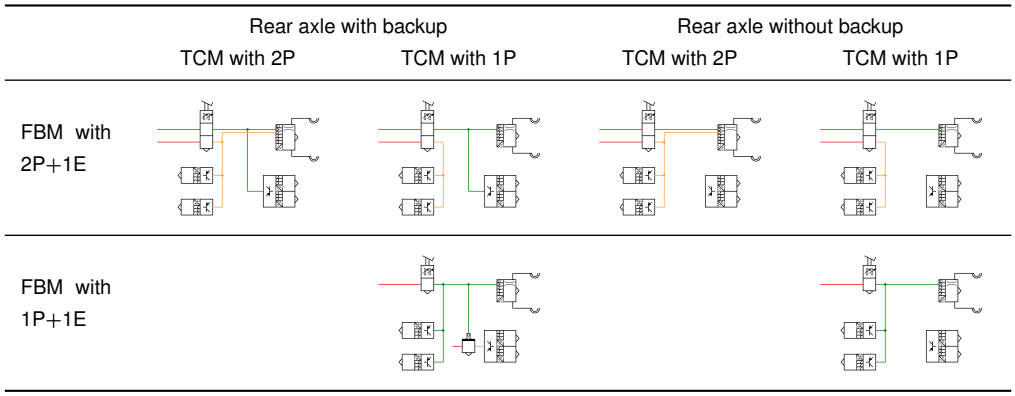

Fig. 1. Possible layouts for brake systems in terms of their back-up

reliability meeting requirements, what means that reliability of systems and their elements is analysed. 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 the pre-design. The concept design phase also defines the design goals from the point of view of meeting the standards and regulations.

Conducting the analysis of failure mode, effects (FMEA) enables identifying all potential and known modes of failure occurrences in system assemblies/parts, their causes, evaluation of consequences. Individual system elements (subsystem, assembly, part) 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 FMEA method. For each failure mode, the possible effect (consequence) is analysed at a higher level, i.e. at the whole system level [1].

3.2 Well-structured Qualitative Reliability Methodology – (MX) FMEA

Before starting the FMEA, it is worth deploying the customer requirements to design specification level. For that purpose, several tools are available, one of them is the Matrix Analyses from Plato, 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.

At the system level, only customer needs or regulatory requirements and the functions by which they are met are mapped to subsystems (Table reftab:1). No components are mapped or analysed at the system level.

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

- What is the system or product to be analysed?
- 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)?

Tab. 1. Top-level representation of the requirements for a redundant electronic semi-trailer brake system (extract)

SPARC semi-trailer system	Legal	Customer	Internal
	Requirements		
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			×

Using this approach, primary functions that are developed using software are mapped to subsystems of a redundant electronic brake system and then linked and marked to their influences on the requirements for the overall system in the matrix (Table 2) which shows a certain subsystem classification concerning an EU-project[1]. These links indicate direct relationships (via 'function') and indirect relationships (via 'failure' only).

The requirements, that the relevant components must meet in order to fulfil a function, are mapped at interfaces (Fig. 2). 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 [8].

There are many benefits of performing FMEA, including a systematic approach to classify hardware failures,it reduces development time and cost,it reduces engineering changes, it is easy to understand, serves as a useful tool for more efficient

[1]SPARC – Secure Propulsion using Advanced Redundant Control (6th Frame Program)

Tab. 2. System and function matrix (extract)

Semi-trailer	CTC[1]	AM1[2]	AM2	AM3	ASU[3]	NRG[4]	TAUX[5]
ABS status info	×	×	×	×			×
RSP status info	×	×	×	×			×
Yellow warning signal required	×	×	×	×	×	×	
Red warning signal required	×	×	×	×	×	×	
Automatic landing leg control	×				×	×	×
Keep level of chassis height	×	×			×	×	
Assure manual handling (LL)	×					×	×
Compressor control	×				×	×	

[1] Central Trailer Controller; [2] Axle Module; [3] Air Supply Unit; [4] Energy Unit; [5] Trailer Auxiliary Unit

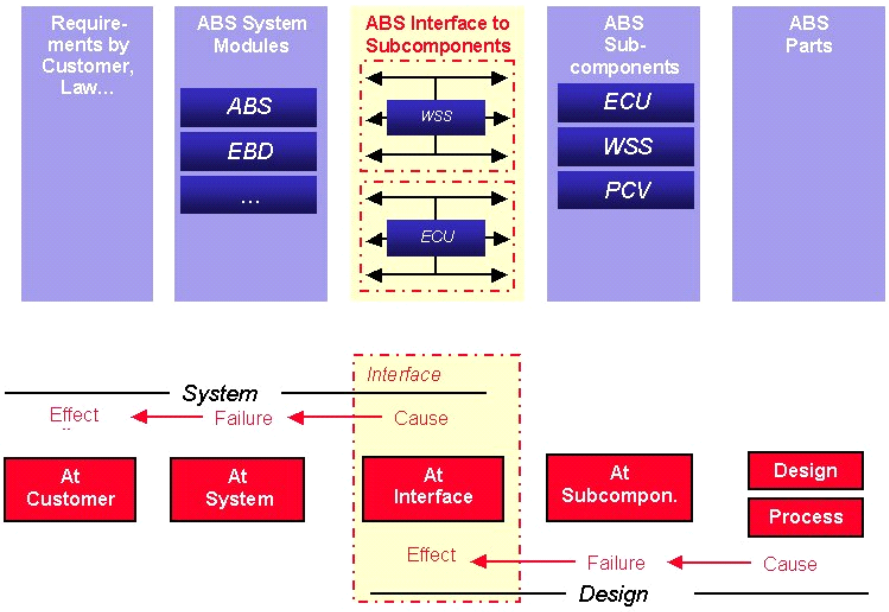

Fig. 2. Representation of the levels involved in System and Design FMEAs with defined interface [8]

test planning, highlights safety concerns to be focused on, improves customer satisfaction. It is an effective tool to analyse small, large, and complex systems, is 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, and useful to improve communication among design interface personnel [9].

3.3 Quantitative Analysis of Structural Reliability

If *availability* is thought of in terms of a repairable system being 'up' and 'down' then a number of concepts and terms can be defined using the mathematical apparatus of probability theory and reliability theory [10]. From this point of view the reliability of a system is usually understood as the *probability of fail-safe operation during a defined period of time*. The reliability of HGV brake systems can be examined using the models describing systems that are composed of items requiring non-negligible repair times.

In the following we assume (referring to Prezenszki and Várlaki [11]) that the operation times are independent random variables, and that the operation times are having the same probability distribution. Similarly, the repair times are considered independent random variables with the same distribution during a given period of operation. Namely, we are given the distribution function of operation times $F(t)$ with mean value T_1 and variance σ_1^2, and also the distribution function of repair times $G(t)$ with mean value T_2 and variance σ_2^2.

The measure of reliability of an item requiring non-negligible repair times is the so-called *availability coefficient* $A(t)$ that is the probability of actual working of the given element at moment t. It can be calculated using the following stationary expression (if a "sufficiently long period" is passed):

$$A_e = \lim_{t\to\infty} A(t) = \frac{T_1}{T_1 + T_2}, \tag{1}$$

where

- T_1 is the so-called Mean Time Between Failures (MTBF), that is, the average 'up' time,
- T_2 is the so-called Mean Time To Repair (MTTR), that is, the average time to restore to the 'up' state.

In non-stationary case the availability coefficient is the following:

$$A(t) = 1 - F(t) + \int_0^t [1 - F(t-x)]\, h(x)dx, \tag{2}$$

where $h(x)$ is the density function of resurrection [11].

$$h(x) = \sum_{n=1}^{\infty} \Phi_n(x),$$
$$\Phi_n(t) = \int_0^t F_n(t-x) dG_n(x),$$

$$F_n(t) = \int_0^t F_{n-1}(t-x) dF(x),$$
$$G_n(t) = \int_0^t G_{n-1}(t-x) dG(x),$$

where n is the number of failures until time t.

It is a common assumption in the reliability analysis of vehicle mechanical parts that operation and maintenance intervals follow exponential rules

- operation time: $F(t) = 1 - e^{-\lambda t}$, and
- maintenance (or repair) time: $G(t) = 1 - e^{-\mu t}$.

Now, in stationary case the availability coefficient is

$$A_e = \frac{\mu}{\lambda + \mu}, \tag{3}$$

and in non-stationary case

$$A(t) = \frac{\mu + \lambda e^{-(\lambda+\mu)t}}{\mu + \lambda}. \tag{4}$$

In the above expressions

- $1/\lambda = T_1$ is the mean time of normal operation (MTBF),
- $1/\mu = T_2$ is the mean time to repair (MTTR).

It is much more important to determine the probability $R(\tau)$ of operation during an interval τ (that is the so-called *reliability coefficient*). In non-stationary case

$$R_t(\tau) = 1 - F(t+\tau) + \int_0^t [1 - F(t+\tau-x)]\, h(x) dx, \tag{5}$$

and in stationary case

$$R_e(\tau) = \lim_{t\to\infty} R_t(\tau) = \frac{1}{T_1 + T_2} \int_\tau^\infty [1 - F(x)]\, dx. \tag{6}$$

In stationary case, using the exponential hypothesis for operation and maintenance times:

$$R_e(\tau) = \frac{\mu}{\mu + \lambda} e^{-\lambda\tau}. \tag{7}$$

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 as [11]

$$A_{\text{serial}} = \frac{1}{1 + \sum_{k=1}^{n} \frac{T_{k2}}{T_{k1}}}, \tag{8}$$

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 as

$$R_{\text{serial}}(\tau) = A_{\text{serial}}\, e^{-\tau/T_1}, \tag{9}$$

where

$$T_1 = \frac{1}{\sum_{k=1}^{n} \frac{1}{T_{k1}}}.$$

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

Parallel coupling between parts. In this case the failures of individual elements do not affect the reliability of the others: the failures of elements are independent, moreover, they can be repaired independently of each other.

Now, in stationary case the availability of the whole system (that is the probability that every individual element is operating at time t) is [11]:

$$A_{\text{parallel}} = \frac{T_{11}}{T_{11} + T_{12}} \cdot \frac{T_{21}}{T_{21} + T_{22}} \cdots \frac{T_{n1}}{T_{n1} + T_{n2}} = \prod_{i=1}^{n} \frac{T_{i1}}{T_{i1} + T_{i2}} \tag{10}$$

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 of k parts among the total number of n at a given time t:

$$A_k = \binom{n}{k} A_e^k (1 - A_e)^{n-k}, \tag{11}$$

where

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

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

$$R_k(\tau) = \binom{n}{k} R_e(\tau)^k \left(1 - R_e(\tau)\right)^{n-k}. \tag{12}$$

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 fail-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.

4 Conclusion

Nowadays during analysing more and more mainly electronically complex automotive systems, the question of the most suitable reliability analysis method has arisen. In this paper two accepted techniques were presented giving hints to a well-structured system analysis. Depending on the aim of the analysis the right reliability analysis tool has to be chosen or in case of complex analysis, more tools should be used at one time supporting each other.

References

1 **Srinivasan SK, Subramanian R**, *Probabilistic Analysis of Redundant Systems*, Springer-Verlag, Berlin, 1980.

2 **Ebeling CE**, *An Introduction to Reliability and Maintainability Engineering*, Mcgraw-Hill Companies, Inc., 1997.

3 **Popović P, Ivanović G**, *Design for reliability of vehicles in the concept phase*, EAEC Congress, 2005.

4 **Péter T**, *Gépjármű lengőrendszerek felfüggesztésparamétereinek optimálása*, MTA, Budapest, 1997. Kandidátusi értekezés.

5 _____, *Mathematical Transformations of Road Profile Excitation for Variable Vehicle Speeds*, Studies in Vehicle Engineering and Transportation Science, 2000, pp. 51–69.

6 **Armbruster M, Bäuerle K, Reichel R, Maisch A, Spiegelberg G**, *X-By-Wire systems of the next generation*, AVEC International Symposium, 2004.

7 **Papadopoulos Y, Grante C, Wedlin J**, *Automating aspects of safety design in contemporary automotive system engineering*, FISITA Conference, 2004.

8 **Dobry A**, *Think globally, act locally*, FMEA: Effective handling of complex systems.

9 **Dhillon BS**, *Design reliability: Fundamentals and Applications*, CRC Press LLC., 1999.

10 **Robinson RM, Anderson KJ**, *SIL Rating Fire Protection Equipment*: *Conferences in Research and Practice in Information Technology*, 8th Australian Workshop on Safety Critical Systems and Software (SCS'03).

11 **Prezenszki J, Várlaki P**, *A raktári anyagmozgatási géprendszerek megbízhatósági és kapacitásvizsgálata*, GÉP **XXX** (March 1978), no. 3, 85-92.