periodica polytechnica

Transportation Engineering
36/1-2 (2008) 57–60
doi: 10.3311/pp.tr.2008-1-2.11
web: http://www.pp.bme.hu/tr
© *Periodica Polytechnica 2008*

RESEARCH ARTICLE

On functional and quantitative reliability of electronic brake systems for heavy duty vehicles

Tímea Fülep / *László* Palkovics

Received 2007-03-03

Abstract

Redundant electronic systems confront us with new challenges in reliability analysis since handling and defining their back-up strategies is not a straightforward task by means of using qualitative approaches. This paper presents a technique through reliability theory, which enables the designer organizing functions and logical relationship between failures from the system level up to the last component.

Keywords

risk assessment · electronic brake system · quantitative 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.

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

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

1 Introduction

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 [1].

2 Functional Reliability Analysis of Brake Systems

2.1 Qualitative Safety Requirements according to Related Standards

The Functional Safety standard IEC 61508 sets out requirements for electrical/electronic and programmable electronic (E/E/PES) systems. A system is said to be safety-related if any failure to function can present a prospect of harm to people.

SILs (Safety Integrity Levels) are used by IEC 61508 to characterize the required functional safety of computer control systems. SIL is a measure of the probability that the safety-related system may fail in a dangerous manner. The value of SIL ranges from 1 (the lowest) to 4 (the highest). For example, SIL 4, the highest rating is for fly-by-wire aircraft and weapons systems and track circuited train signalling systems while SIL 2 is typical of certain Programmable Logic Controllers (PLC). SILs are shown in Table 1, from IEC 61508:

The safety functions necessary to ensure the required functional safety for each determined hazard shall be specified. This shall constitute the specification for the overall safety functions requirements. The necessary risk reduction shall be determined for each determined hazardous event. The necessary risk reduction may be determined in a quantitative and/or qualitative manner. For situations when an application sector international standard exists which includes appropriate methods for directly determining the necessary risk reduction, then such standards may be used to meet the requirement of this sub clause. The safety integrity requirements, in terms of the necessary risk reduction, shall be specified for each safety function.

In determining a SIL, parts 1 and 5 of IEC 61508 take a hazard and risk based approach with progressive refinement [2].

Tab. 1. SIL levels [2]

Safety integrity level (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	$\leq 10^{-5}$ to $< 10^{-4}$	$\leq 10^{-9}$ to $< 10^{-8}$
3	$\leq 10^{-4}$ to $< 10^{-3}$	$\leq 10^{-8}$ to $< 10^{-7}$
2	$\leq 10^{-3}$ to $< 10^{-2}$	$\leq 10^{-7}$ to $< 10^{-6}$
1	$\leq 10^{-2}$ to $< 10^{-1}$	$\leq 10^{-6}$ to $< 10^{-5}$

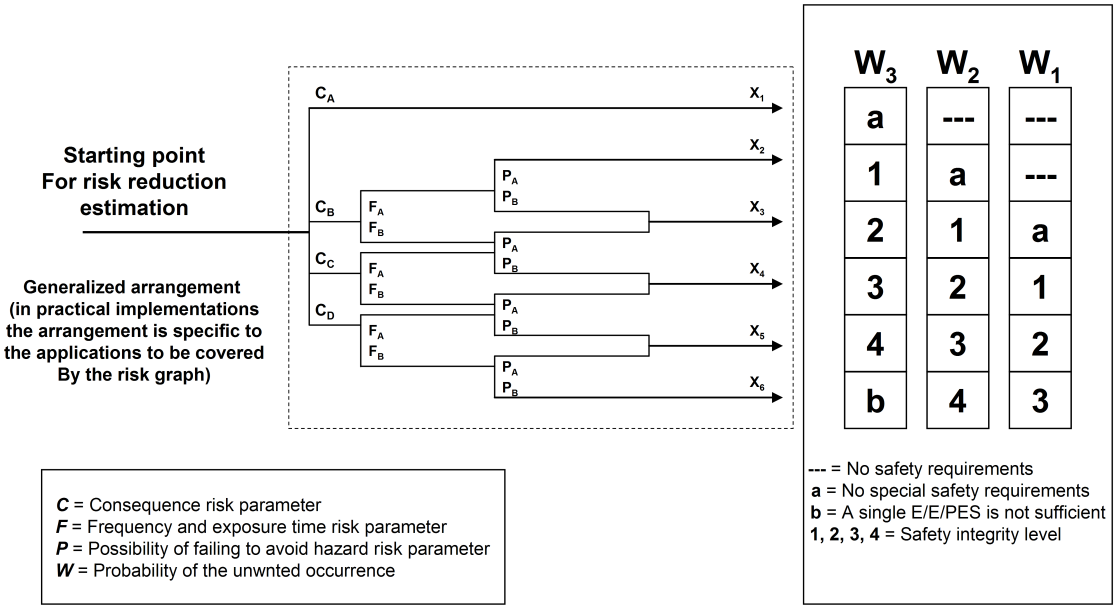

Fig. 1. Established Risk Graph (IEC 1 666/98)

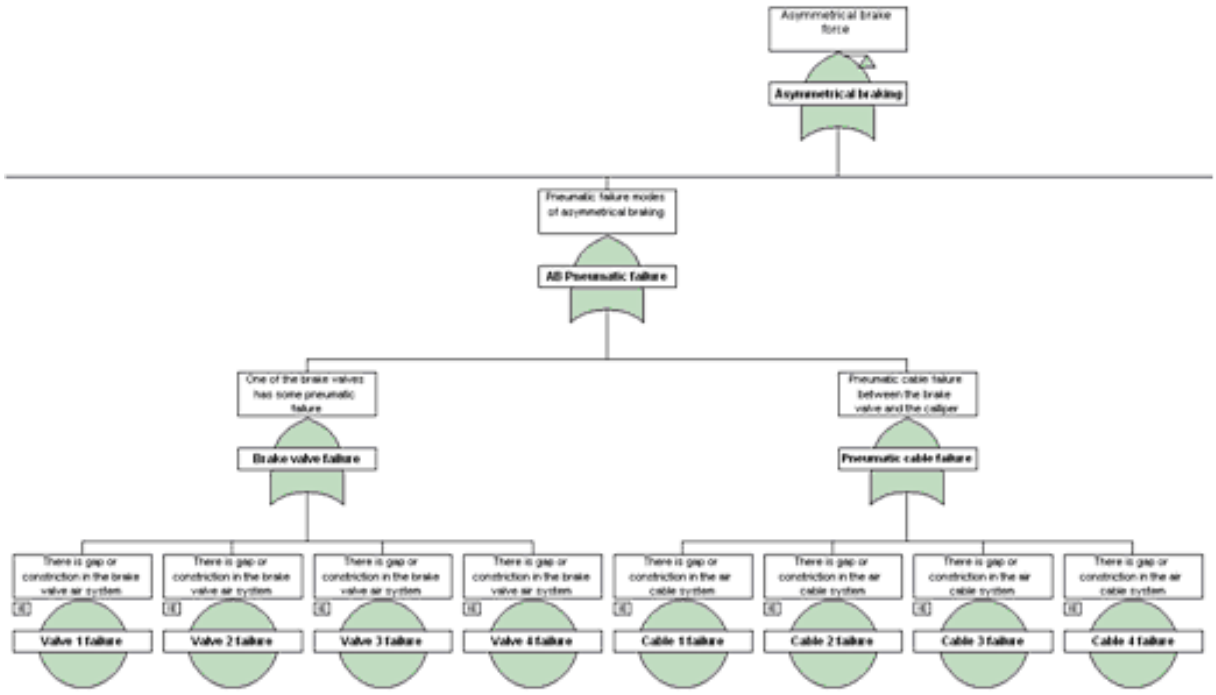

Fig. 2. FTA extract of a redundant electronic brake system with OR gates and basic events

2.2 Qualitative Risk Assessment

The risk graph method 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 EUC (Equipment Under Control) and the EUC control system.

Where a 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 the 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).

By using the qualitative method depicted in Fig. 1 and described earlier in the part of the paper, a detailed safety analysis of the relevant electronic brake system functions has been elaborated.

Table 2 lists 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, 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 kinds of energy the redundancy must be ensured in case of both one.

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

Tab. 2. Assessment of electronic brake functions

Functions	SIL level	4	3	2	1	0
Deceleration (braking)	SIL 3		♢			
ISC – adhesion and wear control	SIL 1				♢	
ISC – coupling force control	SIL 1				♢	
Brake assistant	SIL 2			♢		
Tilt prevention	SIL 0					♢
ABS	SIL 1				♢	
ATC (Automatic Traction Control) / DTC (Drag Torque Control)	SIL 0					♢
ESP	SIL 1				♢	
Differential control	SIL 0					♢
Hill brake	SIL 0					♢
Trailer brake	SIL 0					♢

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 system, 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 analysed and the right conclusion has to be drawn.

2.3 Quantitative Approach

The FTA creates a fault model, and contains the analysis of the model. The fault tree is built from top to down (Fig. **??**), 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. 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. 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 [3]. 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.

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 is a set of basic events (i.e. leaf nodes of the tree or component failures) that if they occur causes the top event of the tree (system failure). A cut-set is called "minimal" if there is no sub-set of events in that set that is also a cut-set, i.e. if there are no redundant events in the set.

3 Conclusions

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

2 **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).

3 available at `http://www.relexsoftware.com/resources/art/art_fta2.asp`.