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

BOOKLET OF PH.D. THESES

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

1. MOTIVATION AND AIM OF THE RESEARCH

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 to 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 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 by-wire technologies (Figure 1) offer functional as well as design benefits, but their application in safety-critical systems, such as the brake and steering requires special care during the design and release process.

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.

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. 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

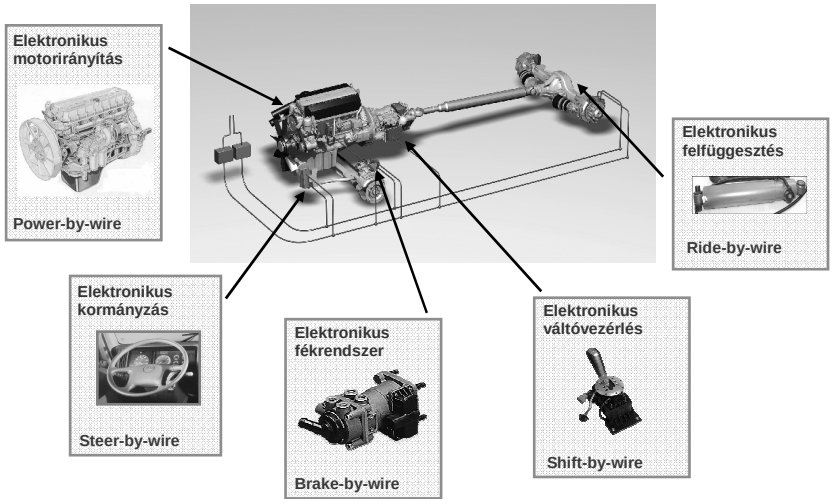
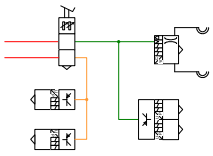
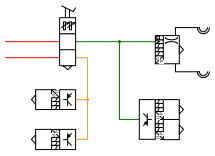
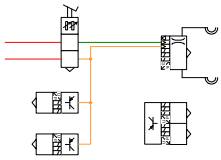
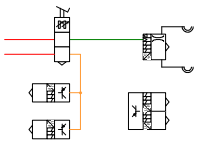
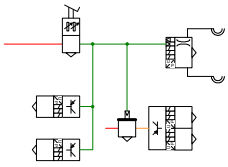
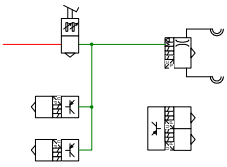


Figure 1. By-wire vehicle systems

Table 2 shows most of the possible layouts for 1E+2P (but no back-up on the rear axle or in the trailer control module-TCM) with two-circuit pneumatic foot brake valve, and also the 1E+1P layouts, where the Foot Brake Module (FBM) has only single circuit.

Table 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 electrical brake system architecture of the since 1996 in heavy commercial vehicle classes typical (in Europe) brake system architecture. It has become wide-spread in passenger cars recently. The system from the control point of view is really brake-by-wire, the deceleration demand is measured by a redundant sensor sending more signals at a time, then based on other parameters the Electrical Control Unit (ECU) calculates the brake moment that should be realized and close to the wheel the electro-pneumatic, hydraulic or in the future the electro-

mechanic actuator execute it. In this case there is no direct connection (mechanic, pneumatic) between the brake pedal and the wheel brake.

Based on experience these systems operate with high reliability. The reason, why the back-up systems are prescribed is the customer demand and a certain-level distrust. The back-up system plays role if the electronic system fails only. Table 2 shows a system with one electronic and two pneumatic circuits (1E+2P). It should be noted that the relevant requirements are also fulfilled by 1E+1P systems. The mentioned brake system, because the brake moment can be executed without the driver's intervention, integrates several additional brake functions, which cannot be provided with pneumatic brake system only. Such advanced functions are for instance, Coupling Force Control (CFC) and ESP. ABS is not a newly developed function, but is one of the most important brake functions. Without electronic intervention there is no chance for the driver to influence a specific traffic situation, while the functionality of ABS in the same circumstances results in stable vehicle behaviour.

2. APPLIED METHOD AND TOOL

Failure Mode and Effects Analysis (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 improved reliability. 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.

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 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.

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 (Figure 2), 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 is 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)?

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

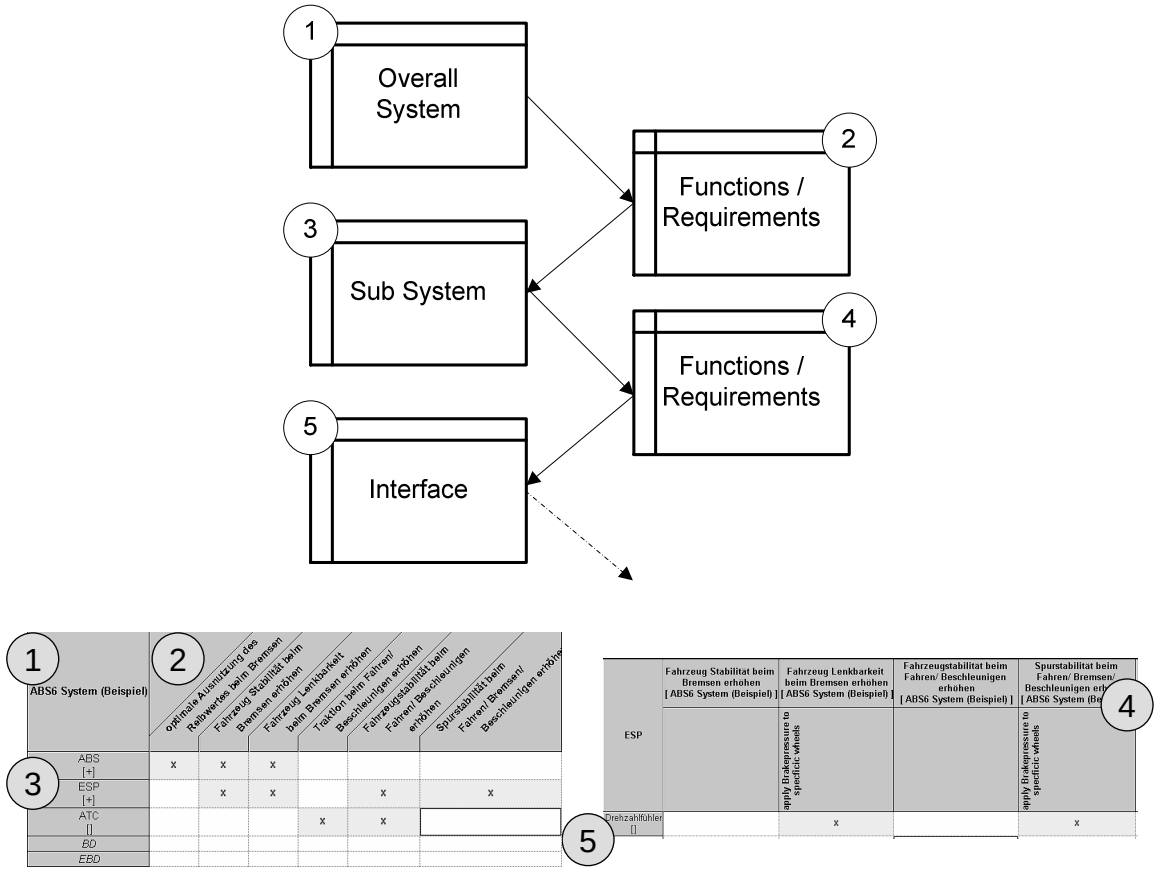


Figure 2. Matrix structure

The scope 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.

The requirements that the relevant components must meet in order to fulfil a function are mapped at interfaces (Figure 3). 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.

There are many benefits of performing FMEA, beside the already mentioned ones, 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.

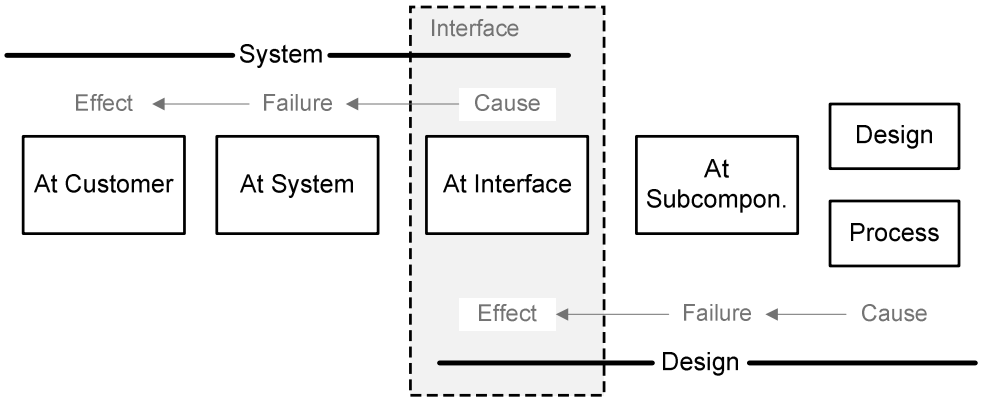


Figure 3. Representation of involved levels in System and Design FMEAs with defined interface**Error! Reference source not found.**

In additional, 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.

3. NEW SCIENTIFIC RESULTS

The proposed theses concerning this research work are summarized below including publications related to each thesis or the dissertation in the next chapter.

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 inter-

vention 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):

$$D_2 = \min\left\lfloor D_{1\_corrective\_action}; D_{1\_redundant\_corrective\_action} \right\rfloor \quad (2)$$

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

4. 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. Jankowskii), 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.