DESIGN OF REDUNDANT BRAKE-BY-WIRE ARCHITECTURE FOR COMMERCIAL VEHICLES BASED ON QUALITATIVE RELIABILITY APPROACH

Tímea Fülep

József Oberling

Department of Automobiles
Budapest University of Technology and Economics
6 Stoczek St, Bldg. J, Budapest, H-1111 Hungary
phone: +36-1-463-1828, fax: +36-1-463-3978
e-mail: fulep.timea@auto.bme.hu

László Palkovics

Knorr Bremse Systems for Commercial Vehicles
Budapest, Major St. 69, Hungary
phone: +36-1-3829 801, fax: +36-1-3829 810
e-mail: laszlo.palkovics@knorr-bremse.com

Abstract

This paper deals with the design problematic of the safety critical systems of future commercial vehicles. The development of these 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 paper derives some design aspects of commercial vehicle control system from the state-of-the-art technology of an airplane, which logically leads to similar architecture. These architectures are analyzed, and a qualitative reliability approach will be shown for their design. An insight into the additional functionality of the designed brake system will be given describing those features, which are not available in systems even with higher level of pneumatic redundancy.

Keywords: *safety, electronic brake system, autonomous systems, matrix fmea, redundancy*

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. 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 by vehicle designers and automotive industry in general [1].

By the integration of modern electronic technologies into an intelligent, a fully electronically controlled power train the overall traffic safety and traffic efficiency for heavy goods vehicles can be improved. The by-wire technologies 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.

2. Definition of the requirements – analogy to airplane industry

In this part of the paper the requirements for the autonomous vehicle control system will be derived, mostly based on the analogy to the safety critical airplane systems. Based on these requirements the upper level system architecture will be defined.

2.1. Intelligent Vehicle Systems – Define the Requirements for System Architecture

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 (Fig. 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.

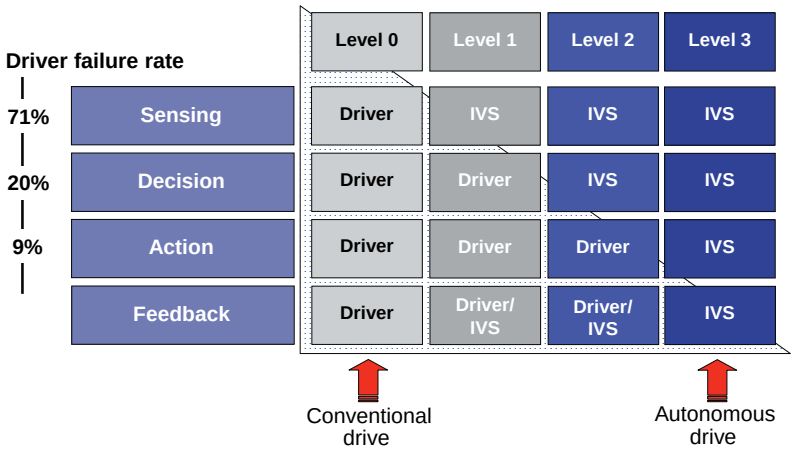

Fig. 1. Classification of the intelligent vehicle systems

Fig. 1. 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 IVS only senses and informs the driver there is no need for fail tolerance, 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.

2.2. Analogy to the Airplane Systems

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. Fig. 2. 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.

	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

Fig. 2. Dependence of the failure rate of a system on the degree of redundancy [6]

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.

2.3. Analogy between the IVS and the Airplane Control Systems – Drivers for System Redundancy in Commercial Vehicles

As already mentioned earlier in this part of the paper, 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, whose application has been started in the type approval process in some countries (e.g. Germany).

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 project (Powertrain Equipped with Intelligent Technologies) the system architecture shown in Fig. 3. has been specified, designed and realized in a prototype truck.

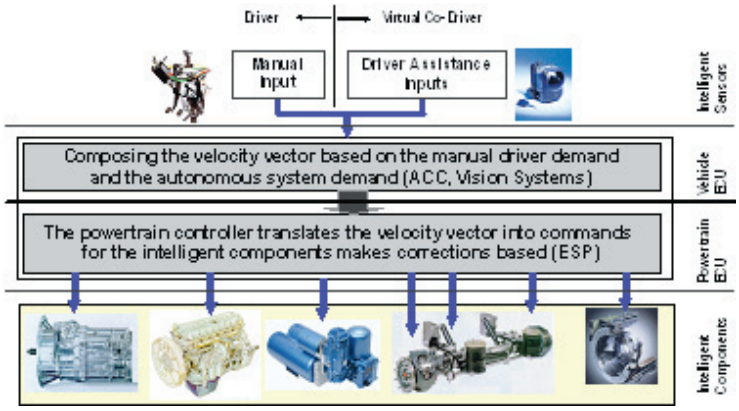

Fig. 3. Analogue vehicle control structure to the airplane systems (PEIT project)

As shown in the Fig. 3., 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 powertrain with all the actuators and sensors) commands the individual actuators and realizes the motion vector.

When analyzing the system shown in the Fig. 3., one can note the composition of the motion vector is very similar to 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, as will be demonstrated in the rest of the paper.

3. Design of the brake-by-wire system

The realization of the system described in the previous paragraph, 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% failure tolerance is required.

3.1. State-of-the-art EBS Architectures in Commercial Vehicles

The main components of a state-of-the art system are the central EBS ECU maintaining communication on several 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 (as shown in the Fig. 4.) 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 specific customer requirement today – 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 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. available. The 1E+1P architecture, however, would not suit the purposes of the autonomous driving, since external brake actuation is not possible in the pneumatic back-up mode. This means that from this perspective the system neither is fail-tolerant nor fail-safe [2].

3.2. 2E System Architecture – As a Result of a Trade-off between Design Constrains

As mentioned earlier the brake system related regulation (UN/ECE Reg. 13) does not require a completely fail-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 Fig. 4.

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. 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 Fig. 4.

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 these ECUs. The intelligent components like electro-pneumatic modulators 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) 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. 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, or 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.

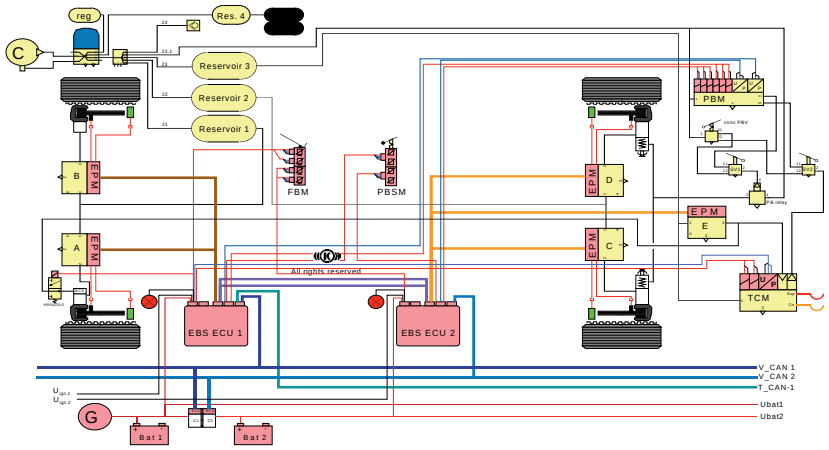

Fig. 4. 2E brake-by-wire architecture

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 [2].

3.3. Safety Gains with the Described Architecture

Although (as described in the previous part) the 2E brake system architecture of the PEIT is not fully fail-tolerant (at least in the classical sense – all function 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. 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 function, since the typical brake functions (load sensing, coupling force control, 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 the 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 [2].

4. Qualitative design approach – application in BbW design

Understandably, the above-mentioned functions 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 these failure modes in the provision of sensitive active safety functions must be established [3].

4.1. Reliability design

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 requirements meeting, which means that reliability of systems and their elements is analysed. The process of system designing is started by translating of 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 of the analysis of failure mode, effects (FMEA) enables identifying of 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 of the FMEA method. For each failure mode, the possible effect (consequence) is analyzed at a higher level, i.e. at the whole system level [1].

4.2. Well-structured qualitative reliability methodology – (MX) FMEA

Before starting the FMEA, it is worth to deploy the customer requirements to design specification level. For that purposes, several tools 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 (Fig. 5.). No components are mapped or analyzed 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 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)?

REBS Truck system	Customer requirements [REBS Truck]	Internal requirements [REBS Truck]	Legal requirements [REBS Truck]
utilization of adhesion (ABS)			X
improve steerability during braking (ABS)			X
direct controlled wheels not allowed to lock (ABS)			X
yaw moment control/steering angle correction (ABS)			X
air consumption regulations (ABS)			X
offroad operation (ABS)			X
retarder switch off (ABS)			X
ABS status info	X		
switch off diff lock (ABS)			X
ABS lamp			X
mu-jump recognization (ABS)			X
deceleration on mu-split (laden vehicle) (ABS)			X

Fig. 5. Extract of top-level representation of the requirements for a redundant electronic brake system according to ABS functions (Function links)

Using this approach, primary functions that are developed using software are mapped to subsystems of a redundant electronic brake system and then linked to their influence on the requirements for the overall system with an “X” in the matrix (Fig. 6.). These links indicate direct relationships (via ‘function’) and indirect relationships (via ‘failure’ only).

REBS Truck system	utilization of adhesion (ABS)	improve steerability during braking (ABS)	direct controlled wheels not allowed to lock (ABS)	yaw moment control/steering angle correction (ABS)	air consumption regulations (ABS)	offroad operation (ABS)	retarder switch off (ABS)	ABS status info	switch off diff lock (ABS)	ABS lamp	mu-jump recognization (ABS)	deceleration on mu-split (laden vehicle) (ABS)
ECU	X	X	X	X		X	X	X	X	X	X	X
BPU	X											X
ESPS												
Interface	X	X	X	X		X	X	X	X	X	X	X
WE	X	X	X	X	X	X					X	X

Fig. 6. System- and function matrix

The requirements that the relevant components must meet in order to fulfil a function are mapped at interfaces (Fig. 7.). 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].

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 useful tool for more efficient test planning, highlights safety concerns to be focused on, improves customer satisfaction, 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, and useful to improve communication among design interface personnel [5].

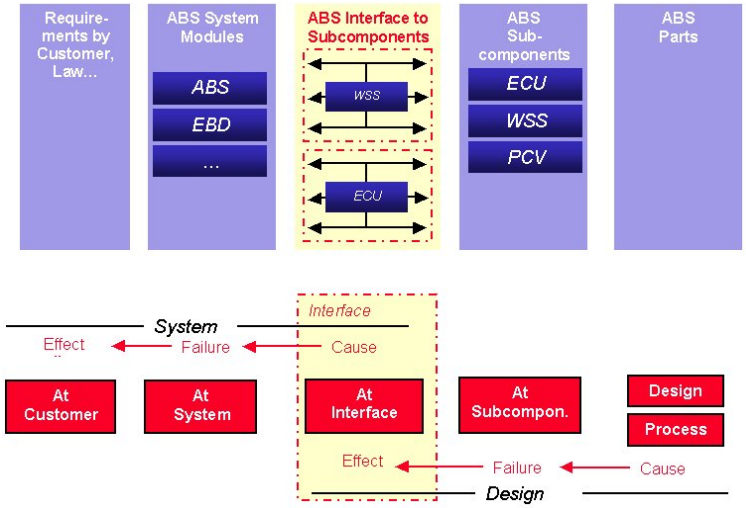

Fig. 7. Representation of the levels involved in System and Design FMEAs, with defined interfaces [4]

4. Summary

With improving or selecting suitable existing or even inventing new approaches the iterative steps of safety design can be reduced, which influences positively time and cost targets as well. The gist of conducting a qualitative reliability analysis is the good preparation for that, i.e. well-structured requirements/functions are presented from the top level until the analysis will be conducted and the same procedure for the system elements which are components of the required system.

Acknowledgments

This research project has been supported by the EU project PEIT and by the Advanced Vehicle and Vehicle Control Knowledge Center at the Technical University of Budapest.

References

[1] Popović, P., Ivanović, G., *Design for reliability of vehicles in the concept phase*, EAEC Congress 2005, Belgrade, Serbia and Montenegro.
[2] Palkovics, L., *Deliverable 7 of the EU project PEIT*.
[3] Papadopoulos, Y., Grante, C., Wedlin, J., *Automating aspects of safety design in contemporary automotive system engineering*, FISITA Congress 2004, Barcelona, Spain.

[4] Dobry, A., *Think globally, act locally; FMEA: Effective handling of complex systems,* Knorr-Bremse Systeme für Nutzfahrzeuge GmbH, Germany.
[5] Dhillon, B. S., *Design reliability: Fundamentals and Applications* http://engnetbase.com/ejournals/books/book_summary/summary.asp?id=556.
[6] Rohacs, J., *Quick market analysis and foresight on aircraft brake system.*