Handling the RAMS parameters of high dependable traffic control and automotive subsystems

Theses of Ph.D. dissertation

Géza SZABÓ
M.Sc. electrical engineer

supervisor:
Dr. József BOKOR
professor, head of department

BUTE Department of Control and Transport Automation

Budapest, 2008

TABLE OF CONTENTS

1. INTRODUCTION AND MOTIVATION

1.1 Requirements for high dependability

Nowadays in all field of the life man uses machines and equipment to support his work. As the techniques evolve, these machines become more and more complex and contain more and more electronic parts.

From the early applications, it was important to know the quality of the service beside the functions of the service. Quality is a mixture of many parameters - one of these parameters (in some cases the most important one) is the reliability. Reliability often expressed as the probability of proper functional execution.

In all of the fields of transportation and in many fields of the industry, high dependability is an important feature. In these fields the improper functions can cause high risk: loss of human lives or loss of high amount of goods. Examples for these fields are railway transportation or aviation in the transportation sector, and nuclear power generation or chemical industries in other fields.

High dependability, as one of the parameters of quality have to be considered during the design and development phases, special system architectures must be used to ensure the high dependable feature. Beside this, in these fields other measures have to be applied in order to avoid human errors in different life-cycle phases; these measures include the application of an independent expert. An independent expert validates the dependability of the system, having reliability analysis results, and searching for the weaknesses of the system. This independent validation is almost always a pre-requirement for official acceptance. According to this, reliability analysis plays an important role during the production of a system, and the reliability evaluation goes to an independent scientific field. Its importance is shown by many annual conferences as well as a lot of papers and journals published on this field.

Although reliability is an evolving field, specialists working on this area have to face new and new challenges. The evolution of electronic components is so quick and allows such a systems with brand new functionality, so traditional analysis techniques are not applicable (or not applicable in an effective way) in many cases. Beside this, the new results in theory generate new problems when they go into practice.

In this dissertation I examine the analysis-possibilities of a few year old system-behavior, the fault-adaptive behavior. First I examine the applicability of traditional reliability analysis techniques, and then I introduce a new method which can provide faster and more precise results for a class of systems. It also examined how the fault-model can be generated automatically, and the applicability of the results in railway field is also investigated.

1.2 Motivation, antecedents in the research institution

The beginning of the research work was motivated by the transportation fields' requirements against high dependable systems. Transportation is one of the most risky areas, and reduction of risk earlier and nowadays is one of the key issues.

BUTE Department of Control and Transport Automation deals with the safety issues of railways. Interlocking systems used in this field are ones of the most complexes, high dependable industrial systems. The Department is carries suitability investigations on and is issuing suitability certificates by many years. These tasks require the application of state-of-the art methods and standards, and give opportunity to get feedbacks and opinions about the applicability as well.

The research published in the dissertation was motivated by a real system, and the problems arisen during the dependability analysis of this system. Paks Nuclear Power Plant Co. started to refurbish the reactor protection system in 1995. The new protection system is based on a computerized technology, highly integrated and can provide a lot of cutting edge services. Certainly during the refurbishment project, an independent expert company has to control the dependability issues. In this task MTA-SzTAKI was involved as independent expert. One of the subtasks of the dependability control was a probabilistic reliability analysis, in which the author of the dissertation participated. The modifications and extensions of the protection system require new analyses till today.

The results published in the dissertation are related to the works of BUTE Advanced Vehicle Control Knowledge Centre (EJJT). Vehicles in road transportation are part of a safety-critical process, thus in the development and operation of their given subsystems (such as brake-by-wire or steer-by-wire systems) the risk based criterion is very important as well as how to a quite safe subsystem be designed and validated. This fact worked as a motivation for the heads of EJJT when started a separated project titled 'Definition of safety level of vehicle systems' in 2005. the author of the dissertation also participated in this project as a project leader.

1.3 Overview of dependability science

The design and validation issues of high dependable systems belong to dependability science. Dependability science is a separated science field. Dependability science can be divided to software issues and hardware issues. Hardware issues include techniques to protect system against random (and may be multiple) failures. Both system architectures and fault-detection algorithms are important [Apostolakis et. al., 1978], [Storey, 1996]. Software issues include techniques to eliminate the negative effects of human failures during the design phase. The aim is here to define the methods well-applicable during software design and software implementation and to define good software structures [Bittanti, 1987]. Both fields deal with the validation beside the design, and produce separated models [Tobias and Trindade, 1998]. As the two fields are highly connected, a new school called as 'hardware-software co-design' started years before [Csertán et. al., 1996].

On another way, dependability science can be divided to design aspects and dependability analysis aspects. This type of division has two main advantages: first, it treated hardware and software objects together; second it acts upon the task separation used during design and development. The design aspects are difficult to formalize into general rules, thus in literature a relatively few papers can be found. Contrarily the systems designed individually can be analyzed by general analysis methods, thus this field is very active.

Today one of the widely used dependability techniques is the Fault Tree Analysis (FTA). This technique has a strong theoretical basis and supported by effective

software tools [Chunning and Dinghua, 1990]. Research efforts on FTA field are made to extend the analysis to areas not covered earlier. The traditional FTA has been extended for multi-state systems [Aven, 1985]. Now research focuses on the dynamic behavior of system. Such system behaviors are cold-spare systems, delayed system-events and restart processes in computer systems [Dugan et. al., 1990]. Fault-adaptive functions which are discussed in the dissertation are also kinds of dynamic objects, and maybe since they are not widely used, their analysis is not supported.

Economical optimization requires the thrift of resources, thus the optimization of maintenance keeps importance as well. as a consequence of this, the analyses have to calculate the time-dependent dependability parameters, not only the average values. In new areas are covered by analyses (as mentioned earlier), new models describing the time-dependencies must be elaborated.

The need of automating the analysis is also partly based on economical reasons. Dependability analysis has two phases: creating a model and analyzing the model created before. Difficulties arise in the model creation phase, here is difficult to give general methods because of the strong relation between the design and the model [Kocza and Bossche, 1997].

2. THE AIMS OF THE RESEARCH

The research aims to get new results in setting reliability criterion up and evaluating of the fulfillment of criterion. The criterion setting plays an important role in the life-cycle of high dependable systems (see Figure 1, [Szabó, 2008]).

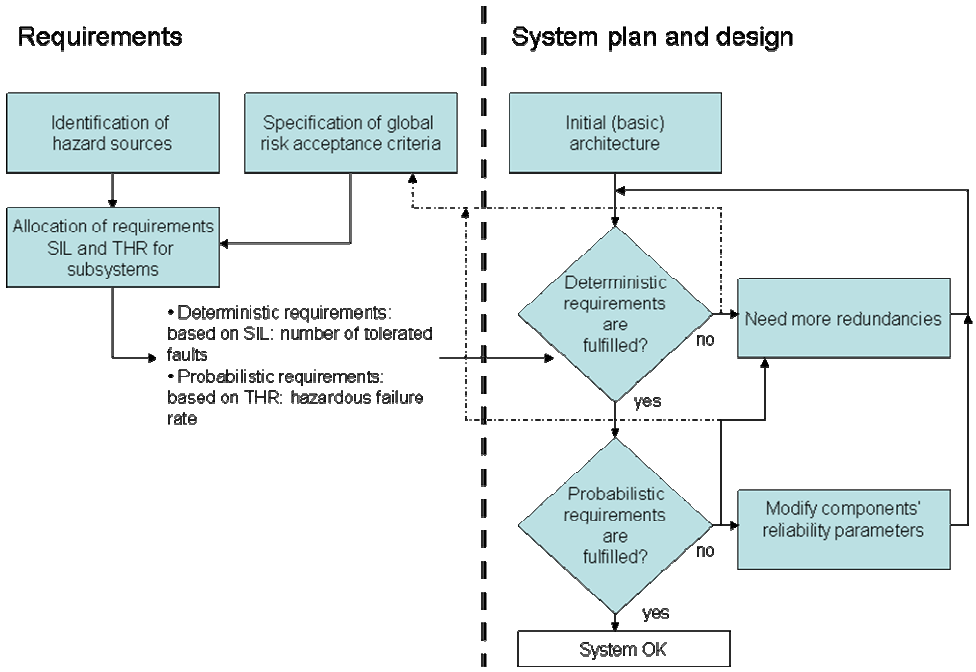

Figure 1. Specification and demonstration of the fulfillment of safety requirements

This dissertation deals with three problems in the dependability analysis (analysis of the safety requirements fulfillment): 1. It defines the fault-adaptive and fault-active functions; summarizes the traditional methods applicable for analysis of these functions and discussed their limitations; and recommends a new method to treat them in the dependability analysis [Szabó and Gáspár, 1999b]; 2. Relating to fault-adaptive functions it introduces complex failure models in order to describe the time dependent behavior of failures [Gáspár and Szabó, 1998b]; 3. It recommends automatic fault-tree model generation algorithm [Gáspár and Szabó, 1999b], [Szabó and Tarnai, 2000], [Szabó and Csiszár, 2000a].

The main application fields of dependability science are the transportation sectors (mainly the railway transportation and aviation), and nuclear power generation. In a group of systems used in different transportation areas, railway interlocking systems requires highly the high dependable design, and for these interlocking systems the proof of the actual safety level is also very important [Hudoklin and Rozman, 1985]. Both the dependable design and the proof phase rely on the pre-set safety criteria. In railway industry, different ways can be followed to produce criterion, these ways are investigated in the dissertation [Szabó and Tarnai, 1999], [Szabó, 2008], [Szabó et. al., 2008].

3. NEW SCIENTIFIC RESULTS

3.1 Dependability analyses of fault-adaptive components

In control systems, which are required to be fault-tolerant (especially in safety industrial systems) increasing dependability is one of the most important aims. Dependability can be expressed as a probability, and it is specified as requirement limit values to be fulfilled mostly during the specification phase. These limit values are based on experiences coming from previous works or set by authorities.

Increasing dependability can be made by using high reliable components (safe-life technique), using more redundancies, decreasing inspection intervals etc. In state of the art programmable systems - beside the measures mentioned above - fault-adaptive functions can also be used for this purpose. Fault-adaptive feature in this context means the ability of the system or equipment to change (re-configure) its function if failures occur. The pre-requirement of this feature is to detect the failures (or a part of failures) and to direct the information into processing units. In general principle, the additional information coming from failure detection (the signal is faulty in a detected way or not) is merged to the signal itself as a binary status information.

Adaptive components are kinds of dynamic component and special need required when they are analyzed in dependability analysis (e.g. in fault tree analysis). Fault tree analysis was selected in the dissertation as a basic method for analyzing adaptive components because of its well-elaborated methodology and a lot of widely accepted supporting software tools. The other reason behind the selection is that analyzing special dynamic behaviors (e.g. restart processes cold and hot spares) is one of the new areas of dependability science and researchers working on this area also select FTA as basic method - sometimes combined with Markov chains. Models with Markov chains are difficult to build but are easy to analyze, this is why the fault tree models (which are easy to built and easy to understand) often converted to Markov chains and after the conversion it is analyzed.

Traditional fault-tree analysis techniques work with two-state model: event describing the fault is occurs or not. When fault-adaptive feature is modeled, two-state model has not been adequate already, since event has three different states: event is not occurred; event is occurred, but we have no precise information on it (it is not detected); and event is occurred, and we have precise information on it (detected). The three different states can be handled with traditional analysis tools, separating detected and non-detected failures and modeling adaptive functions with classical AND and OR gates. Unfortunately some of reconfigurable logics require NOT and XOR gates also for modeling - these gates are not found in the basic set of fault tree elements, and a lot of FTA software cannot treat them. Separating detected and non-detected failures into two events has a disadvantage of no complex failure modes can be applied [Gáspár és Szabó, 1998b].

In the real life there are systems which fault modes or system degradation modes cannot be described with two-state models. Multi-state FTA has been developed for these systems - this multi-state FTA can handle *n* degradation states for each events and the number of states can be different for different events. The application of this type of analysis is so complicated and this is a serious disadvantage compared with

the traditional two-state fault tree analysis. As a consequence of this complication, the multi-state technique is hardly used.

As a finally described technique, a new technique is introduced called as closed-formulas method. These closed formulas were developed specially for fault-adaptive components, thus this method can provide more precise and faster results for a class of systems (systems with separated redundancies). Although a few papers can be found in literature dealing with fault-models of dynamic behaviors, no papers for fault-adaptive functions can be found. Thus my papers on theoretical aspects of this subject [Gáspár and Szabó, 1998a], [Szabó and Gáspár, 1999a], [Szabó and Gáspár, 1999b] are based on general fault-tree researches, and my papers on practical, application aspects [Szabó and Gáspár, 1998a], [Szabó and Gáspár, 1998b] are based on our theoretical papers.

I. I stated that fault-active and fault adaptive functions applied in computer based control systems can be analyzed in the view of dependability by fault tree analysis.

I.A: I find out that these functions can be modeled by so called macro models, Markov chains or the general multi-state FTA.

I.B: I establish closed formulas method to model and analyze fault-active and fault-adaptive functions in an optimal way. The closed formulas established by me are applicable for dependability analysis of control systems with separated redundancies.

3.2 Time dependent behavior of dependability parameters

Most of the dependability parameters vary their values versus time. This variation has two sources: the value of failure rate varies itself, and a lot of dependability parameters are expressed as an exponential function of failure rate (some parameters, such as testability are time-invariants). The evaluation of time-dependent behavior of system's dependability parameters is very important is situations when pre-set safety targets must be met and where dependability of many subsystems can be modified separately.

According to the statement above, we can conclude that in high dependable systems the knowledge of how parameters vary versus time (and the knowledge of which model describes this correctly) is as important as the knowledge of parameters themselves. The dissertation summarizes the general models for describing time dependencies in dependability parameters and their extension for adaptive logics (complex models).

If we work detected and undetected failure probabilities of an event and time dependent dependability of a system must be calculated, general time dependent models must be adapted for the solution. Detected and undetected failures of a given event cannot be treated as separated, independent failure events and general models are not suitable, although complex models are based on them [Gáspár and Szabó, 1998b].

II. I stated that analyzing time dependent dependability of fault-active and fault-adaptive logics requires complex failure models.

II.A: I stated that complex failure models must describe the detected and undetected failure probabilities versus time as two dependent events.

II.B: I created complex failure models for periodically tested components.

3.3 Generating fault-models automatically

During the development of high-dependable systems (nuclear power plant protection systems, railway interlocking systems, airplane on-board systems etc.) the assessment of the dependability (in a probabilistic and/or in a deterministic way) is very important step [Bokor et. al., 1997]. For this assessment many of analysis techniques can be used, such as Failure Modes and Effects Analysis (FMEA), Markov analysis, Event-tree analysis, Fault-tree analysis and so on. Maybe the fault tree analysis is the method which is used mostly - it has a strong theoretical background as well as strong software support.

Traditional fault-tree analysis starts with a manual fault-model construction. This phase of analysis requires deep system-knowledge and large experience with system- and analysis methods. Beside this, manual model construction is time-consuming and thus very expensive, and can be a source of human mistakes and errors. The analysis becomes faster and error-free if the fault-model generated automatically. Another important point is that the model generator can be verified and during a particular model generation only the pre-requisites must be proved or verified, but mot the whole generated model.

The automatic fault-model generation solves the problem of handling the system-variants in an equivalent way and allows in-depth analysis during quite short time. As a consequence of this, during the development phase it provides quasi on-line dependability analysis and this is a high value support for designers.

In our case the automatic fault-tree generation was motivated by the adaptive logics also. Modeling adaptive logics in many cases requires large sub-trees which make the model building slow and very complex.

Certainly in many places of the world scientists work on automatic model generation. As new results, we can mention the RIDL graphical language and its fault-model which supports the component (low) level modeling of computerized systems; KB3 system for modeling of power plants' mechanical components; Formal Risk Analysis (FRA) which describe the relationship of the system being analyzed and its environment; IRAS which method is based on system block diagram.

The methods and works mentioned above allow in-depth analysis, but cannot take into account a feature of modern computerized systems to modify the high level functions without modifying hardware structure; and cannot take into account the requirement on this level of analysis that only a few parameters of systems components are available. This was the motivation behind the development of a new generation algorithm [Gáspár and Szabó, 1999a], [Gáspár and Szabó, 1999b], and

the evaluation of applicability in railway interlocking systems [Szabó and Tarnai, 2000].

The steps of the new generation algorithm:

Step 1.: Selection of the point of the system we want to analyze (top event). Selection of the type of the model generation. We can distinguish two main kinds of analysis which require different fault-model: the analysis of function masking (fault of a function) and the analysis of a spurious actuation (unwanted function execution).

The top event, a not proper working of a selected function occurs if the hardware unit which executes the function has a fault ***OR*** this hardware unit does not receive correct input signals. Consequently we need a branch in the fault tree to model this: we need a subtree describing the hardware fault (failure modes) and we need a functional subtree which will contain the faults and failures which can produce incorrect input signals for the selected function. Between the two subtree, OR fault tree gate makes the connection.

Step 2.: Establish the two subtrees. Subtree describing hardware failures can be created based on the failure modes definition and failure parameters stored for a rule collection for this hardware type. Subtree describing the incorrect input signals will be branched further according to the function under analysis.

Step 3.: Searching for the first input of the function under analysis. In a further we treat the function provides the input for the actual function as new actual one. If this function executed by a different hardware unit as executed the previous one, we need two subtree again, a hardware and a functional subtree and there will be an ***OR*** relationship between them (see the previous step). If the actual function is executed by a same hardware, we do not need at this point a kinds of subtrees mentioned above (the failures of this HW were modeled earlier already.

Step 4: Searching for the first input of the function under analysis. If this input is defined as system input (INPUT function), no further functional modeling is necessary at this way, only the input hardware must be modeled by creating a hardware subtree (and this step is necessary only if the input is in a separated hardware as previous function). Consequently input functions form ends of functional description. If the actually found function is not an INPUT function, we need to decide whether new hardware subtree is necessary or not, and after we need to model the functionality in the functional subtree. Consider that from this point the Step 3. is repeated till an INPUT function has reached.

Step 5: If the actually modeled function was an INPUT, after deciding if hardware subtree is necessary or not, a special modeling function, rollback is executed, because the INPUT function is an end of the functional description and no other analysis is necessary here. Rollback function goes back in the functional description searching a function to be analyzed which has an input not analyzed earlier. To manage this, we append a counter for every function to be analyzed - this counter shows the way in which the model generation was executed. If the number of this counter equals to the number of inputs of a function analyzed, rollback function can go to a higher level back. If the number of this counter is lower than the number of inputs, the counter is increased and Step 3. is executed, but for not the first input, but for the input pointed by the counter. (More exactly Step 3. is always executed for the first not modeled input of a given function.) In a fault tree, new FT gate to be inserted

if function with not modeled input was found. In order to maintain the connection between functions and fault tree and in order to find a point to where the new gate must be inserted, every function has a pointer points to a fault tree gate modeling the relationship between the function's inputs and outputs.

Modeling algorithm can finish is rollback function can go back to the top event function and all of the inputs of this function is always processed.

The algorithm shown above was verified by analyzing real tasks in the world-wide accepted RiskSpectrum software environment [Szabó and Csiszár, 2000a], [Szabó and Csiszár, 2000b], and the applicability for special railway cases was also examined [Szabó and Tarnai, 2000].

III. I stated that fault tree model of computer based industrial control systems can be generated automatically by processing the functional description of the system.

III.A: I stated that automatical model generation requires the hardware and functional description of the system as well as the description of the relations between hardware and functions. Descriptions should be formalized to support processing.

III.B: I stated that model generation can be made by following the functional paths, searching and modeling hardware modules and their boundaries. Modeling is made using a formalized rule-collection.

III.C: I developed an algorithm to generate fault-models automatically.

III.D: I validated the algorithm using generator software integrated into RiskSpectrum software environment.

3.4 Creating dependability limit values for interlocking systems

Different transportation areas set different dependability requirements against systems used in track-side and on-board. The two areas which have the highest requirements are airplane on-board systems and railway interlocking systems.

For on-board airplane systems it is not possible to find a safe system state except working state, thus correct working of these systems must be ensured even in a faulty situation. This aim can be reached using fault-tolerant redundant systems.

For railway interlocking system man can accept the system state in which no train movements are enabled as a safe state. System shout-down and safe state reaching in case of failures in interlocking systems treated as correct reaction. This behavior characterizes the fail-safe systems. By the way we must know that continuous operation keeps important role in faulty situation - not in respect of safety but in availability (economical) view.

When a new interlocking system is installed or an old one renewed and put back to operation, it must be proved that the pre-defined requirements are met. This process is referenced as validation. Validation must cover all the three areas of requirements: functional, technical and dependability. The proof of functional and technical

requirements' fulfillment, a failure-free system is examined. In contrast with this, the proof of dependability requirements starts with assumptions of failures [Görög et. al., 1998].

Examination methods used here are:

- Deterministic approach,
- Deterministic approach using some probabilistic values,
- Probabilistic approach.

Dependability requirements (limit values) can be set according to:

1. Originating from the tolerable hazard level,
2. Adapting requirements used in other industries,
3. Calculating the dependability level of systems in operation for longer time,
4. Originating from the non-probabilistic validation methods of existing systems.

IV. I proved that dependability limit value can be established based on previously accepted systems for probabilistic analysis of interlocking systems.

IV.A: I declared that neither safety nor reliability can be quantified if the system was accepted previously with pure deterministic approach.

IV.B: I proved that upper limit of safety can be calculated for systems which were accepted previously with MÜ8004 standard (this calculation relies on that two undetected failures exist in a given time can be dangerous). I declared that a value obtained in this way can be used as limit value for new interlocking systems. The value of upper limit is independent from the reliability parameters of components used in the system, but it depends on the multiplication factor used for second error occurrence time. I suggested the value of upper limit; the suggested probability limit value is 10^{-6}.

IV.C: I declared that the availability of systems accepted previously with MÜ8004 standard cannot be calculated.

4. REFERENCES

4.1 Papers and articles relating to the dissertation and theses published by the author of dissertation

[Bartha et. al., 2005]: Bartha T. – Varga, I. – Soumelidis, A. – **Szabó, G**.: Implementation of a Testing and Diagnostic Concept for an NPP Reactor protection System. *In: Dependable Computing – EDCC-5 (Eds. M. Dal Chin, M. Kaaniche, A. Pataricza). Proceedings of the 5th European Dependable Computing Conference. Springer*, pp. 391-402, Budapest, 2005.

[Bokor et. al., 1997]: Bokor, J. - **Szabó G.** - Gáspár P. - Hetthésy 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.

[Gáspár and Szabó, 1998a]: Gáspár P. - **Szabó G.**: Analysis of Adaptive Multi-State Logic in Fault-Tolerant Systems. *Proceedings of the Probabilistic Safety Assessment and Management - PSAM 4 Conference*, pp. 13-17, New York, 1998

[Gáspár and Szabó, 1998b]: Gáspár P. - **Szabó G.**: Complex Failure Models for Dependability Assessment. *Digest of FastAbstracts, International Symposium on Fault Tolerant Computing, FTCS-28*, pp 94-95. Munich, 1998.

[Gáspár and Szabó, 1999a]: Gáspár P. - **Szabó G.**: Automatic Fault-Tree Generation as a Part of a Complex Development System. *Proceedings of the 3rd International Scientific Conference Elektro '99, Section Information & Safety Systems*, pp. 19-24, Zilina, 1999.

[Gáspár and Szabó, 1999b]: Gáspár P. - **Szabó G.**: On-line System Verification Applying an Automatic Fault-Tree Generation Method Integrated into Development Tools. *Proceedings of the European Safety and Reliability Conference-ESREL* pp. 809-814, Münich, 1999.

[Görög et. al., 1998]: Görög B. - **Szabó G.** - Tarnai G.: Biztosítóberendezési funkciók PLC-s megvalósításának biztonsági és megbízhatósági szempontú elemzése (in Hungarian). *Vezetékek Világa, Magyar Vasúttechnikai Szemle, 1998. Vol. 3. pp. 6-10.*

[Szabó and Csiszár, 2000a]: **Szabó G.** – Csiszár Z.: Fault-Tree Synthesis: a Practical Approach. *TU Budapest, Research News, Special Issue 2000.*

[Szabó and Csiszár, 2000b]: **Szabó G.** – Csiszár Z.: Automatikus hibafa generálás – Tanszéki kutatási jelentés (in Hungarian). *BME Közlekedésautomatikai Tanszék*, 2000.

[Szabó and Gáspár, 1998a]: **Szabó G.** - Gáspár P.: Probabilistic Dependability Analysis of Adaptive Functions: A Fault-Tree Based Approach and Its Application in Transportation. *Periodica Politachnica Ser. Transp. Eng., 1998. Vol. 26, No 1-2, pp. 187-200.*

[Szabó and Gáspár, 1998b]: **Szabó G.** - Gáspár P.: Practical Aspects of Dependability Analysis for Vehicle Systems. *Proceedings of the 6th Mini Conference*

on Vehicle System Dynamics, Identification, and Anomalies, VSDIA, pp. 437-446. Budapest, 1998.

[Szabó and Gáspár, 1999a]: **Szabó G.** - Gáspár P.: Fault-tree analysis of System Functionality modelled as Binary Adaptive Functions*. Proceedings of the European Safety and Reliability Conference-ESREL* pp. 1033-1038, Münich, 1999.

[Szabó and Gáspár, 1999b]: **Szabó G.** - Gáspár P.: Practical Treatment-Methods of Adaptive Components in the Fault-Tree Analysis*. Proceedings of the Annual Reliability and Maintainability Symposium*, pp. 97-104, Washington D.C., 1999

[Szabó et. al., 2008]: **Szabó G.** – Sághi B. –Darai L.– Jakubovics J. – Héray T. – Kirilly K. – Buzás M. – Gál I.: Biztosítóberendezések időszakos vizsgálatainak koncepciója (in Hungarian). *Vezetékek Világa, Magyar Vasúttechnikai Szemle*, 2008.

[Szabó et. al., 2004]: **Szabó G.** – Szabó K. – Zerényi R.: Safety Management Systems in Transportation: Aims and Solutions. *Periodica Politechnica, Ser. Transp. Eng, 2004.* Vol. 32. No. 1-2, pp. 123-134., 2004.

[Szabó and Tarnai, 1999]: **Szabó G.** - Tarnai G.: Dependability Analysis of Interlocking Systems - A Comparison of the Probabilistic and the Deterministic Approaches. *Proceedings of the 3rd Inernational Scientific Conference Elektro '99, Section Information & Safety Systems*, pp. 7-12, Zilina, 1999.

[Szabó and Tarnai, 2000]: **Szabó G.** - Tarnai G.: Automatic Fault-Tree Generation as a Support for Safety Studies of Railway Interlocking Systems*. Proceedings of the IFAC Symposium on Control in Transportation Systems*, pp. 453-458, Braunschweig, 2000.

[Szabó and Tarnai, 2002]: **Szabó G.** – Tarnai G.: A vasúti biztosítóberendezések biztonságigazolási módszereinek fejlődése, az új, eurokonform szabályozás alkalmazásának kérdései (in Hungarian). *Vezetékek Világa, Magyar Vasúttechnikai Szemle*, 2002/4. szám, 5-9 oldal, 2002.

[Szabó and Tarnai, 2003]: **Szabó G.** – Tarnai G.: A vasúti biztonság bizonyítására vonatkozó új európai szabványok alkalmazási kérdései (in Hungarian). *Vezetékek Világa, Magyar Vasúttechnikai Szemle*, 2003/1. szám, 2-6 oldal, 2003.

[Szabó, 1995]: **Szabó G**.: Bevezetés a hibafa-analízisbe. Oktatási segédlet. (In Hungarian). *BME Közlekedésautomatikai Tanszék*, 1996.

[Szabó, 2007a]: **Szabó G.:** Kockázati alapú fejlesztési kritériumok a járművek biztonsági rendszereinél (in Hungarian). *Jövő Járműve*, 2007/1-2 szám, 38-41 oldal, 2007.

[Szabó, 2007b]: **Szabó G**.: Műszaki okú kockázatok kezelése a közlekedésben (in Hungarian). *Innováció és fenntartható felszíni közlekedés c. konferencia.* Magyar Mérnöki Akadémia, 2008. Available:
http://kitt.bmf.hu/mmaws/2007/pages/participants.html.

[Szabó, 2008]: **Szabó, G**.: Setting Up the Concept of Periodic Testing and Examinations of Safety Systems. *In: Formal Methods for Automation and Safety in Railway and Automotive Systems (Eds. G. Tarnai, E. Schnieder). Proceedings of Symposium FORMS/FORMAT2008*. pp. 321-324, Budapest, 2008.

4.2 Papers by other authors referenced in this booklet

[Apostolakis et. al.,1978]: Apostolakis, G. - S. Garribba - G. Volta, (Eds.): Synthesis and Analysis Methods for Safety and Reliability Studies. *Plenum*, 1978.

[Aven, 1985]: Aven, T.: Reliability evaluation of multistate systems with multistate components. *IEEE Transactions on Reliability*, Vol. R-34, No. 5., pp. 473-479. 1985.

[Bittanti, 1987]: Bittanti, S. (ed.): Software Reliability Modelling and Identification. *Springer-Verlag*, 1987.

[Chunning and Dinghua, 1990]: Chunning, Y. - S. Dinghua: Classification of fault trees and algorithms of fault tree analysis. *Microelectronics and Reliability*, Vol. 30, No. 5, pp. 891-895. 1990.

[Csertán et. al., 1996]: Csertán Gy. – Pataricza A. – Selényi E.: Design for Testability with HW-SW Co-design. *Periodica Polytechnica*, Vol 40(1), pp. 25-37, 1996.

[Dugan et. al., 1990]: Dugan, J. B. - S. J. Bavuso - M. A. Boyd: Fault trees and sequence dependencies. *Proc. of the Annual Reliability and Maintainability Symp.*, 1990, pp. 286-293.

[Hudoklin and Rozman, 1985]: Hudoklin, A. - V. Rozman: Safety Analysis of the Railway Traffic System. *Reliability Engineering and System Safety,*. Vol. 37, No. 3., pp. 7-13. 1985.

[Kocza and Bossche, 1997]: Kocza G. - A. Bossche: Automatic fault-tree synthesis and real-time tree trimming, based on computer models, *Proc. Ann. Reliability & Maintainability Symp.*, 71-75.,1997

[Storey, 1996]: Storey, N: Safety-Critical Computer Systems. *Addison-Wesley*, 1996.

[Tobias and Trindade, 1998]: Tobias, P. –D. Trindade: Applied Reliability. *Chapman &Hall /CRC*, 1998.