Predictive Analysis of Mission Critical Systems Dependability

Martin Daňhel[1, 2], Hana Kubátová[1],
Radek Dobiáš [1, 2]

[1]Department of Digital Design
Faculty of Information Technology, Czech Technical University of Prague
Prague, Czech Republic

[2]AŽD Praha s. r. o.
Research and Development Department
Prague, Czech Republic

martin.danhel@fit.cvut.cz, hana.kubatova@fit.cvut.cz, radek.dobias@fit.cvut.cz

***Abstract* - This paper describes the analysis of dependability and predictive reliability. The proposed methodology is based on hierarchical models and the generally acclaimed standard MIL-HDBK 217F. The equipment is a real component of the railway interlocking system in Czech Republic. The equipment is designed for high dependability and with respect of disturbances caused by the near environment. A possible encapsulation using UML to model processes affecting the reliability is shown.**

Keywords - dependebility computation, FMEA/FMECA, railway signalling equipment, predictive analysis, hierarchical model, SHAMAP

I. Introduction and Motivation

Requirements for the predefined level of reliability and safety parameters become recently inseparable part of the technical requirements for modern technical systems. The development and the design methods of any technical system will not be successful without clearly defined requirements for the reliability and the safety issues. These requirements are usually formulated by a future user of the designed systems (mainly when the system is developed for some concrete user) and by a manufacturer (especially for systems intended for the serial production). For systems which failures could lead to health or human lives hazard , large material losses, the requirements for reliability and safety are often laid down by mandatory regulation (laws, notice, directives, standards…) [1].

There are also requirements to prove requested level of reliability before proceeding to own manufacturing system or before a construction of the prototype. These requirements follow from experience that every forced change of the system structure implemented before preproduction phases is considerably simpler and cheaper than in following phases. Practically, a customer requires a proof, that the developed system will meet his requirements for reliability and safety in starting phases of the system lifecycle. This proof is obligatory and in the case of later system failure, there is a possibility of high sanctions for the manufacturer. It is accepted that the results are mainly used as a proofs of prediction analyses of reliability and safety [1].

In the past the safety function in the railways application was always based on the gravitational attraction (e.g. by relays) for the stop-signals and on the mechanical pull or on the big value of the electrical current for the permit signal.

Now the electronics blocks are being used for the railway interlocking system. Since the electronic blocks were successfully used in the space program, the railway infrastructure managers have accepted to use these blocks in railway interlocking equipment's, too. High availability of such electronic devices has to be shown before and during the trial operation, and also during the standard operation of the railway equipment. The reliability model [2] is a method for showing its high dependability parameters in such cases.

This paper is focused on the predictive analyses methodology used in the railway applications. However the results can be used in other types of safety related systems, too. The following text describes railway interlocking and signalling equipment in the section *Example: Railway Interlocking Equipment with Electronic Blocks.*

The basic questions to be solved are the following:

- How do you to determine the optimal requirements for reliability parameters?
- How to ensure these requirements concurrently both in development and production processes?
- How to verify the actually achieved level of dependability (reliability and safety) parameters?
- How to ensure the best (optimum) reliable operation?

The purpose of the reliability testing is to provide objective and reproducible data about the system reliability.

II. Background and State of the Art

The base methods of the increasing the dependability parameters are the following:

- Backup: dynamical and static;
- Redundancy: spatial or time;
- Robust components.

The dependability parameters are called **RAMS** standards [3]:

Reliability is the probability of a correct component function over a given period of time under a given set of operating conditions.

Availability of the system is the probability that the system will operate correctly at a given time.

Maintainability is the ability of a system to be maintained.

Safety is a property of the system that it will not endanger human life or environment.

Current approaches of predictive analysis can be divided into two types, qualitative and quantitative ones. However, both types can be used simultaneously to solve very complex system properties.

A. Qualitative AnalysisFMEA/FMECA

A failure Mode and an Effect Analysis (FMEA) is a structured qualitative method used to identify system failures and their causes and consequences. If the estimate of consequences of the occurrence of a failure criticality and probability is included into the analysis we can talk about: Failure Mode, Effects and Critically Analysis (FMECA). FMECA method is not a standalone method of analysis; it is merely an extension of FMEA. The basic principles of an implementation and an application of the method can be found in standards [4], [5].

FMEA method belongs to the most widely used method for predictive analysis of reliability and safety of the system from lower to higher level system classification and it examines the failure of a system to a higher levels. This method is inductive (bottom-up one), which performs qualitative analysis of reliability and system safety from lower to higher level system classification and which explores the objects failure at lower levels. This method says when these failures are transmitted to the higher system levels. This method is applied in almost all kinds of industries where something should be improved, during production time, development and delivery of services. The primary objectives of FMEA/FMECA are as follows:

1. The evaluation of all adverse consequences and sequences of events.
2. The detection of all system function failures.
3. The classification of the identified failure manners.
4. The improvement of the design.
5. The support for the creation of the maintenance plan.

B. Quantitative Analysis

Reliability models are used for predictive analysis of the reliability, by which the proposed system and its states will be described. The basic and the most common models used in reliability include following models:

- Reliability Block Diagrams (RBD), together with the FTA are used for the analysis of complex fault states (current failure more elements). Their use is usually limited to the failure states with hazardous or catastrophic consequences. RBD can be put into the hierarchical models [6].
- Fault Tree Analysis (FTA) is used for the same purpose as reliability block diagrams. FTA can be put into the hierarchical models too [6].
- Markov chains are used during the development and certification processes to solve complicated failure states. (They are used when FTA or RBD is not possible to use). Markov chains can be placed into the hierarchical models [6].

C. Current Approaches to Predict the Reliability Parameters Acceptable Industry Standards

a) MIL-HDBK-217F

The Reliability Prediction of Electronic Equipment – U.S. military standard are used to estimate the failure rate for electronic equipment [7]. Data for this standard comes from the large amount of collected data by the U.S. armed forces and they often form the basis for the estimations used in this area. This norm has become an industry standard over time. The standard distinguishes two different methods for reliability parameters ‘calculating:

Stress Analysis Prediction

This method is based on the knowledge of the specific interconnection parts. The stress for each part is calculated by the wiring diagram.

Count Reliability Prediction

This method is applicable in the initial stages of a design process, when there are no data needed for the application of the stress elements method.

The advantage is that this standard is available as a free package. The standard is already time-tested and therefore the systems can be comparable in terms of reliability with other ones. The disadvantage is that this standard was updated in 1995 and its development was finished.

b) MIL-HDBK-338B

The Electronic Reliability Design Handbook standard is mentioned only to complete the standard MIL-HDBK-217F, which is basically connected to. It is an important basis for the methodology of FMEA / FMECA, because it is formed for similar purposes.

c) Database EPRD-97 a NPRD-95

These databases Electronic Parts Reliability Data - EPRD-97 and Non-electronic Parts Reliability Data - NPRD-95 were created by American Society of Reliability Analysis Center (RAC). They complement each other and do not contain duplicate data. The disadvantage is their price and the impossibility to specify components used in railway applications.

d) FIDES

FIDES is an European standard (French consortium of industrial companies aerospace and defence industry) equivalent MIL-HDBK-217F for electronic equipment. It is the latest methodology of the reliability prediction, which is primarily used in the aviation (Airbus [8]). The main disadvantage is especially the price of a complete software solution containing this methodology. The database is also not paper-available but a manual containing this methodology can

be free downloaded from the web. Another drawback for the intended application is the practical impossibility to use commercial components with the required parameters knowledge.

e) GBJ/z (299B)

The Chinese equivalent of MIL-HDBK-217F for electronic equipment disadvantage is that it is not available in Czech or English language versions.

f) RAC PRISM

This standard contains successful application of some military standards. It is a method for the reliability prediction calculating using electronic and non-electronic components. It is not available as a free paper version but only in the software package.

g) RELEX

The manufacturer is Relex Software Corporation (USA). The above standards are not primarily intended for the use in railway signalling equipment. This is due to the high voltages and currents; it is primarily used in specific parts, which these methodologies mostly do not describe.) At the same time MIL-HDBK-217 standard is used for plenty of years, including various modifications with associated operational databases.

III. PREDICTIVE ANALYSIS

There are four main steps (phases) in the implementation of predictive analysis reliability and safety:

1. **Functional and technical analysis**. The phase "Functional and technical analysis" is used to collect data and maximize awareness of elementary elements of the system.
2. **Qualitative analysis.** The final goal of the qualitative analysis is to find all the faults, their causes and to describe the consequences, which failures could have and to specify their effect to the system operation. The qualitative analysis will be used primarily to build appropriate model of the system reliability. The modelling of the system reliability is closely connected to the modelling of physical phenomena and processes (degradation processes), which can result in certain stage of operation until a fault state comes.
3. **Quantitative analysis.** The calculation (or the estimation) of a quantitative (numerical) values of appropriately selected indicators of the reliability is performed under the terms of the quantitative analysis. The numerical values of a phenomenon probability can be obtained from the reliability model. The quantitative analysis can be generally done "by hand" if the systems are simple and not too large; otherwise it is done by using some specialized software tools.
4. **Synthesis of results**. The phase "synthesis of results" is used to assess the required level of reliability, to determine conclusions and recommendations.

This paper is primarily focused on the highlighted parts – Qualitative and Quantitative Analysis on the Figure 1.

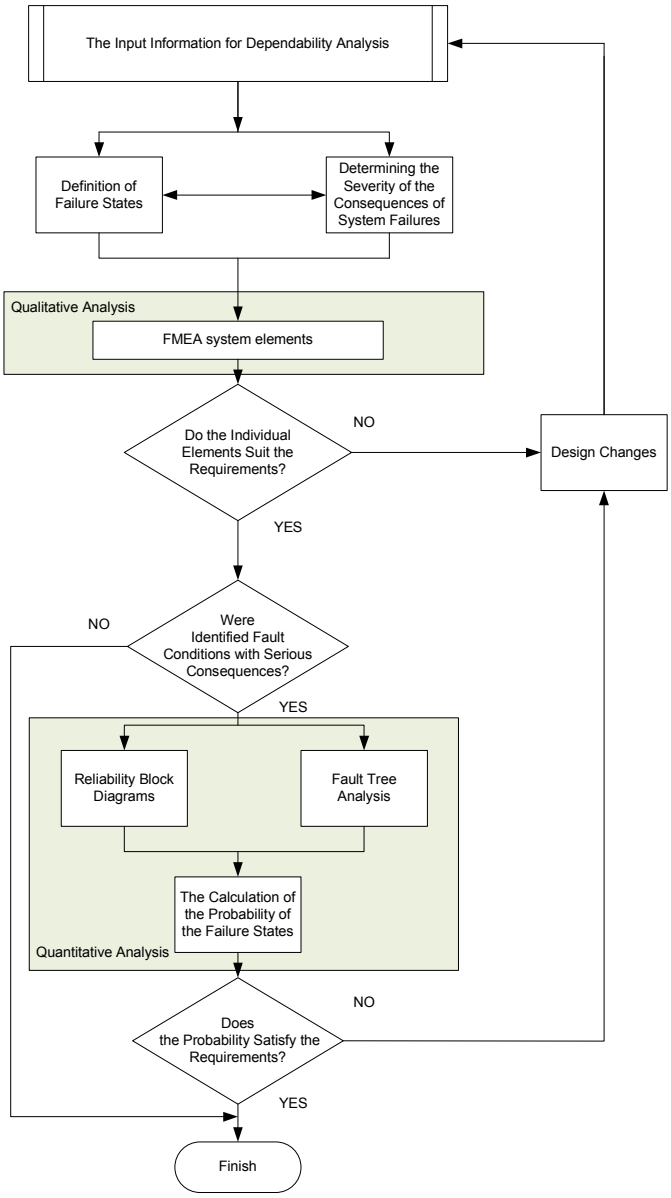

Figure 1.The process of predictive dependability analysis

IV. THE METHODOLOGY BASED ON HIERACHICAL BLOCK MODELS

The contribution of the proposed methodology consists of the simplification of the model: either of the whole one or of a part of a system. The simulation or the verification is made easily using the model. It is necessary to check and compare the results with the observed reality permanently with respect to the recommendations of the standard [3], [9].

Hierarchical reliability block models can be used if the system is composed of the independent components (Reliability Block Diagrams [6]). The basic idea of the hierarchical block model is the possibility to imagine a large block model as a separate block. This idea can be used for both abstraction and simplification of the models. This idea is currently used for predictive analysis of FMEA/FMECA

method, where safety of the system is calculated from the lower level to the higher level (Bottom-Up method). Furthermore other reliability models can be nested into these models. The model of individual parts levels (elements from the every Printed Circuit Boards - PCB) is shown in Figure 2.

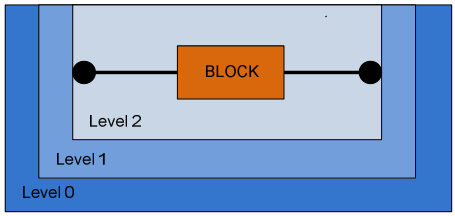

Figure 2.The process of predictive dependability analysis

A. *Tree Structure*

The hierarchical models can be easily visualized and transferred using a tree structure. It is possible to generate the equation with the parameters required for the calculations using the model [10], [11], [12].

B. *Sub-model*

The sub-model is a model nested into the block at the higher level. Each block of the hierarchical model may contain another model type. A sub-model of any particular block in the design may not necessarily be the block model, but Markov reliability model, stochastic Petri net, etc. [10], [11], [12].

C. *Model with a Backup*

The backup system can be modeled by a tree structure. Each leaf of a tree must be an element representing a part of the system, see Figure 3. There can be any mathematical operation at each node.

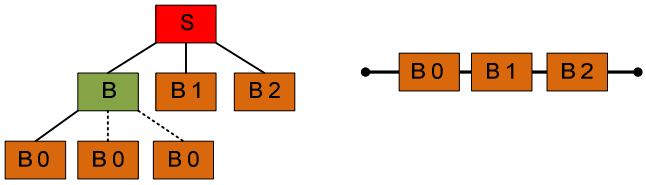

Figure 3.Hierarchical model with backup

Node B has to be replaced by an adequate mathematical operation corresponding with the types or parameters of a used backup. The mathematical operation expressing a backup process can be simplified by the estimation and/or experience.

D. *Possible Ways to the Design*

It is possible to distinguish two basic proposals:

1) *Top-Down*

This way calculates the reliability parameters of the system or its part gradually. The model will consist of a single block that will be refined by inserted sub-models. Each level of sub-models will refine the model until the required level of details is achieved.

2) *Bottom-Up*

A user knows all the elements of the system. He builds a model from these elements (that can be generalized by using a hierarchical model) and then he determines its reliability parameters. These parameters will correspond with the data of the whole system. This methodology is used in predictive analysis such as FMEA/FMECA.

E. *SHAMAP*

We have implemented a software tool [10], [11], [12] for modeling and calculations of reliability parameters. This tool is developed to satisfy the requirements of practice over the time (e.g. for hierarchical models and reliability models for predictive analysis). The SHAMAP tool allows symbolic computations that can be used for calculations of reliability parameters for the railway equipment (but not only for them).

The tool supports the following reliability models: Markov models, RBDs, FTAs. The hierarchical models are supported, too. The calculations are performed in software mathematical tools (Maple, Mathematica). The original purpose of the tool was very accurate calculations (calculations in a symbolic form) of reliability parameters using the aforementioned mathematical systems.

There are some issues concerning numerical accuracy during the calculations of the models of safety devices. For example, the probability of potentially dangerous conditions that are applied in the models according to the recommendations of EN standards [3] are in the order of around 10^{-10}, which brings major complications in the numerical calculations (the calculations are frequently impossible not only in a simple precision, but also in the double precision). Therefore we propose to use SHAMAP tool with the symbolic computation possibility.

V. Example: Railway Interlocking Equipment with Electronic Blocks

The Programmable Coding Unit – *PCU* is an equipment currently developed in AZD company. The Czech Republic railways and many other European and non-European countries use the low frequency continuous train controls requiring the construction of the appropriate coding units. Besides, most signaling systems use oscillating light signals where oscillations should be defined safely.

It is necessary to use different coding units for each type of continuous train control and the different signal set for continuous train controls and signals, because of the differences of codes and signal light oscillations. The basic principle of the *PCU* is shown in Figures 4, 5 and 6.

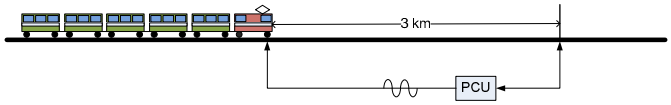

Figure 4.There is a train on rails before the signaling equipment. The signaling equipment indicates free passage. The *PCU* emit a signal into rails. This frequency means that everything is in order.

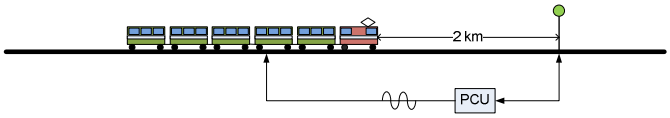

Figure 5.Here is the critical limit, where the train can stop before the signaling equipment.

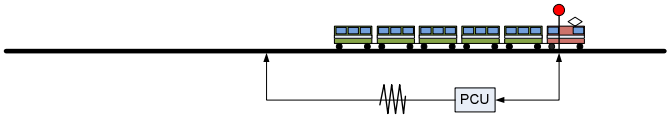

Figure 6.The train passed signaling equipment. At this moment the signal has changed to STOP. But this information was given train only using *PCU*.

The SHAMAP tool is used to calculate the reliability parameters of *PCU*. This tool allows the simulation of faults, what is one option how to test the equipment.

The reliability model will be created by top-down method. The estimated mean time between failures (MTBF) is known when the project is assigned. Estimated MTBF = 30 000 [h]. The block in the root level will be restricted by MTBF estimation. The system consists of five modules, according the description of *PCU*. These modules can be developed together. Each module contains minimally one PCB (Printed Circuit Boards). The calculation will be performed using the standard [7] by Stress Analysis Prediction method. Let's assume that each block in the highest level (root) is formed by just one module. If a module contains more boards, it will be reflected in the next level (it is also a series model). This is the case of the *LVZ* module, whose detailed model is in this case not known yet, so it is shown as the white rectangle only in the SHAMAP tool. See Figure 7.

The topmost (root, level 2) block represents the whole *PCU* system that is modeled. Its (*PCU* block) color (red) indicates that something is wrong. A closer look reveals that the original assumption of mean time between failures (MTBF) should be greater than 30 000 [h], but the SHAMAP calculated its value to 14 677 [h] only using current information.

The blue block called *S* represents an operation indicating that this is the series model at level 2 (the *PCU* block and *S* block are on the same level).

Green blocks (*PM*, *DM* and *LM*) are the specific coder modules, which the reliability models are known and enumerated for.

White blocks (*LVZ* and *ZP*) are also reliability models of the coder module, but these models are not known yet and therefore they are not calculated.

It is assumed that we have no information about them, so their failure rate λ and MTBF are not defined. The model takes into account only three elements. The other blocks associated with model represent only the information messages. Initial criterion (the MTBF in this case) breach can be found quickly using the color.

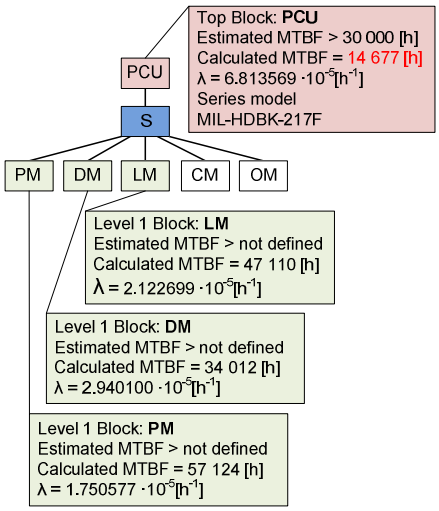

Figure 7.The process of predictive dependability analysis

The following Figure 8 shows a part of the level 1 – reliability model of power units of the module (*PM* block). The blocks in level 0 are of the different types of parts used in the module. For each type of parts the total failure rate is determined. In level 1 there is a simplified view of the series model again for the same kind of the parts. Each block contains not only the failure rate λ, but all parameters required to calculations.

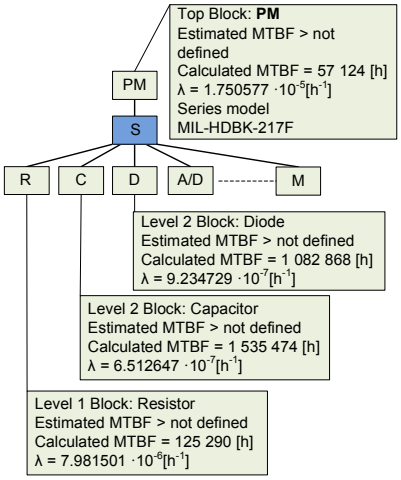

Figure 8.Screenshot from SHAMAP - Hierarchical model of the module *PM* with associated information

VI. Encapsulation of Design Phases of by UML

Descriptions of the systems using UML will allow easier model transfer to the databases (relational or object-oriented ones). The UML can easily describes not only the system, but also the processes of life and its development and mainly the use cases (e.g. service procedures, backup process, etc.) [13]. The model used for UML modelling is shown in Figure 9.

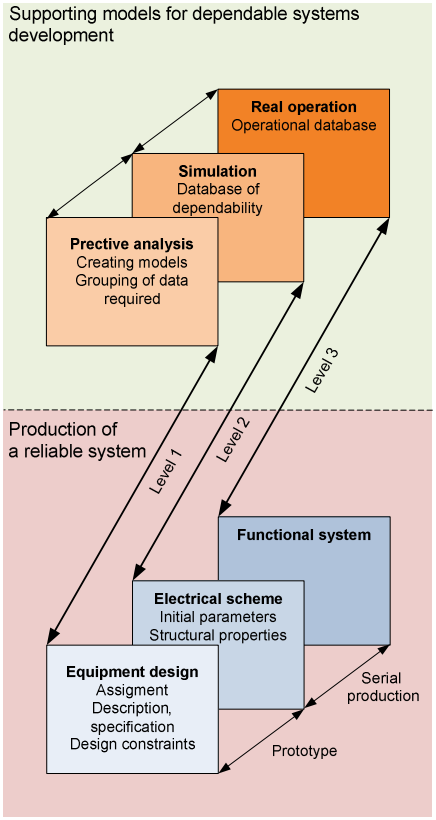

Figure 9.Reliable system development methodology roofed by hierarchical UML models

The phases of the real system development are described in Figure 9. The development of an equipment can be divided into three parts:

- Level 1 is: The equipment design or the project documentation consisting of the description and the specification of an equipment. Predictive analysis is used in specifications.
- Level 2 is: The electrical scheme. Here comes the first prototype development. The simulation is needed for the prototype production.
- Level 3 is the serial production of system functions. Functional system needs own operation feedback for ensure higher reliability. This feedback provides an operational database.

The supporting models are on the top of the dependable system development. Each level of a real design has its own support.

VII. Conclusions and Future works

The aim of the proposed paper is to create a methodology for the prediction analysis of dependability of the design of fail-safe systems. The method was especially intended for railway signalling equipment but it can be used in other mission-critical system design too. There are the following main directions of the methodology for fault-tolerant design:

- The design of an equipment with the guaranteed level of reliability and safety.
- The preparation of materials for reliability tests' acceleration based on simulations derived from the dependability parameters predictions.

It is necessary to create an object-oriented database, which will be more suitable than existing solutions using relational databases. The idea is not only the maintenance of information about the reliability parameters, but also the interaction between system devices. This will allow simulating the system at the design time. Thus, it is necessary also to extend the hierarchical model, which can be easily described by UML.

Extend SHAMAP tool allows to encapsulate different types of hierarchical models. Hierarchical models allow progressive calculation of the parameters for predictive analysis of reliability and safety according to methods FMEA/FMECA, MIL-HDBK-217F and EN CSN 50126. Hierarchical models also allow to hide details of the lower levels and to model the interaction between the individual blocks.

We would like to implement the analysis of event trees and stochastic Petri net in our future research. We found that the development tool needs AutoCAD or OrCAD and tools for simulation and calculations of reliability as SHAMAP. This will simplify the system design and will accelerate the predictive analysis.

Acknowledgment

This research has been in part supported by CTU grant SGS13/101/OHK3/1T/18.

References

[1] Z. Vintr – D. Valis – M. Vintr – J. Hlinka, *"Analysis of Reliability and Safety in Practice"*, CSJ Brno, 2009 (in Czech)

[2] N. Storey, *"Safety-Critical Computer Systems"*, Prentice Hall ptr, New Jersey, page 453, 1996

[3] EN 50126: Railway Applications – *"The specification and demonstration of Reliability, Availability, Maintainability and Safety (RAMS)"*, CENELEC, 2001

[4] IEC 812, Standard: *"Procedure for Failure Mode and Effects Analysis (FMEA)"*

[5] *MIL-STD-1629, Military Standards: "Procedures for Performing a Failure Mode, Effects and Criticality Analysis Notice 3", 1998*

[6] I. Koren - C.M. Krishna, "*Fault-Tolerant Systems*", 2007

[7] MIL-HDBK-217F *Military Handbook: "Reliability Prediction of Electronic Equipment Notice 2"*, 1995

[8] Presentation FIDES, https://cct.cnes.fr/system/files/cnes_cct/459-mce/public/07__FidesEurocalce.pdf, 2007

[9] S. Klapka, *"The Markov Modeling of the Safety"*, Dissertation Thesis, MFF UK Prague, pages 12-24, 2002

[10] M. Danhel, *"Hierarchical Block Diagrams in the Program SHAMAP*, Poster 2011", 15th International Student Conference on Electrical Engineering, Prague, Czech Republic, May 2011.

[11] M. Danhel - H. Kubatova , *"Methods of Hierarchical Reliability Block Diagrams in the program SHAMAP"*, DSD 2011, 14th Euromicro Conference on Digital System Design, pages 31-32, August – September 2011, Oulu, Finland.

[12] M. Danhel, *"Use of the MAPLE System for Calculate Reliability Parameters*", Diploma Thesis, CTU in Prague, 2011 (in Czech)

[13] OMG (February 2009). "OMG Unified Modeling Language (OMG UML), Superstructure Version 2.2", http://www.omg.org/spec/UML/2.2/Superstructure/PDF, 2009.