FACULTY
OF INFORMATION
TECHNOLOGY
CTU IN PRAGUE

Prediction and Analysis of Mission Critical Systems Dependability

by

Martin Daňhel

A dissertation thesis submitted to
the Faculty of Information Technology, Czech Technical University in Prague,
in partial fulfilment of the requirements for the degree of Doctor.

Dissertation degree study programme: Informatics
Department of Digital Design

Prague, January 2018

Supervisor:
Doc. Ing. Hana Kubátová, CSc.
Department of Digital Design
Faculty of Information Technology
Czech Technical University in Prague
Thákurova 9
160 00 Prague 6
Czech Republic

Co-Supervisor:
Ing. Radek Dobiáš, Ph.D., MBA
Department of Digital Design
Faculty of Information Technology
Czech Technical University in Prague
Thákurova 9
160 00 Prague 6
Czech Republic

Abstract and contributions

This dissertation thesis deals with dependability issues: methods for reliability, availability, and safety properties prediction to guarantee their requested level before proceeding to the manufacturing process or before the construction of the prototype of designed electronic equipment. My research has been realized in a close cooperation with the industry. The described methods and experimental results are based on solutions of real, practical, and up-to-day real-world problems and they are based on industrial standards. Therefore, one of the main contributions is declaring an insufficiency of currently used standards and presentation of new methods how to overcome these problems. The dissertation thesis precisely describes the mostly inconsistent area of dependability, used terminology, modelling methods, and historical developments in this area, up to present technology problems concerning types and probabilities of possible faults.

The dissertation thesis contribution and research results are divided into three areas:

1. Reliability prediction based on a new Heterogeneous Dependability Model (HDM), which can use Reliability Block Diagrams (RBD), serial, parallel, or combined models, Markov chains, etc., and where the calculation of dependability parameters can be realized at pre-defined accuracy.

2. The method and principles how to model both permanent and general transient faults and how to use such model to achieve more realistic dependability parameters computation. Space and temporal redundancy can be incorporated into the used dependability models.

3. The results are based on practical experiments described in two case studies. Mathematical methods to process a large amount of unordered and often unlimited data were used here. The first study deals with predictive analysis of a parameter failure rate of *Electronic Track Circuits* according to the standard MIL-HDBK-217 and according to the operation data. The second study deals with predictive analysis of a parameter failure rate of *Eurobalise* according to the same standard.

However, although all the examples and experiments are based on Czech railways and rail transportation and FPGA-based boards used in AŽD railways safety equipments, this dissertation thesis is not focused on any concrete field of electronic systems dependability. The presented methods can be used in different fields of all human activities, where a predefined dependability parameters level must be guaranteed. A proper and understandable dependability model has been designed with the aim to design a realizable system fulfilling predefined dependability constraints. The last important result is finding and denomination of other problems in this area to be solved. The partial foreshadow how to do it (dynamical dependability database, coloured hierarchical model, optional choice of fault distribution, multiple faults modelling) is presented.

Keywords:
availability, dependability, hierarchical block model, Markov chains, reliability model, reliability prediction, safety, permanent fault, transient fault.

Acknowledgements

First of all, I would like to express my gratitude to my dissertation thesis supervisor, Dr. Hana Kubátová. She has been a constant source of encouragement during my research and helped me with numerous problems and professional advancements.

I would also like to thank to Dr. Radek Dobiáš for giving me an opportunity to work with real safety-critical equipment. Without this valuable experience, my dissertation would never be possible.

Special thanks go to the staff of the Department of Digital Design, whose employees maintained a pleasant and flexible environment for my research. I would like to express special thanks to the department management for providing most of the funding for my research.

There are individuals who helped me most during my research namely Filip Štěpánek, Martin Kohlík, Jarda Borecký and Honza Řezníček for their valuable comments and proofreading.

Finally, my greatest thanks go to my family members & my little hippos, friends and all others for their infinite patience and care during my studies.

Chtěl bych také moc poděkovat svým rodičům, bratrům Honzovi a Jirkovi a i všem ostatním, kteří mě po celou dobu studia podporovali. Bez Vás bych to nezvládl.

This research has also been partially supported by the Ministry of Education, Youth, and Sport of the Czech Republic under research program MSM 6840770014, by the Czech Science Foundation as project No. 201/06/1039, and by CTU sudents's grants: SGS11/090/OHK3/1T/18, SGS12/094/OHK3/1T/18, SGS13/101/OHK3/1T/18, SGS14/105/OHK3/1T/18, SGS15/119/OHK3/1T/18, MOBILITY 7AMB14SK177 and GA16-05179S.

Contents

List of Figures

List of Tables

Abbreviations

Dependability parameters

α_C	Frequency of the critical part of a calculation
α_N	Frequency of the non-critical part of a calculation
λ	Failure rate
μ	Repaire rate
t_C	Duration of the critical part of a calculation...
t_N	Duration of the non-critical part of a calculation...
t	Time [hours]

Used Abbreviations

ABA-12	Balise from AŽD Praha, s.r.o.
AŽD	AŽD Praha, s.r.o. – Producer of safety signalling systems
CMOS	Complementary MetalOxideSemiconductor
CRC	Cyclic Redundancy Check
DoD	Department of Defence
ENIAC	Electronic Numerical Integrator And Computer
ETCS	European Train Control System
FMEA	Failure Mode and an Effect Analysis
FMECA	Failure Mode, Effect and Critically Analysis
FPGA	Field-Programmable Gate Array
FT	Fault Tolerant
FTA	Fault Tree Analysis
GSM	Global System for Mobile Communications
HDM	Heterogeneous Dependability Model
IEC	International Electrotechnical Commission
JAN	Joint Army-Navy Standards
JIS	Japanese Industrial Standards
KOA	Track Circuit Systems from AŽD Praha, s.r.o.
MIL-HDBK	Military Handbook
MTBF	Mean Time Between Failure
MTTF	Mean Time To Failure
MTTR	Mean Time To Repaire
PCB	Printed Circuit Board
RAM	Reliability Availability Maintainability
RAMS	Reliability Availability Maintainability Safety
RBD	Reliability Block Diagram
RIAC	Reliability Information Analysis Center
SHAMAP	SHARPE to Maple
SHARPE	Symbolic Hierarchical Automated Reliability and Performance Evaluator
SIL	Safety Integrity Level
TC	Technical Committee
TCS	Track Circuit System
TR	Technical Report
VLSI	Very Large Scale Integration

Chapter 1

Introduction

Requirements for the predefined level of reliability and safety parameters recently became an inseparable part of the technical requirements for all modern safety-critical systems. Development and design methods of any safety-critical system must guarantee strictly defined requirements for reliability and safety, in order to guarantee a high level of system availability. These requirements are usually defined according to specific needs of the designed system (mainly when the system is developed for some specific application or operation) and by a manufacturer (especially for systems intended for mass production). For systems where failures could lead to injury, loss of lives, damage to property or equipment, the requirements for reliability and safety are often determined by mandatory regulations (laws, notices, directives, standards, etc.) [1].

Such requirements should guarantee the requested level of reliability properties before proceeding to the manufacturing process or before the construction of the prototype. This is due to the fact that any change of the system structure or behaviour made in later stages of the development, is more expensive than the change that is realized sooner. Therefore, the requirements on reliability and safety of the system are defined and verified in early stages of the system development. In order to verify these requirements, the customer needs a proof, that the developed system will meet the requirements for the reliability and safety required in the system lifecycle. This proof is obligatory and in a case of a system failure, there is a possibility of high penalties both for the manufacturer and for the developer. It is accepted that the results are mainly used as proofs of prediction analyses of reliability and safety [1].

Every new technology always brings a number of new problems. Standards and Regulations that are valid for that time, might not have – and in most cases do not have – recommendations on how to take these new changes into account. Unfortunately, it will take some time before new procedures and processes that solve this problem are developed. For example, reducing the area of a chip brings a problem of transient faults, which are ever more frequent and that have not been considered before. This is due to the fact that the necessary technology allowing this reduced scale of integration (e.g., reducing the physical area of the chip) introduces other constraints in the form of higher liability to

faults produced by the hazardous environment. Another explanation for this phenomena is that higher density of electronic parts reduces the robustness to transient faults of the integrated circuit [2, 3]. For these reasons, critical systems are referred to processes and technologies that are already time-proven. On the other hand, this means that these technologies have been obsolete for some time now. However, it is the only solution in order to guarantee a reliable and dependable operation of the system.

1.1 My Motivation

My current doctoral study is closely related to my previous studies at the Faculty of Electrical Engineering at CTU in Prague. The problems solved in my Bachelor and Diploma theses have brought me to the area of dependability issues.

It all began in the winter semester of the academic year 2005. My current co-supervisor Dr. Radek Dobiáš asked me for a specific tool for accurate reliability calculations. Radek proposed models of high-reliability fault-tolerant systems. He used a tool SHARPE [4] for the reliability modeling of the mentioned systems by Markov chains. The program SHARPE uses numerical methods for dependability calculation. But these numerical methods add an error into the result. This error is small, but in the area of dependability computation, it can lead to inapplicable results. The SHARPE tool uses for its calculations a primitive data type **double**. However, numerical methods return results in an inappropriate format – only 8 valid digits and an exponent. If appropriate and real failure and repair rates were chosen, the computations can give inapplicable results: comparison of minimal changes (but which increases or decreases the reliability of the whole system) was impossible. Nevertheless, Radek needed these dependability properties calculations with more precise results.

My Bachelor thesis[A.17] solved the problem mentioned above, because all calculations of reliability parameters from SHARPE were calculated in another special mathematical system – Maple. As an added outcome I have allowed some Markov models to be computed in a symbolic form. The symbolic calculation is more demanding for computing time and performance, but it ensures an accurate result[1]. This provided a much better solution than originally expected. After the defence of my Bachelor thesis I wanted to continue in this theme. Radek asked me to create a new and better tool than the program SHARPE. This opportunity was a big challenge because this tool has been the only one of its kind known at that time.

Therefore, I have conducted and defend my Master thesis [A.18] on the same topic. My goal was to create a tool similar to SHARPE, but with all calculations directly solved in Maple [5]. This mathematical system can solve some differential equations in a symbolic form – without loss of accuracy. Unfortunately, not all differential equations can be possible to solve in a symbolic form. However, my improved SHARPE is able to use not only Markov chains models. I have created a tool with this new approach and I termed it SHAMAP.

[1]More information about Maple and its symbolic form of calculation can be found in this book **Mathematics for Engineers and Scientists** from **Alan Jeffrey**, 2014, in page 916

It can work with Reliability Block Diagrams (RBD) [6, 7, 8], Fault Trees [6, 7, 9, 10], Petri nets [6, 7, 11], etc. see in Chapter 2. Perhaps its main advantage has been the possibility to join two or more models into one – in other words, SHARPE can work hierarchically. I wanted to keep this advantageous property. It was necessary to invent some internal form. I designed a general model, which I called the *Hierarchical Reliability Block Diagram*. A more accurate name – *Heterogeneous Dependability Model* (HDM) – will be used in this thesis.

When I continued my research as a Ph.D. student, I have published a more detailed description of this model and examples of its application in my papers [A.1, A.8, A.13]. Each of them brought some improvements to the current model. Since then, I have been using this model regularly for predictive reliability analyzes, similarly to these [A.14, A.15]. This model will be presented in this thesis.

1.2 Problem Statement

Up to my best knowledge, the basic problem is a view on the dependability itself. The definition itself is not uniform. At the beginning of the 1990's, there was a general belief that the problem of reliability of systems is resolved, but there are still many unclear or imprecise problems especially as concerns a general electronic system:

- How to make a decomposition on a suitable dependability model?
  The decomposition is necessary due to increasing complexity of every model. The question is: how to achieve a proper level of detail and the possibility to precisely compute dependability characteristics at the same time?

- Where to take parameters from and how to calculate this model?
  Are the parameters values constant, or is it necessary to take into account, e.g., aging and how?

- How to verify the correctness of the result?
  Do we obtain the same results under the same input conditions and by using the same methods? In section 4 you can see that this is a real problem and that the parameters may be different by orders of magnitude.

- How to interpret the result and how to use it?
  There is only one possibility: to make a lot of experiments and compare their results with reality. The question is, how to make a realistic prediction?

- How to compare two similar systems – the problem is that if we have a list of parts, an electronic schema, and a detailed description of both systems, the internal parts of the system still may not be visible, and this can significantly influence the final decision.

- Is it possible to use current standards mostly used in industry?
  Although the development of the technology of electronic systems has done a great leap forward, the original reliability models are still used in the predictive analysis of reliability. Fault models for individual electronic parts are very sophisticated, but the reliability model for the whole system is mostly serial only. Some methodologies do not take into account the architecture of the system, such as redundancy, backup, etc., at all. The big problem is that each reliability methodology provides completely different estimates with the same input assumptions (according to published experiments). Sometimes, this difference is really too big. However, most of the methodologies are based on the same foundations.

- Is it necessary to include transient faults into dependability models and computations somehow?
  This is a real nowadays problem, because transient faults are very difficult to predict and to model. The effect of transient faults does not necessarily mean an equipment failure, but only a failure of calculation or its part. The system may evaluate the incorrect result as a fault and due to this fact, for example:

  - a recovery event will be triggered, which may result in suspended unavailable services,
  - the system will turn off a faulty module and switch to a backup module,
  - it will be necessary to call a maintenance.

  Unfortunately, the repairman will not detect anything; only an error in a calculation and a fault record will exist.

This thesis seeks answers to these questions. It is based on practical experiments, and the proposed methods try to cover the most problematic aspects in the area of dependability modelling and computations of dependability parameters. An exhaustive discussion about the usability of industrial standards is given (see Chapter 2). The Heterogeneous Dependability Model is proposed in Chapter 3. The conclusions, that not only constant parameters values and not only exponential probability distributions are suitable to use, are stated and experimentally proven (see Chapter 4). Finally the way how to model and include computations of transient faults into dependability parameters is proposed (see Chapter 5). Nevertheless, a lot of unsolved or not completely finished areas still remain; there is a great space for future work (see Conclusions 6).

1.3 Progress of my Research

Research in this area must be realized in a close cooperation with the industry, as real-world experience and particular data on the function of the system safety are needed.

This work is based on data and materials mainly from the AŽD Praha, s.r.o. company[2] (AŽD). Most of these data and materials are not publicly accessible. I am going to designate these materials with the generic name of the **original data**.

My doctoral study has begun on February 2011. I worked at the AŽD company during my studies, where I gained invaluable experience. My work has been directly related to my research because I have dealt with predictive dependability analysis of the railway interlocking signalling equipment. During my studies I was able to personally participate in two important and key projects. The first one was related to a predictive dependability analysis of Track circuit systems for Prague's Metro (KOA), see in [A.14]. This experience is described in details as a case study in Chapter 4. The second project was related to predictive dependability analysis of Eurobalise[3] (ABA-12) for railway tracks of European countries, see in [A.15] and in Chapter 4. Both projects are led as comprehensive research reports and they are protected business secrets. For that reason, it is not possible to provide an internal documentation and specific values of results.

The Figure 1.1 shows chronological evaluation of my research and practice from Bachelor and Master theses [A.17, A.18] (*step 0*) to this thesis (*step 6*). I have published these results in individual steps:

1. I published articles on the topic *Hierarchical reliability block diagram* [A.8, A.11, A.13]. It is an incremental contribution to my Master thesis [A.18]. In this thesis is *Hierarchical Reliability Block Diagram* renamed to *Heterogeneous Dependability Model*.

2. I defended a Ph.D. Thesis Report on the topic *Reliability of digital systems* [A.7]. Thanks to my work at AŽD, I started to study reliability standards. The results of my efforts were published in papers on the topic *Predictive analysis of mission critical systems dependability*, [A.1, A.12]. The first paper was published at the *Euromicro Conference on Digital System Design* in Spain in 2013.

3. I led a project in cooperation between my faculty and AŽD – Predictive Dependability Analysis for track circuits. The results of this analysis are described in detail in section 4. Based on this analysis, I have published these articles: [A.9, A.14, A.20].

4. After a successful defense of the summary research report of the predictive dependability analysis of KOA [A.14], I have led an another project using the same meth-

[2]The AŽD Praha company is a significant and all-Czech producer and supplier of signalling, telecommunication, information, and automation technologies. It is mainly focused on the rail and road transport field including telematics and other technologies. More information is available at: http://www.azd.cz/en.

[3]An Eurobalise is a track part of *European Track Control System*. The Eurobalise is a passive or active antenna device mounted on rail sleepers. Mostly it transmits information to the driving vehicle. It can be arranged in groups to transfer information. There are Fixed and Transparent Data Balises that are sending changing information to the trains, e.g., signal indications. Fixed Balises contain particular information, like gradients and speed restrictions [12].

odology applied to ABA-12. The results of this analysis are described in detail in section 4.

Besides of this, I worked on the possibility to model transient faults using spatial redundancy. I have published my proposed solutions of this topic in these papers [A.2, A.10, A.16].

5. The project ABA-12 continued in year 2017 as the next new version of the Balise equipment. I have finished the project with this publication [A.15]. In the *Journal of Microprocessors and Microsystems – Embedded Hardware Design.* I published an extended paper on the topic *The effect of the transient faults in dependability prediction* [A.3]. The extended version is based on the article [A.2] of the same name published at the *Euromicro Conference on Digital System Design* in Cyprus in 2016.

   Thanks to original data from project KOA, I have published an article on the topic *Predicting the Life Expectancy of Railway Fail-safe Signaling System Using Dynamic Models with Censoring* [A.5] at the *International Conference on Software Quality, Reliability and Security* in Czech Republic in 2017.

   Moreover, I published these articles about predictive analysis of dependability and history of reliability computation [A.4, A.19].

6. Currently, I am working together with my colleagues on the:

   - possibility of reliability calculations using non-constant failure rates[4] of electronic systems,
   - design of the *Hierarchical Colored Blocks Dependability Model*,
   - improvement of my proposed *Database of Dependability.*

   The final step is a defense of my dissertation thesis (for now).

1.4 Structure of the Dissertation Thesis

The thesis is organized into six chapters and three appendixes as follows:

1. *Introduction*: describes my motivation and my efforts together with my goals. There is also a list of questions to solve in the area of dependability.

2. *Background and State-of-the-Art*: a point of view into a history of electronic systems dependability is briefly described. Basic definitions and terms are introduced here. The related work and previous first results are presented.

[4] There are not always unified terminology used, failure rate should be probably named *fault rate.* In [13] and in other classical publications[14, 15, 16] *failure rate* is used, and instantaneous failure rates were taken into account only. But to emphasize that failure rate could not be classical bath-curve only, *hazard rate* term is preferred, e.g. in [17], see Section 2.2

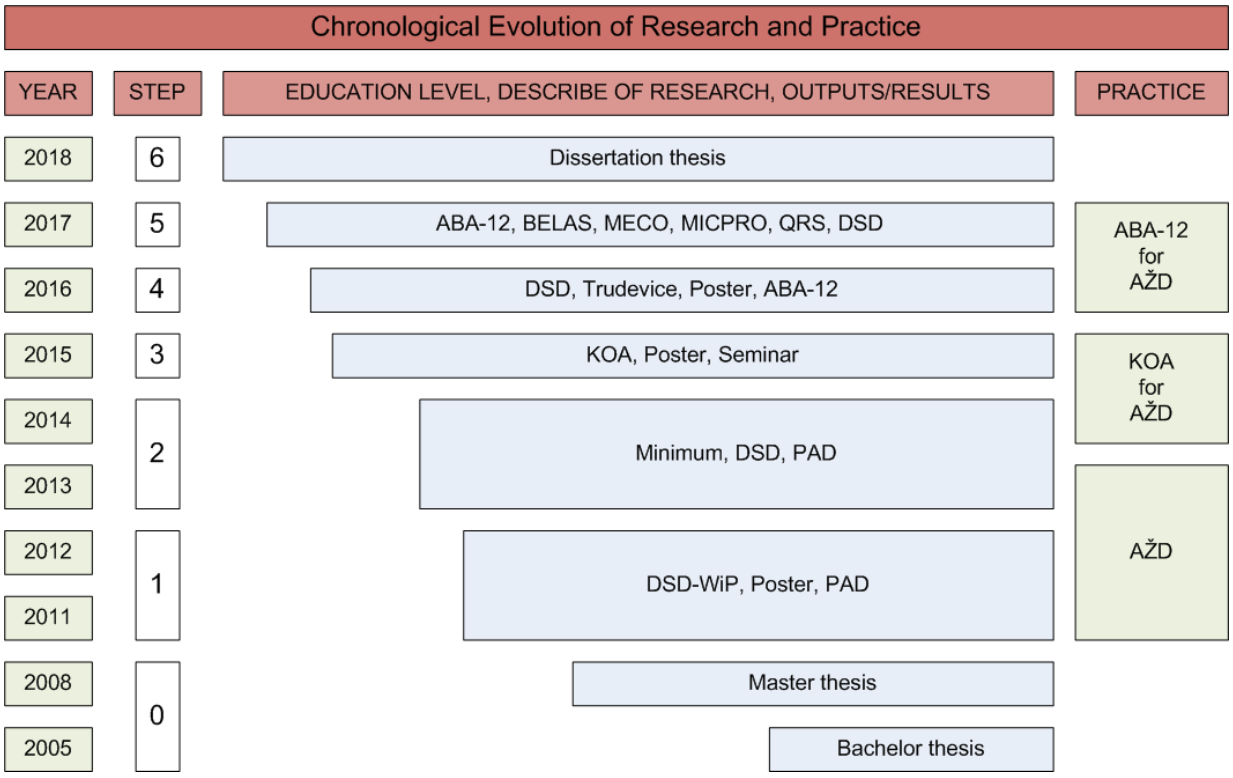

Figure 1.1: The figure shows the progress of my research. The meanings of the individual abbreviations and terms are given in Tab. 1.1.

3. *Heterogeneous Dependability Model*: shows a new approach to modeling the reliability using a Heterogeneous Dependability Model. Further, this chapter summarises the results from papers [A.1, A.8, A.11, A.12, A.13]. The Appendix. A is attached to this chapter.

4. *Case Studies*: describes two case studies *Electronic Track Circuit* [A.5, A.9, A.14] and *Eurobalise* [A.15]. The aim of both studies was predictive analysis of reliability. The problems arising from two different industrial case studies are described. The Appendix B is attached to this chapter.

5. *Modelling of Effect of General Transient Faults*: describes the addition an influence of transient faults into the dependability prediction using the Markov chain model [A.2, A.3, A.6, A.10, A.16]. Transient faults are considered for redundant TMR systems only. The Appendix C is attached to this chapter.

6. *Conclusion*: summarizes the results of my research and experiments and suggests possible topics for further research.

Abbreviation	Description
BELAS	Summer School on Design, Test and Reliability
DSD	Euromicro Conference on Digital System Design
DSD-WiP	Euromicro Conference on Digital System Design, Work in Progress
MECO	Workshop on Embedded and Cyber-Physical Systems
MICPRO	Journal of Microprocessors and Microsystems – Embedded Hardware Design
Minimum	Ph.D. Thesis Report
PAD	Počítačové Architektury a Diagnostika – Students Workshop
Poster	International Student Conference on Electrical Engineering
QRS	International Conference on Software Quality, Reliability and Security
Seminar	Czechoslovak Student Workshop
Trudevice	Workshop on Trustworthy Manufacturing and Utilization of Secure Devices

Table 1.1: The meaning of individual abbreviations used in Fig. 1.1 is described in this table.

A. *Predictive Analysis of Mission Critical Systems Dependability*: contains the paper [A.1]. This paper was published at the *Euromicro Conference on Digital System Design* in Spain in 2013.

B. *Predicting the Life Expectancy of Railway Fail-safe Signaling System Using Dynamic Models with Censoring*: contains the paper [A.5]. This article was published at the *International Conference on Software Quality, Reliability and Security* in Czech Republic in 2017.

C. *The Effect of the Transient Faults in Dependability Prediction*: contains the article [A.3]. This article was published in the *Journal of Microprocessors and Microsystems – Embedded Hardware Design* in 2017.

Chapter 2

Background and State-of-the-Art

The basic terms, definitions and methods from the field of dependability are described in this chapter. Terminology and definitions are considerably diverse. The problems with their understanding occur often. This chapter offers a look back when the first requirements for the reliability of electronic systems began to be formed. The paper [A.4] described problems with terminology in this field.

2.1 History of Dependability Approaches

The needs for dependability are not new. As soon as humans began to manufacture weapons and tools with stone, wood and bone, they quickly understood the need to produce solid and durable objects. The financial and commercial needs appeared later on [7].

This notion of reliability was structured into a scientific discipline even later according to the historic scale. The current explosion of digital electronics and its application to computing have extended and amplified studies on reliability [7].

Origin of the words dependability and reliability

The term **dependability** has the origin derived from the word 'dependable'. The first using of this word dates back to 1725 – 1735 [18]. However, another source states that the term dependability was first used in the *Oxford English Dictionary* in 1901 [19]. On the other hand, the term **reliability** has its first using dated back to 1816 [20].

The term **reliability** is discussed by both scientific and engineering publications [21]. For the purpose of this thesis the term **reliability** needs to be differentiated from the term **dependability**. The difference is described as follows:

- Reliability is a probability of a system functioning correctly over a given period of time under a given set of operating conditions.

- Dependability has not a specific value. It is a complex property of system. This concept consists of several parameters including the reliability.

Summary

Both definitions have evolved over time into the today's form. Put simply, if it is a statistical calculation and the result is a specific numerical value, reliability is meant. I the case of an overall assessment of the system, it means dependability. Previously, the term **reliability** was used for both variants. Therefore, some former sources use misleading terminology. These two words also cause problems when translating, for example, into the Czech language. This situation is explained in this chapter.

The thirties...

The mathematical theory of dependability has begun to form since the early 1930s. One of the first areas of reliability to be approached with any mathematical sophistication was the area of machine maintenance [22, 23]. In 1939, the Swedish Professor Waloddi Weibull described the distribution (see Section 2.3), later named after him, as a distribution suitable for the strength of materials and for the life-cycle [24].

The forties...

During the 1940's, the major statistical effort on reliability problems was in the area of quality control. N. R. Campbell described replacement problems using renewal theory techniques in 1941 [22]. The first attempt to solve reliability issues for electronic circuits and systems began during the Second World War, when the first "reliability" model was constructed by German Rocket Scientist Wernher von Braun and his team, in course of the V1 and V2 rocket construction. Wernher von Braun assumed that the rocket is as reliable as its least reliable part. This idea was taken from mechanical reliability (the weakest link in a chain) [25]. Eric Pieruschka, a German mathematician working with Wernher von Braun, was able to help him with his reliability troubles. Pieruschka pointed out to Wernher von Braun that his reliability model was incorrect. Pieruschka showed that the reliability of the rocket would be equal to the product of the reliability of its components, which was the first documented modern predictive reliability model. This result formed the basis for what later became known as Lusser's law [25]. Thanks to this, Robert Lusser was later regarded as the "father of reliability". He was the first, who described a *serial reliability model*.

The famous computer ENIAC of the 40s had 18 800 vacuum tubes, 6 000 switches, 10 thousand of passive components and offered an average life-time of half an hour [7].

The fifties...

In the 1950s, at the starting point of computer systems, the first logical electronic components used (relays, then vacuum tubes, and then elementary transistors) had a very short average life-time [7]. Simultaneously with the mathematical theory of reliability, the industry was evolving in a direction oriented towards the technology of electrotechnical

parts manufacturing. Discovery of failure mechanisms and degradation processes, relevant analytical tools, and fault diagnosis procedures have resulted in so-called reliability physics or physics failures. Specialization has advanced so far, that separate conferences are held for this area of reliability [24].
Then, new standards and quality controls of electronic parts manufacturing originated in Japan and America after the Second World War (JAN, JIS, MIL) [26].

The sixtes...

In 1961, the first edition of the MIL-HDBK-217 Handbook on analysis of the stress of electronic equipment reliability was published in the United States, which included models for calculating component failure rates. The handbook has become a world standard [14]. The reliability of systems had developed into modelling of redundancy, Bayesian statistics and Markov processes [24].
In 1965, the Technical Committee by the International Electrotechnical Commission was formed, as *TC 56 – Reliability and Maintainability* (TC 56 cannot be called the RAM Committee) [27]. This committee develops and maintains international standards in the field of dependability. By the way, the IEC founded 1906 is the oldest International Standardization organisation.
In this decade, the first books about a classical dependability theory were published. They were *Mathematical theory of reliability* [23], and *Mathematical methods of reliability theory* [28].

The seventies...

Thanks to the development of space flights and nuclear power plants, control computers with very high level of dependability were developed. This dependability was achieved using a high level of redundancy. Gradually, the first *Fault Tolerant systems* began to emerge. Further, *soft errors* in dynamic memories [3] were observed and described. These errors can be caused by the effect of cosmic rays and they can have a negative impact on computer memories [29].
The decreasing price of integrated circuits and processor units led to the fact that the principles of fault tolerant systems have also been applied in military and later in civilian systems [24]. The first self-diagnosis systems were developed. These systems were designed to *locate faults* [30].
During this time, the use of FMEA – *Failure Mode and Effect Analysis* and related techniques spread to other industries. Primarily the automotive industry began to use FMEA [31].

The eighties...

In 1982 at the Symposium on Fault Tolerant Computing in California, a term "dependability" was established to encapsulate and unify all these concepts. Mathematical theory of reliability was extended to digital systems, and a multilevel approach was introduced. In the area of technical resources, various systems were studied with redundancy, the

theory of *software reliability* was developed. In contrast to the hardware reliability, the software reliability was only at its beginning. Definitions of concepts and taxonomy were create [13, 32]. Further, the first version of MIL-HDBK-338 – *Electronic Reliability Design Handbook* [33] was published.
For the most of complex systems with repair, simplification of their reliability models is necessary. Markov models are often used [9]. The Improved Fault Tree is again applied [10]. Thanks to the expansion of graph theory, computer nets, and programming languages, it can possible to solve extensive tasks of dependability using computers [24].

The nineties...

The 1990s are marked by the development and improvement used methods and procedures. The reliability of software resources, fuzzy reliability models, and qualitative reliability models were studied. Effective algorithms for dealing with typical tasks were sought. A number of user-oriented professional programs and software packages for system reliability analysis on personal computers were developed. The impact of automation on safety was studied [24].
During the nineties, questions regarding the correctness of the MTBF – *Mean Time To Failure* parameter emerged; especially when this parameter was estimated according to the classical standards [34]. The development of the very known (maybe legendary) military standard MIL-HDBK-217 [14] was terminated by DoD of U.S., for the reason of unreliability of the predicted results. Nevertheless, this standard is still the most used to date. Why? Because of its simplicity and, above all, the certainty of a pessimistic estimate.

Millennium...

Standards and technical reports began to emerge and they included more complex models. For example, the first version of the standard FIDES:2005 (otherwise labeled UTE C 80 811) can also take the reliability of production processes into account [15]. Furthermore, IEC TR 62380:2004, which can take into account the breakdown of failures for different types of components [16], was proposed. There are a variety of software tools on the market that contain databases of failures and countless different reliability methodologies, for example Relex [35] or RIAC [36].

Present day...

There are ongoing efforts to modernize the standard MIL-HDBK-217. The new work version of this standard was published and released as *revision G* for public review in 2010, but it was quickly retracted due to pending internal discussions in the DoD about the reliability policy [37].

The Reliability Information Analysis Center (RIAC) supports it now under the name RIAC-HDBK-217 Plus, or 217Plus^{TM}:2015 respectively. This methodology can predict software reliability [36].

2.2 Dependability Basics, Terms & Definitions

The **dependability parameters** and their definitions are introduced in this section. These definitions of some parameters have changed over time. It is generally believed that there are no unified *steady* names, definitions, and meanings in the field of dependability. The problem is often with the pairs of the words **dependability** and **reliability** [24, 38].

Many definitions on dependability from relevant literature will be used in the following text. However, first it is necessary to define the general used terms.

- **System** – A set of equipment capable of making or supporting an operational role. A complete system includes all equipment, hardware, software, services and personnel necessary for its operation so that it is sufficient to itself in its usage environment.
  For example a track circuit, a train etc.

- **Subsystem** – A set of equipment capable of performing an operational function of a system. The subsystem is a major subdivision of the system. The subsystem itself is often called a system.
  For example a diagnosis and checker in track circuit, an Eurobalise etc.

- **Equipment** – A term denoting a group of items capable of performing a complete function.
  For example computing module in the track circuit.

- **Subassembly (module)** – A term denoting an item or an assembled group of items capable of performing a function of the equipment. This definition also includes the printed circuit board – PCB.

- **Electronic component (part)** – A term denoting an element that will be assembled with other elements in order to perform one or several electronic functions. In this work, an item refers to an elementary entity, not broken down, for which the reliability can be studied.
  For example transistor, resistor, capacitor etc.

- **Product** – this work refers to the assembled entity for which reliability is being studied. Usually equipment.

Some definitions from the list above overlap. This is necessary for a detailed description and analysis of very complex systems as, for example, track circuits.

This term covers considerations of reliability, availability, maintainability, safety, and other important issues in safety critical systems.
Dependability is a property of a system that justifies placing ones reliance on it.

2.2.1 Dependability Basics

There are at least two points of view on the dependability definition:

- dependability as an attribute of systems,
- dependability as a science.

Due to the role and responsibilities attached to them, computing systems have to be characterized by their capacity to deliver services for which they have been designed. They should not fail. This ability is expressed by attributes defining the *dependability* of these systems. To obtain proper results, predictive means throughout to the whole development cycle must be used. These methods, techniques and tools will be regrouped in a scientific domain also known as *dependability*.

A measure of the degree of operability and capability of performing required function of an item at any (random) time during a specified mission profile, gives to the item availability at mission start (item state during a mission includes the combined effects of the mission-related system R&M parameters but excludes non-mission time; see availability) [33].

The term dependability encapsulates the following probabilistic concepts (also called RAMS parameters [39]):

- **Reliability** is the probability of a component or a system functioning correctly over a given period of time under given set of operating conditions [6].
- **Availability** of a system is the probability that the system will be functioning correctly at given time [6].
- **Maintainability** is the ability of a system to be maintained [6].
- **Safety** is a property of system that will not endanger human life or the environment [6].

The other mentioned source [7] introduces that the term dependability includes other parameters such as **testability** and **security**. On the other hand, another source [32] lists even other parameters as **integrity** and **security** listed separately. From the listed sources it follows that **dependability** is not always a totally uniform concept that it is defined by concrete parameters. In the same way, definitions of some parameters may vary. Because this work focuses only on RAMS parameters, especially on reliability, the other parameters are not listed. The terms RAMS are closely explained including their mathematical approaches in the following text of this chapter.

Electronic reliability design handbook MIL-HDBK-338B [33] introduces the basic dependability terms clearly and comprehensibly. Therefore, Sections 2.2.2 – 2.2.3, and 2.3 are almost literally taken from this handbook.

2.2.2 Reliability

Reliability is the ability of a system or component to perform its required functions under stated conditions for a specified period of time [40].

Reliability is defined in terms of probability, probabilistic parameters such as random variables, density functions, and distribution functions are utilized in the development of reliability theory. Reliability studies are concerned with both discrete and continuous random variables. An example of a discrete variable is the number of failures in a given interval of time. Examples of continuous random variables are the time from system installation to failure and the time between successive system failures.

The cumulative (failure) distribution function $F(t)$ is defined as the probability in a random trial that the random variable is not greater than t, or

$$F(t) = \int_{-\infty}^{t} f(t)\,dt$$

where $f(t)$ is the probability density function of the random variable, time to failure. $F(t)$ is termed the "unreliability function" when speaking of failure. It can be thought of as representing the probability of failure prior to some time t. If the random variable is discrete, the integral is replaced by a summation. Since $F(t)$ is zero until $t = 0$, the integration can be from zero to t.

The reliability function, $R(t)$, or the probability of a device not failing prior to some time t, is given by

$$R(t) = 1 - F(t) = \int_{t}^{\infty} f(t)\,dt$$

The rate at which failures occur in the interval $t1$ to $t2$, the failure rate, $\lambda(t)$, is defined as the ratio of probability that failure occurs in the interval, given that it has not occurred prior to $t1$, the start of the interval, divided by the interval length. Thus,

$$\lambda(t) = \frac{R(t) - R(t + \Delta t)}{\Delta t\, R(t)}$$

where $t = t1$ and $t2 = t + \Delta t$. The hazard rate, $h(t)$, or instantaneous failure rate, is defined as the limit of the failure rate as the interval length approaches zero, or

$$h(t) = \frac{f(t)}{R(t)}$$

Only constant hazard rates are used in models presented in this thesis, thus a hazard rate will be denoted as λ.

Mean time to failure is nothing more than the expected value of time to failure and is derived from basic statistical theory as follows:

$$MTTF = \int_{0}^{\infty} t\, f(t)\,dt = \int_{0}^{\infty} R(t)\,dt$$

2.2.3 Availability

Availability on the other hand, is the degree to which a system or component is operational and accessible when required for use [40].

The concept of availability was originally developed for repairable systems that are required to operate continuously, and are at any random point in time either operating or "down" because of failure and are being worked upon so as to restore their operation in minimum time. In this original concept a system is considered to be in only two possible states – operating or in repair – and availability is defined as the probability that a system is operating at any random point in time t, when subject to a sequence of "up" and "down" cycles which constitute an alternating renewal process. In other words, availability is a combination of reliability and maintainability parameters.

System availability can be defined in the following ways:

- *Instantaneous Availability* $A(t)$ – Probability that a system will be available for use at any random time t after the start of operation.

- *Mission Availability* $A_m(t_2 - t_1)$ – The proportion of time in an interval $(t_2 - t_1)$, during a mission, when a system is available for use, or

$$A_m(t_2 - t_1) = \frac{1}{t_2 - t_1} \int_{t_1}^{t_2} A(t)\, dt$$

  This is also called average availability A_{AV}.

- *Steady State of Availability* $A_S(t)$ – Probability a system will be available for use at a point in time t after the start of system operation as t becomes very large, or as $t \to \infty$, or

$$A_S = \lim_{t \to \infty} A(t)$$

2.2.4 Maintainability

The reliability express as long as possible function without a failure. The maintainability emphasises that a system can be repaired as quickly as possible. The combination of high reliability and high maintainability leads to higher system availability (see Section 2.2.3).

Maintainability is a measure, how easily and rapidly a system or equipment can be restored to operational status following a failure. It depends on parameters given by the function of the equipment design and installation, personnel availability in the required skill levels, adequacy of maintenance procedures and test equipment, and the physical environment under which maintenance is performed.

Both reliability and maintainability parameters are also probabilistic and can be analyzed by the use of continuous and discrete random variables, probabilistic parameters, and statistical distributions. An example of a discrete maintainability parameter is the number of maintenance actions completed in some time t, whereas an example of a continuous maintainability parameter is the time to complete a maintenance action.

2.2.5 Safety

Definitions of safety vary considerably. Mentioned definition of the safety is true, but it says nothing about the measurable level of the safety. From this reason following definitions is also used (these definitions are taken over [6, 39, 41, 42]):

- Safety is the probability that on the system output will not be an undetected error [42].

  From the point of view of an attribute of a system: safety is the probability that the system will not have failures belonging to unacceptable seriousness classes, between the initial time and the given time t.

- Safety is the state of being "safe", the condition of being protected against physical, social, spiritual, financial, political, emotional, occupational, psychological, educational or other types or consequences of failure, damage, error, accidents, harm or any other event which could be considered non-desirable [41]. Safety can also be defined to be the control of recognized hazards to achieve an acceptable level of risk. This can take the form of being protected from the event or from exposure to something that causes health or economical losses. It can include protection of people or of possessions.

A target level of risk reduction in safety-critical systems (e.g. railway station signaling and interlocking equipment, automotive systems, etc.) is specified by SIL [39].

The value of SIL is calculated using the hazard rate of the system [39] and Tab. 2.1. E.g. the system classified as SI 4 is the only one safe enough to be used in the most critical applications, where hundreds or thousands of lives may be endangered by its failure.

Failure rate $\lambda\,[\mathbf{h^{-1}}]$	**SIL** $[-]$
$10^{-5} - 10^{-6}$	1
$10^{-6} - 10^{-7}$	2
$10^{-7} - 10^{-8}$	3
$10^{-8} - 10^{-9}$	4

Table 2.1: Table describes the Safety Integrity Level (taken from [39]).

2.2.6 Related Terms and Definitions

Maintenance

Maintainability closely related to maintenance – all actions necessary for retaining an item in or restoring it to a specified condition.

Mission Profile
A time-phased description of the events and environments experienced by an item during a given mission. The description includes the criteria for mission success and critical failures.

Mission Reliability
The measure of the ability of an item to perform its required function for the duration of a specified mission profile. Mission reliability defines the probability that the system will not fail to complete the mission, considering all possible redundant modes of operation.

Mission Time
That element of up time required to perform a stated mission profile.

Mean Time Between Failure – MTBF
A basic measure of reliability for repairable items. The mean number of life units during which all parts of the item perform within their specified limits, during a particular measurement interval under stated conditions. **Mean Time Between Failure** is a reliability term used loosely throughout many industries and has become widely abused in some. Over the years the original meaning of this term has been altered which has led to confusion and cynicism.

Mean Time To Failure – MTTF
A basic measure of reliability for non-repairable items. The total number of life units of an item population divided by the number of failures within that population, during a particular measurement interval under stated conditions.

Mean Time To Repair – MTTR
A basic measure of maintainability. The sum of corrective maintenance times at any specific level of repair, divided by the total number of failures within an item repaired at that level, during a particular interval under stated conditions.

Relationship Between Dependability Parameters The relationship between mentioned dependability parameters is shown in Fig. 2.1

2.3 Dependability Oriented Continuous Probability Distributions

Electronic reliability design handbook MIL-HDBK-338B [33] introduces several commonly used continuous distributions (some descriptions of distributions are taken from [41]):

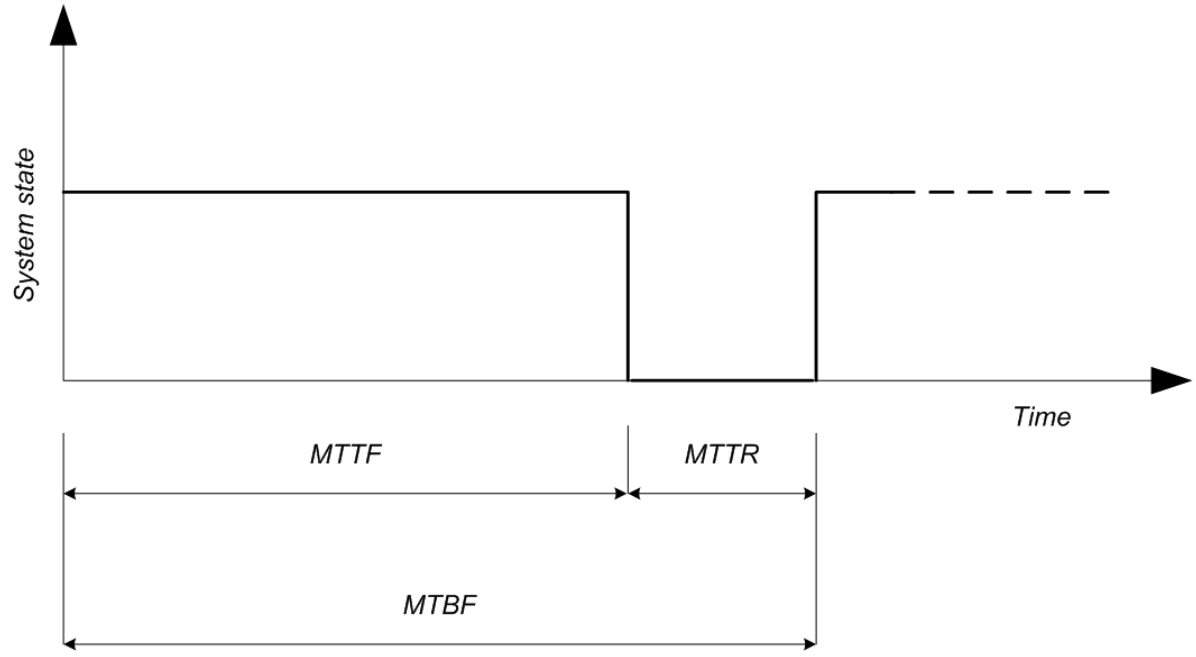

Figure 2.1: Relationship Between Dependability Parameters MTBF = MTTF + MTTR

- *Exponential* – This is probably the most important distribution in reliability work and is used almost exclusively for reliability prediction of electronic equipment [14]. It describes the situation wherein the hazard rate is constant (see Fig. 2.3). The main advantages:
  - A single, easily estimated parameter (λ).
  - Has fairly wide applicability.
  - Is additive – that is, the sum of a number of independent exponentially distributed variables is exponentially distributed.
- *Gamma* – The gamma distribution is used in reliability analysis for cases where partial failures can exist, i.e. when a given number of partial failures must occur before an item fails (e.g. redundant systems) or the time to second failure when the time to failure is exponentially distributed.
- *Weibull* – The Weibull distribution is particularly useful in reliability work since it is a general distribution which, by adjustment of the distribution parameters, can be made to model a wide range of life distribution characteristics of different classes of engineered items.
- *Normal (Gaussian)* – There are two principal applications of the normal distribution to reliability. One application deals with the analysis of items which exhibit failure due to wear, such as mechanical devices. Another application is in the analysis of

manufactured items and their ability to meet specifications. No two parts made to the same specification are exactly alike. The variability of parts leads to a variability in systems composed of those parts. The design must take this part variability into account, otherwise the system may not meet the specification requirement due to the combined effect of part variability. Another aspect of this application is in quality control procedures.

- *Lognormal* – The lognormal distribution is the distribution of a random variable whose natural logarithm is distributed normally; in other words, it is the normal distribution with $\ln(t)$ as the variate. This is the most commonly used distribution in maintainability analysis. It applies to most maintenance tasks and repair actions comprised of several subsidiary tasks of unequal frequency and time duration.

Table shown in Fig. 2.2 taken from [33] shows the shapes of failure density, reliability and failure (hazard) rate functions for these distributions.

2.4 Mission, Malfunction, Faults, Errors and System Failures

Some parts of this section are taken from Basic Concepts and Taxonomy of Dependable and Secure Computing [13] or Dependability: Basic Concepts and Terminology [32]. The main definitions are taken from [6] and Fault Tolerant Computing in Industrial Automation [43].

Computers, electronic devices, industrial plants, etc. are complex systems that depend on the correct function of a large number of elements to work properly. We will speak of an "element" when considering a part of a system which we do not want to detail further, although it may well consist itself of sub-elements. When we do not want to detail whether we consider a system or an element, we speak of an item. An item is required to provide a certain service under given conditions for a stated period of time, that is, to fulfill a specific mission, defined by a mission specification.

Example:
The mission of a car can be defined as: "transport up to 5 persons over roads at a maximum speed of at least 130 km/h while consuming less than 3 l/km over a useful lifetime of at least 20 years".

A failure occurs when car is not capable of performing its mission – regardless how significant the deviation from the specification is. It does not need to be an accident.

Example:
It is not a failure of the car if it can not transport people over railroads, but if the car consumes more than the amount specified, this can be considered a failure with respect to

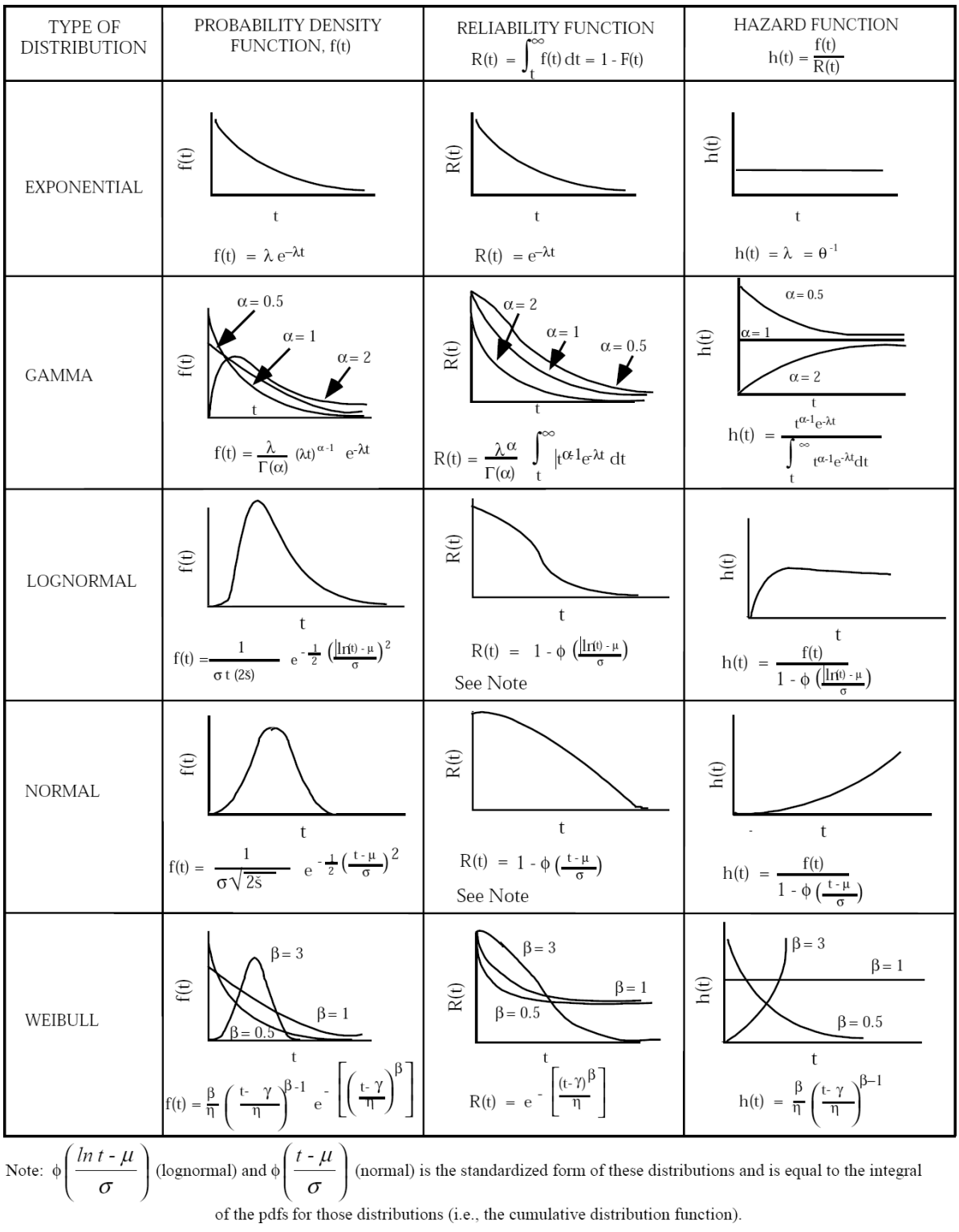

Figure 2.2: Shapes of failure density, reliability and failure (hazard) rate functions for commonly used continuous distributions (taken from [33], [41]).

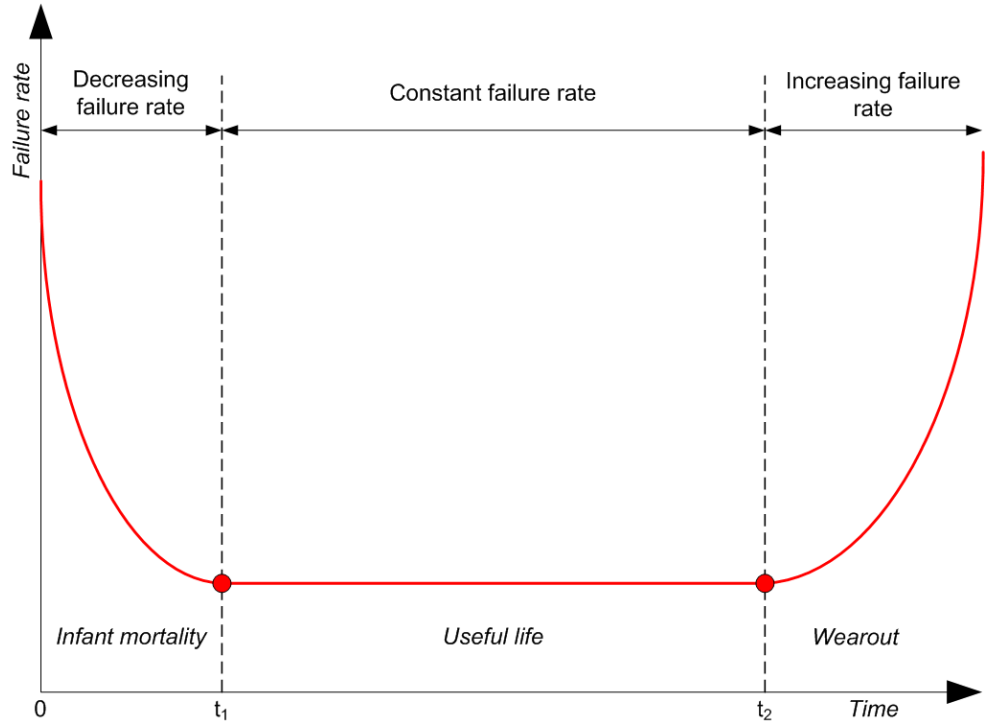

Figure 2.3: The bath curve describes a life cycle of electronic equipment. It is really assumed that exponential distribution and therefore constant failure rate (hazard rate).

the specification.

Therefore, the definition of a failure is bound to the idea of a contract, and to the notion of quality. Success or failure, like quality, is not a property of an element, but a point of view of an external user. For any analysis, one should first quantify exactly what one understands as a failure.

A general definition of a failure is:

"A failure is the termination of the ability of an item to perform its required function"

(by definition of the IEC- International Electrotechnical Commission).

The above definition supposes that the mission specification includes a yes/no criterion like reject/accept. Complex systems exhibit a variety of failure modes, some major, some minor. In these cases, one should define service classes or performance levels, as we shall see below.

The above definition makes no assumption about the duration of the failure: it rather

expresses a transition. "Failure" can also express a state. When it is necessary to make the distinction, we will use "failed" (for the state) and "failure for the event.

An item can cease to provide the required service during a certain time, but return to service shortly afterwards, either because the cause of the disruption (for instance an external disturbance) disappeared by itself or because the item was repaired, either by its own means or by an external action.

"A malfunction is a temporary disruption of service."

This disruption is not necessarily caused by damage. In the power utilities, an outage is the inability to supply electrical energy – this may be due to network instability.

2.4.1 Fault Classification

The fault classification is shown in Fig. 2.4. This thesis deals primarily with two types of faults – permanent and transient. The following text explains the fundamental differences between these two types of faults, from point of view a system and its elementary electronic parts. A simple general system is shown in Fig 2.5.

Permanent Fault
Permanent fault means a fault with lasting effects. The failed component or system must be replaced [10].

Transient Fault
Transient fault means a fault of limited duration that causes no permanent hardware damage. Transient faults can be cause by excessive heat, power disruptions, timing issues or environmental influences, for example. It is often possible to recover from a transient fault without discarding the affected component or system. [10].

In addition, there are mentioned several sources in which the transient faults are well described:

- New Physical Mechanism for Soft Errors in Dynamic Memories [3].
- Dr. Tomas Vanat closely showed and described possible kind of transient faults in his defended thesis from July 2017 [44]. His thesis deals with especially effects caused by ionizing radiation increases. These effects can have negative consequences for electronic equipment.
- The Use of Lasers to Simulate Radiation-Induced Transients in Semiconductor Devices and Circuits [45].
- Effect of Cosmic Rays on Computer Memories [29].

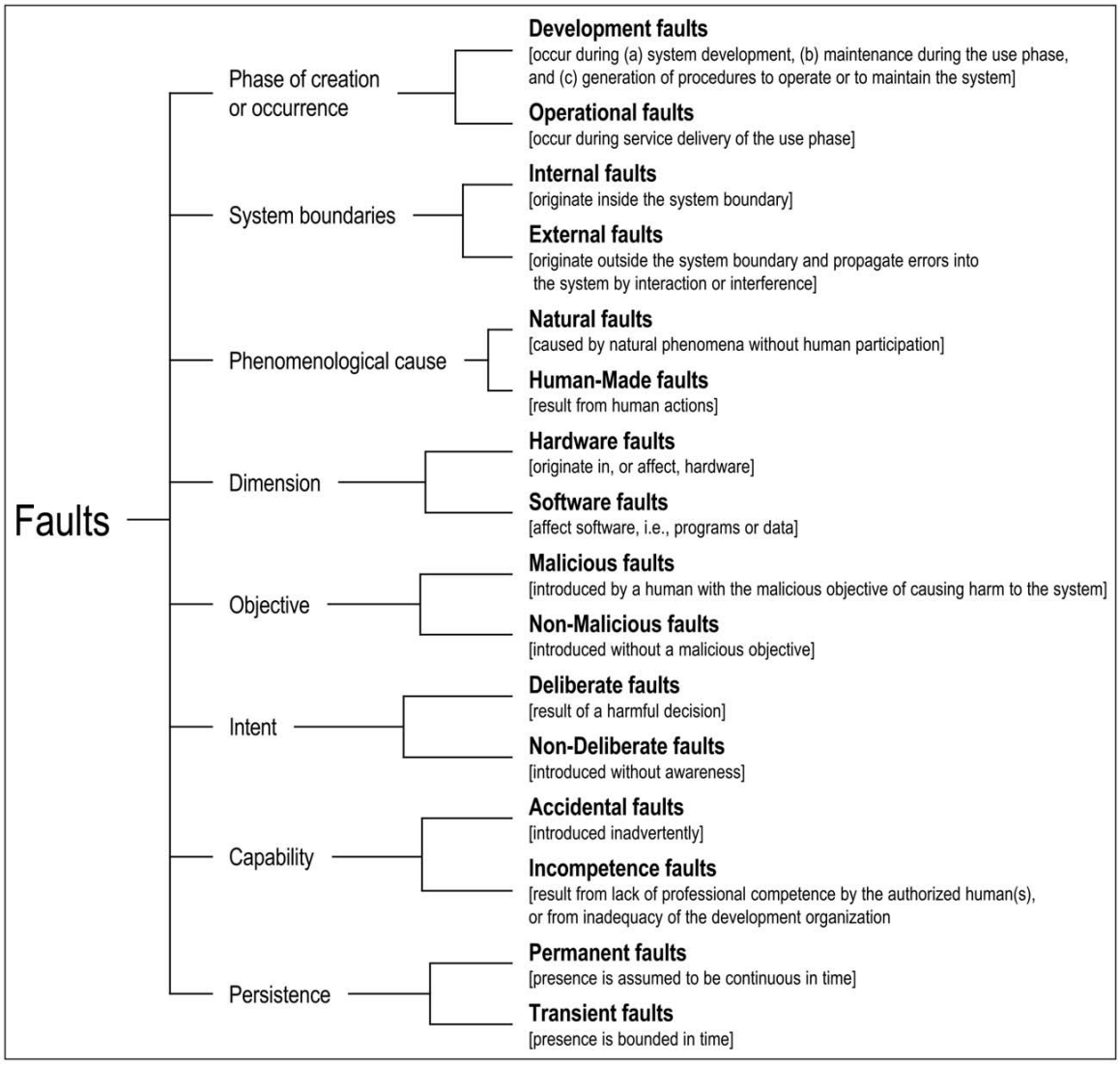

Figure 2.4: Fault classification (taken from [13]).

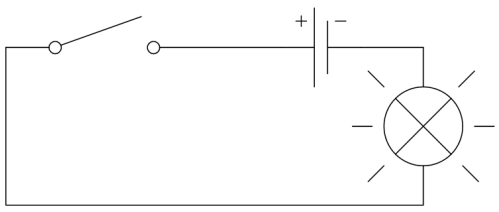

Figure 2.5: This circuit represents a general system. The bulb represents a failure indicator and constantly on. In case of a permanent fault (somewhere in this system) the bulb turn off. The bulb will blink in case of transient faults.

- Transient fault characterization in dynamic noisy environments [2].

The problem of protection of digital circuits (only combinational logic), e.g. FPGAs against transient faults, is solved [46, 47].

2.5 Increasing Dependability Parameters – Redundancy

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

- Backup: dynamical and static.
- Redundancy: hardware, software, temporal, information.
- Robust components: fault tolerant design, diversity.

The most critical factor for this work is using the redundancy. Regarding use and design, redundancy can be divided into four basic forms:

- **Hardware**: The use of hardware in addition to that which would be required to implement the system in the absence of faults, with the aim of detecting or tolerating faults [6]. An example of such a system is the triple modular redundancy (TMR). In TMR modules receive identical input signals and therefore should produce identical outputs. A voting mechanism (voter) compares the outputs from all the modules and using the majority function safeguards the correct output. If the output of one of the units (blocks) differs from those of its neighbours as a result of a single fault, the voter will produce an output corresponding to the majority voting scheme. Therefore TMR is able to masks a failure of any single module [A.2].
- **Software**: The use of software in addition to that which would be required to implement the system in the absence of faults, whit the aim of detecting or tolerating faults [6].
- **Temporal**: The use of information in addition to that required to implement a given function, with th aim of detecting or tolerating faults. Temporal redundancy might involve repeating calculations and comparing the results obtained. This can be used to detect a transient fault, and, if more that two calculations are performed, could allow a single faulty calculation to be ignored [6].
- **Information**: The use of information in addition to that required to implement a given function, with the aim of detecting or tolerating faults. Examples include the use of parity bits, error detecting or correcting codes (CRC) and checksums. Information redundancy may be implemented using hardware or software techniques, and is widely used within communications and VLSI devices such as memories and processors [6].

2.6 Reliability Prediction Methods

2.6.1 MIL-HDBK-217

The Reliability Prediction of Electronic Equipment U.S. military standard (MIL-HDBK-217) are used to estimate the failure rate for electronic equipment [14]. Data for this standard comes from the large amount of collected data by the U.S. armed forces and they often form the base 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 about the specific interconnection parts. The stress for each part is calculated by the wiring diagram.

The general rule is used for a failure rate calculation of a specific part, for example resistor:

$$\lambda_p = \lambda_b \pi_T \pi_P \pi_S \pi_Q \pi_E \tag{2.1}$$

Factor	Description
λ_p	Failure rate – λ of a resistor
λ_b	Base failure rate for a common resistor
π_T	Temperature factor
π_P	Power factor
π_S	Power stress factor
π_Q	Quality factor
π_E	Environment factor

Table 2.2: Table describes a meaning of individual factors.

Each factor can be determined using a specific equation or table, for example, π_S factor and π_E factor. For π_S factor holds following rules:

$$\pi_S = 0.71e^{1.1(S)} \tag{2.2}$$

or

$$\pi_S = 0.54e^{2.04(S)} \tag{2.3}$$

where S is:

$$S = \frac{ActualPowerDissipation}{RatedPower}$$

The difference between the Eq. 2.2 and Eq. 2.3 is determined according to the type of resistor respectively λ_b. This decision has to be made by a reliability engineer. The π_E

factor must be chosen from a table in the handbook. In this case, the π_E factor is a specific value number according to the used environment.

By this procedure a failure rate of a specific electronic part is determined. If equipment contains more parts it is necessary to determine failure rate for each part and to create a serial or different model (see 2.8.1). Then a specific failure rate for a whole equipment can be calculated.

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.

$$\lambda_{EQUIP} = \sum_{i=1}^{n} N_i(\lambda_g \pi_q)_i \tag{2.4}$$

Factor	Description
λ_{EQUIP}	Total equipment failure rate – λ of a whole system
λ_g	Generic failure rate for the i$^{\text{th}}$ generic part
N_i	Quantity of i$^{\text{th}}$ generic part
n	Number of different generic part categories in the equipment
π_Q	Quality factor of i$^{\text{th}}$ generic part

Table 2.3: Table describes a meaning of Eq. 2.4, this equation always holds for a given equipment environment.

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.

2.6.2 FIDES

FIDES is an French standard – Reliability Methodology for Electronic Systems in many ways improved than MIL-HDBK-217F. FIDES is a French consortium of industrial companies from aerospace and defence area, the group is composed of these companies:

- AIRBUS France,
- Eurocopter,
- Nexter Electronics,
- MBDA France,

- Thales Systèmes Aéroportés SA,
- Thales Avionics,
- Thales Corporate Services SAS,
- Thales Underwater Systems.

The first version was released in 2004 and the latest version of this standard is FIDES guide 2009 Edition. The first aim of this standard was to develop a new reliability assessment method for electronic components which takes into consideration commercial and specific parts and the new technologies.

The second aim was to write a reliability engineering guide in order to provide engineering process and tools to improve reliability in the development of new electronic systems. The global aim is to find a replacement to the standard MIL-HDBK-217F, which is old and has not been revised since 1995 (issue F notice 2). The basic formulas for calculating individual factors are below.

The FIDES general reliability model for an item is based on the following equation:

$$\lambda = \lambda_{Physical_Contributions} \Pi_{PM} \Pi_{Process} \tag{2.5}$$

where:

- λ – means the part failure rate.
- Π_{PM} – represents the quality and technical control over manufacturing of the item (part). PM means Part Manufacturing.
- $\Pi_{Process}$ – represents the quality and technical over the development manufacturing and usage process for the product containing the item.

Failure rates predicted by the FIDES methodology are hourly failure rates expressed per calendar hour and based on the use of an annual life profile. The failure rate for each phase is weighted by the duration of the phase:

$$\lambda_{Physical} = \sum_{i}^{Phases} \left(\frac{Annual_time_{phase-i}}{8760} \lambda_{phase-i} \right) \tag{2.6}$$

A non-leap year contains 8760 calendar hours. All models are presented with this value of 8760 hours. Obviously, this method could be adapted if the life profiles can be better described over longer or shorter periods of time. The annual calculation is still recommended in general.

The physical and technological contributing factors – $\lambda_{Physical}$:

$$\lambda_{Physical} = \left[\sum_{Physical_Contribution} (\lambda_0 \Pi_{Acceleration}) \right] \Pi_{Induced} \tag{2.7}$$

where:

- The term between brackets represents the contribution of normal stresses.
- $\Pi_{inducted}$ – represents the contribution of induced factors (also called overstresses) inherent to an application field.

It follows from the above equations that this standard is much more sophisticated than the MIL-HDBK-217. However, this can lead to problems, if the reliability engineer needs a model to be adapted to specific needs.

2.6.3 IEC TR 62380:2004

This is not a standard it is a technical report about *Reliability data handbook – Universal model for reliability prediction of electronics components, PCBs and equipment.* The methodology takes into account some influencing factors and, in particular, allows the element load profile to be taken into account. This methodology is an appropriate addition to the two previous ones from Section 2.6.1 and 2.6.2.

This technical report provides elements to calculate failure rate of mounted electronic components. It makes equipment reliability optimization studies easier to carry out, due to the introduction of influence factors [16].

2.6.4 Other reliability methodologies and standards

HDBK 217 Plus

The 217 Plus prediction module incorporates the component failure rate prediction models developed by the RIAC (Reliability Information Analysis Center). The 217 Plus is updated to develop a replacement prediction methodology for MIL-HDBK-217 "Reliability Prediction of Electronic Equipment," the widely used approach since 1995. 217 Plus implements the models presented in the "Handbook of 217 Plus^{TM} Reliability Prediction Models" [36].

FMEA/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 its implementation and application can be found in standards [48]. FMEA 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), 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:

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

The other reliability methodologies and standards are introduced in Tab. 2.5. The most well-known databases of reliability are in Tab. 2.5.

2.7 Predictive Analysis of System Dependability

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

- Functional and technical analysis.
- Qualitative analysis.
- Quantitative analysis.
- Synthesis of results.

The scheme of predictive analysis is shown in Fig. 2.6.

Functional and technical analysis

First phase Functional and technical analysis is used to collect data and maximize awareness of elementary elements of the system.

Qualitative analysis

The final goal of the "Qualitative analysis" is to find all 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.

Database	Current (previous) version	Producer	Types of parts	Specific area	Last updated
NPRD	NPRD-2016 (NPRD-2011, NPRD-95)	Quanterion Solutions Inc. (USA)	electric, electromechanical, mechanical	–	2015
EPRD	EPRD-2014 (EPRD-97)	Quanterion Solutions Inc. (USA)	electronic	–	2014
FMD	FMD-2016 (FMD-97)	Quanterion Solutions Inc. (USA)	electronic, electric, electromechanical, mechanical	–	2015
SPIDR	SPIDR	System Reliability Center (SRC) (USA)	electronic, electric, electromechanical, mechanical	–	2006
OREDA	OREDA, OREDA-2015	OREDA (Norway)	electric and mechanical parts of oil/gas systems	oil and gas industry	2015
PDS Data Handbook	PDS Data Handbook 2013	SINTEF (Norway)	Safety Instrumented Systems (SIS) components	(oil) processing industry	2013
SERH	SERH, SERH 4th ed.	exida (USA, Germany)	Safety Instrumented Systems (SIS) components	processing industry	2015
EIREDA	EIREDA	European Safety, Reliability & Data Association (ESReDA)	electronic, electric, mechanical parts of nuclear systems	nuclear power engineering	1998
IAEA-TECDOC-478	IAEA-TECDOC-478	International Atomic Energy Agency (IAEA)	electronic, electric, mechanical parts of nuclear systems	nuclear power engineering	1988

Table 2.4: Brief overview of reliability databases.

Methodology	Current (previous) version	Producer	Types of parts	Specific area	Last updated
MIL-HDBK-217	MIL-HDBK-217F Notice 2, MIL-HDBK-217G (unofficial)	US Department of Defense	electronic	–	1995, 2011 (unofficial)
PRISM	PRISM	System Reliability Center (SRC) (USA)	electronic, non-electronic	–	2003
217Plus	217Plus:2015 (217Plus)	Quanterion Solutions Inc.	electronic	–	2015
FIDES	FIDES, FIDES 2009, UTE C 80-811	FIDES (France)	electric, electronic, electromechanical, and printed circuit parts	aeronautics and defense industry	2010
RDF 2000	RDF 2000, UTE C 80-810, IEC/TR 62380	International Electrotechnical Commission	electronic and printed circuit parts	telecommunications industry	2004
Telcordia SR-332	SR-332 Issue 4, Telcordia SR-332 (Bellcore SR-332)	Telcordia Technologies (Ericsson) (USA)	electronic	telecommunications industry	2016
GJB/z 299	GJB/z 299C, China 299C (GJB/z 299B)	Chinese People's Liberation Army	electronic	(Chinese) defense industry	2006
NSWC	NSWC, NSWC-11	NSWC, Caderock Division (USA)	mechanical	defense and shipbuilding industry	2011
Siemens SN29500	SN29500, Siemens SN29500	Siemens (Germany)	electric, electronic	Siemens-related areas	2011
HRD	HRD-5 (HRD-4)	British Telecommunications (BT Group)	electronic	telecommunications industry	1994

Table 2.5: Brief overview of reliability prediction methodologies

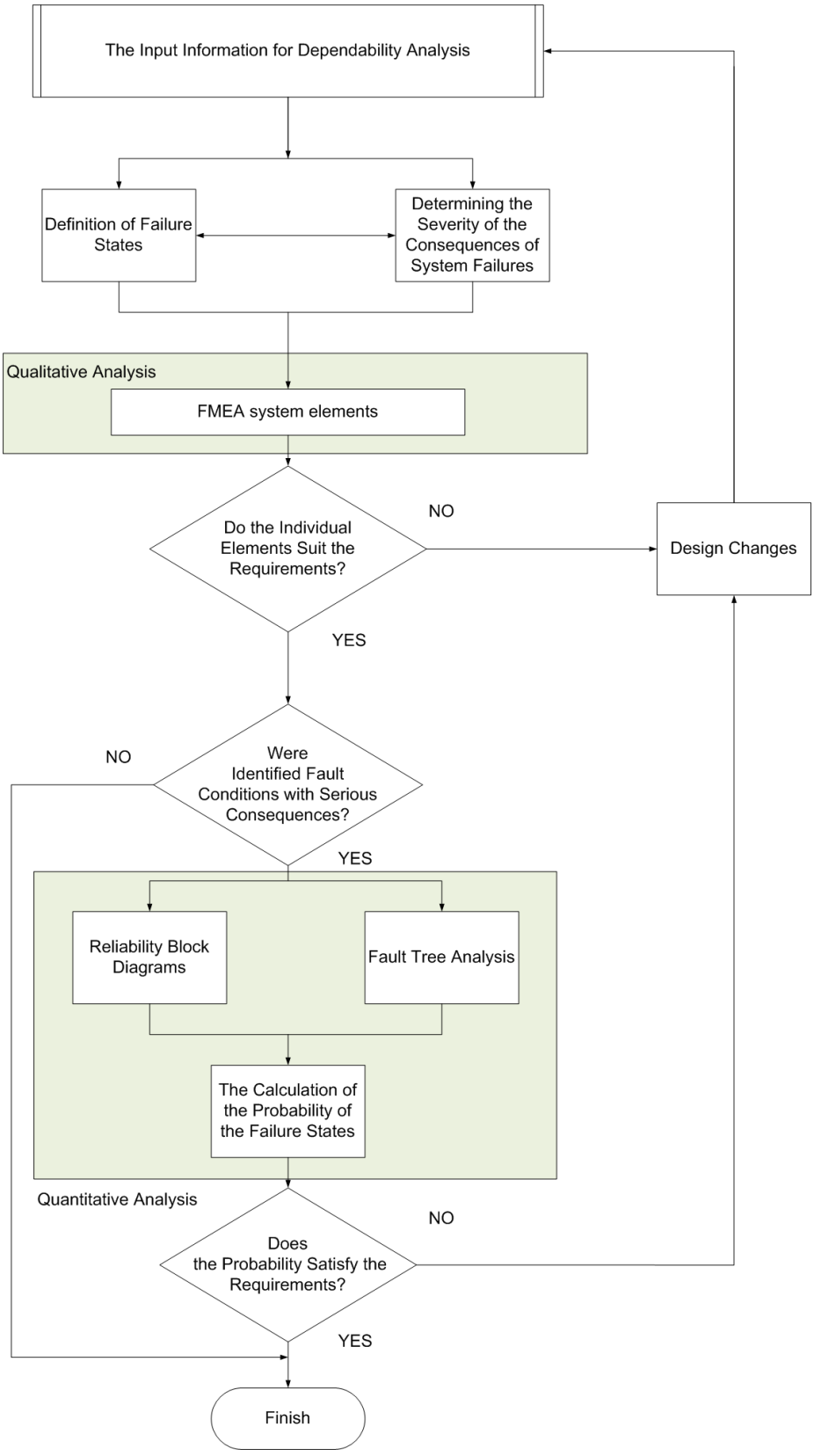

Figure 2.6: The process of predictive dependability analysis

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.

Synthesis of results

The phase Synthesis of results is used to assess the required level of reliability, to determine conclusions and recommendations.

2.8 Reliability Modelling

Most of the explanations and definitions in this section are taken from [6, 9]. It is essential to be able to predict the final reliability of a complete system containing many parts during the design stage of the project. In this section several methods for a reliability modelling to estimate the reliaiblity of complex systems are shown and described. The list of mentioned methods is not exhaustive because this text focuses only on methods related to this work.

2.8.1 Reliability Block Diagrams

The symbols within reliability block diagrams are described in the international standard IEC 61078 [8]. These models consist of blocks. The block can be a whole system, subsystem, functional module or individual part. The term *block* will be used for all above mentioned items in this section.

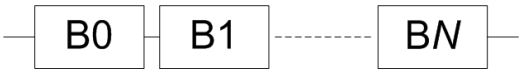

Figure 2.7: The example of a serial RBD model.

Serial Systems
This model represents the *Lusser's Law* that was introduced in the Section 2.1. It is a basic reliability model that is used for example in the standard MIL-HDBK-217 [14].

Within any module that is not itself fault tolerant, it can be assumed, that failure of any of its components may cause a system failure. Such an arrangement is represented in Fig. 2.7. Here, the blocks describe various components or parts of the designed system. It is not the aim of the individual blocks to map physical interconnection of the system components but to show the dependency of their reliability properties. A failure of any of the blocks will result in overall failure, the failure rate of a serial model is equal to the sum of the failure rates of the individual blocks. If a system contains N components, then failures of various components must be independent. The system's failure rate – λ, during its constant failure rate period, is given by

$$\lambda = \lambda_1 + \lambda_2 + \cdots + \lambda_N \tag{2.8}$$

where λ_i is the constant failure rate of the ith component. This expression can be rewriten as

$$\lambda = \sum_{i=1}^{N} \lambda_i \tag{2.9}$$

The reliability of the arrangement may also be expressed in terms of reliability of the components. If $R_i(t)$ is the reliability of the ith component in the system, then the overall system reliability $R(t)$ is given by the expression

$$R(t) = R_1(t) \times R_2(t) \times \cdots \times R_N(t) \tag{2.10}$$

that may be written as

$$R(t) = \prod_{i=1}^{N} R_i(t) \tag{2.11}$$

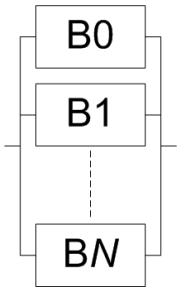

Figure 2.8: The example of a parallel RBD model.

Parallel Systems

In systems with redundancy, failure of one of the modules or one of the components may not result in failure of the whole system or subsystem. Such an arrangement is described as a parallel system and is shown in Fig. 2.8. In this arrangement it is assumed that the system will remain operational if at least one of the parallel blocks works correctly. To determine the reliability of a parallel system we start by considering the probability of a failure, first of an individual block, and then of the complete system. As the reliability of a block $R(t)$ is the probability of its correct function for a period of time t, then $[1 - R(t)]$ must be the probability of its failing within this time. The quantity $[1 - R(t)]$ is referred to the unreliability of a component$Q(t)$.

If a system contains N parallel (independent) blocks, then the probability of the whole system failure, will be the product of probabilities of each units. Thus, the probability of failure of the system is given by

$$Q(t) = [1 - R_1(t)][1 - R_2(t)] \ldots [1 - R_N(t)] \tag{2.12}$$

where $R_i(t)$ is the reliability of the ith block. The reliability of the system is therefore

$$R(t) = 1 - Q(t) = 1 - [1 - R_1(t)][1 - R_2(t)] \ldots [1 - R_N(t)] \tag{2.13}$$

or simply

$$R(t) = 1 - \prod_{i=1}^{N}[1 - R_i(t)] \tag{2.14}$$

If, as is often the case, the parallel blocks are identical, each with a reliability of $R_m(t)$, then this expression may be simplified. The system reliability then becomes

$$R(t) = 1 - Q(t) = 1 - (1 - R_m(t))^N \tag{2.15}$$

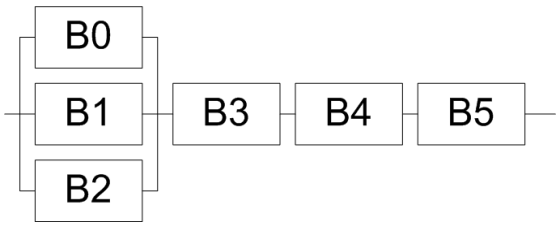

Figure 2.9: The example of a combined RBD model.

Combined Systems

In practice, real systems are often more complicated than the simple serial and parallel ones described above. However, all these systems can be reduced to a combination of these two structures. It is necessary to know that these models are hierarchical and every system can be expressed as one block. Fig. 2.9 shows an example of system consisting of several functional blocks. The calculation procedure is as follows

- At first, the parallel part of system – block B0 to block B2 must be calculated.

$$R_{012}(t) = 1 - [1 - R_0(t)][1 - R_1(t)][1 - R_2(t)]$$

- Then can be calculated the serial part of system included new block B012 (the original parallel combination).

$$R(t) = [1 - R_{012}(t)][1 - R_3(t)][1 - R_4(t)][1 - R_5(t)]$$

- For completeness, let's note that the mean time to failure (MTTF) is calculated by the relationship

$$MTTF = \int_0^\infty R(t)dt \tag{2.16}$$

Summary

The list of the above mentioned RBD models is not final. There are, for example *cut and tie sets* and models with dynamic redundancies [6]. The advantages and disadvantages of these reliability models – RBDs is described in Tab 2.6.

	Advantages
1	Simplicity & speed of using.
2	Usability – model can be used on most systems.
3	Hierarchical model – individual blocks can be nested.

	Disadvantages
1	Model provides only one attribute – failure rate.
2	Model does not support time dependancies – for example, in case of failure of the block B_x the system will be restored to n hours.
3	It is necessary to use further model for complex systems, for example Markov chain.

Table 2.6: Table describes advantages and disadvantages of RBD.

2.8.2 Fault Tree Analysis

Event trees start with all possible events and work forward to determine their outcomes. Consequently, much of the analysis is concerned with operations that have no safety implications. Fault tree analysis, in contrast, start with all identified hazards and works backwards to determine their possible causes. In application where information is available from similar systems already in production, data from earlier accidents, or incidents, may also be used as a starting point for the analysis. Logical operators, similar to those used in Boolean algebra, are used to combine the effects of events to determine relationships between cause and effects. Concentrating on events that are known to lead to hazards, results in a simplified tree structure for event tree analysis.

Fault tree analysis is a graphical method starting by an event directly related to an identified hazard, called the *top event*, and works backwards to determine its cause. Intermediate events related to the top event are combined using logical operations such as AND or OR (often called **gates**), and the process is repeated, working back to the basic event (or input), that are the root cause of the hazard. The graphical nature of the analysis simplifies interpretation, and FTA is often used to represent dependencies, identified using other hazard analysis techniques such as FMEA (*Failure Modes and Effects Analysis*) and HAZOP (*HAZard and OPerability studies*) [6].

Events are combined by logical operations that are represented using a set of symbols (gate AND, OR, etc.). These symbols are described in the international standard IEC 1025 [49].

Example

A very simple example of fault tree is shown in Fig. 2.10 and Fig. 2.11. This example refers to the Fig. 2.5. It shows the conditions for failure f – either event f_1 or f_2 or f_3.If one of these failures occur the system fails. The meaning of block names may be

- f – control circuit failure (the bulb does not light),

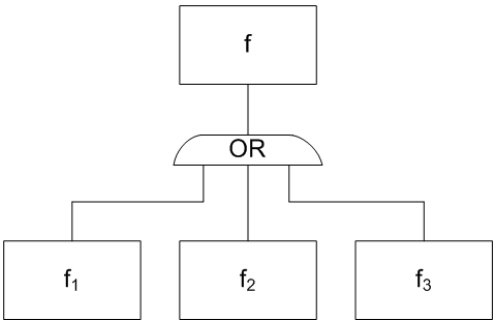

Figure 2.10: The example of Fault Tree for a top event – f. A possible failure of a system. This fault tree has not defined any **basic event**.

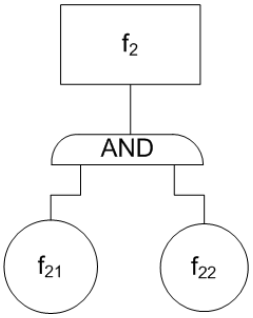

Figure 2.11: The example of Fault Tree containing basic events (taken as inputs) f_{21} and f_{22}. The top event f_2 occurs if both inputs occurs together.

- f_1 – failure of the bulb,
- f_2 – failure of the battery,
- f_3 – failure of the switch,
- f_{21} – the battery is dead – the basic event with probability p_{21},
- f_{22} – the battery is short-circuited – the basic event with probability p_{22}.

The trees from both figures can be joined. For more information about this analysis can find in this Fault Tree Handbook see [10].

Summary

A popularity of fault trees in reliability analysis is mainly due to its benefits, followed in Tab. 2.7.

	Advantages
1	Clarity and expediency.
2	Allow gradual fine down of the reliability model to any level of detail.
3	It is possible to divide the trees into sub-trees that are evaluated separately.
4	The fault tree can be simply converted to the Markov model for the specified constant intensity of the basic events.
5	Provide a qualitative and quantitative reliability analysis.

	Disadvantages
1	Can be enormous (thousands of gates and intermediate events).
2	Not necessarily all failure modes are considered.
3	External events not correctly treated.
4	An analysis of basic events can be time consuming.
5	Need experienced engineers.

Table 2.7: Table describes advantages and disadvantages of FTA.

2.8.3 Markov Chains

The modelling techniques described above determine the overall reliability of the system by using measured or predicted values for the reliability of its constituent parts. One of the advantages of Markov chains is that it provides a more powerful way of modelling of the systems, that is repairable, allowing variables as is the time taken to repair a system to be incorporated. An alternative approach is to assign various states to a system and to determine the probability of being in any of these states [6]. Markov models can be divided into two basic category – discrete and continuous Markov models. Continuous Markov chains are more important for this thesis.

Markov chains can model stochastic processes using random variables to describe the states of the process, transition probabilities for changes of state and time or event parameters for measuring the process. A stochastic process is said to have a Markov property, if the conditional probability of any future events, is given by any past events and if the present state is independent of the past events and depends only on the present state of the process. The advantages of using Markov modelling methods include the flexibility in expressing dynamic system behaviour. The Markov models are widely used to estimate the dependability parameters and performance. These models can be used for both permanent (or stuck-at) and transient faults representations.

Discrete Markov Modelling

Consider the system shown in Fig. 2.5. A simple Markov chain of this system is shown in Fig. 2.12.

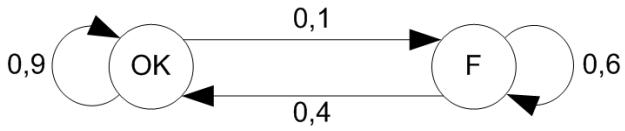

Figure 2.12: The example of Markov chain with repair rate (this figure is taken from [6]).

Continuous Markov Modelling

In many cases it is more sensible to consider a system in a continuous time domain rather that as a serial of discrete time intervals. This can be done using continuous Markov modelling, where the probabilities of state transitions are replaced by transition rates.

The Markov chains of redundant system is considered in the following two examples, see Fig. 2.14 and Fig. 2.13, because this thesis deals mainly with redundant TMR based systems. The first one Fig. 2.14 represents a system with absorption state (state F) and the second one is a system that is renewed.

The meaning of states of these models:

- OK – represents the state of a system where all is in order. In case TMR – all modules and voter is in operational
- $1F$ – represents the state of a system where one module is faulty.
- F – represents the absorption state – the system failure (two or more modules or voter is faulty).

Both Markov chains have specific sets of equations for solving dependability parameters. Fig. 2.14 shows the Markov chain with one absorption state (F).

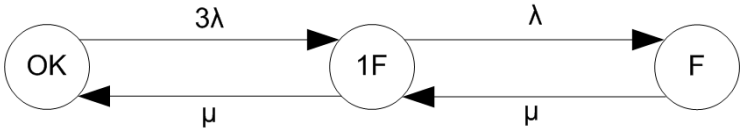

Figure 2.13: The example of Markov chain with a repair rate – a renewed system.

$$\begin{aligned} p'_{OK}(t) &= -3\lambda p_{OK}(t) + \mu p_{1F}(t) \\ p'_{1F}(t) &= 3\lambda p_{OK}(t) - (\lambda + \mu) p_1(t) \\ p'_F(t) &= \lambda p_{1F}(t) \\ p_{OK}(0) &= 1; p_{1F}(0) = p_F(0) = 0 \end{aligned} \tag{2.17}$$

where p_{OK}, p_{1F}, p_F are specific probability of individual states. The last row describes initial conditions.

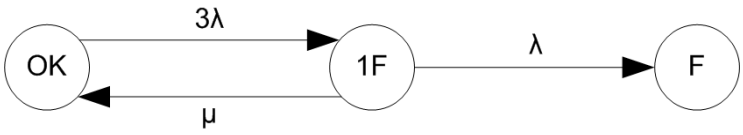

Figure 2.14: The example of a Markov chain with a basic repair.

The set of equations for renewed system is in Eq. 2.18. These equations are linearly dependent.

$$\begin{aligned} 3\lambda p_{OK} &= \mu p_{1F} \\ 3\lambda p_{OK} + \mu p_F &= (\lambda + \mu) p_{1F} \\ \lambda p_{1F} &= \mu p_F \\ p_{OK} + p_{1F} + p_F &= 1 \end{aligned} \tag{2.18}$$

where p_{OK}, p_{1F}, p_F are specific probability of individual states. The last equation means, that sum of all probability must be 1.

Summary

A popularity of Markov chains in reliability analysis is mainly due to its benefits, followed in Tab. 2.7.

	Advantages
1	Clarity and expediency.
2	Intuitive, mathematically tractable, well-studied topic, many good applications.
3	Hierarchical usage.
	Disadvantages
1	The number of states is growing rapidly.
2	The need to use numerical methods (if the model has multiple states).
3	Time consuming calculations (if the model has multiple states).

Table 2.8: Table describes advantages and disadvantages of Markov chains.

2.9 Previous Results and Related Work

My current work extends defended dissertation thesis whose author is Dr. Radek Dobiáš. Concurrently this thesis continues in my bachelor and diploma thesis which subject was the implementation for modelling and following calculation of reliable models in the available mathematical systems (Maple [5], Mathematica [50]) with defined arithmetical precision in advance. Part of my current research is also a creation of database of dependability that aims to contribute to the prediction of reliability proposed systems.

2.9.1 Previous Results

I have been a member of AŽD development department for two years. I have dealt with sufficiently objective predictive analysis of railway equipment there. It is not only about the proof of reliability but also ensuring maintainability throughout the lifecycle of the system. The main result of this research will be to procedure: *How to design system architecture with guaranteed level of reliability and safety.*

This dissertation thesis follows up on these already defended dissertation works *Methodology of Fail-safe and Fault Tolerant System Design* from Dr. Radek Dobiáš [42] and *Hierarchical Dependability Models Based on Markov Chains* from Dr. Martin Kohlík [41].

The first thesis *Methodology of Fail-safe and Fault Tolerant System Design* deals with fault tolerant and fail-safe system development for railway interlocking equipment based on the FPGAs. It proposes a procedure how to prove that FPGA-based railway equipment meet the requirements of European standards EN 50126 [39] and EN 50129 [51].

The further topic included in his thesis is the temporary fault modelling and the dependability models of the railway equipment including influence of the dangerous behaviour of human operators. He is also a co-author of the KOA device and his thesis contains the basic dependability models, hazard rate and availability calculations related to this equipment.

The second thesis *Hierarchical Dependability Models Based on Markov Chains* deals with the similar topic. His work is focused on the simplification of hierarchical Markov chains. His method allows independent calculations of the hazard rates of the redundant subsystems of the system. The main advantage of his method is the speedup of the calculations, but at the cost of the accuracy (the solutions are more pessimistic than the solutions provided by the exact methods).

We have collaborated on the KOA case study project [A.14] presented in my work. The data collecting, extraction and classification was my participation on the project; he has focused on the simplification of the hierarchical dependability models and the final failure rate calculations.

2.9.2 Related Work

Modelling of Transient Faults

The transient fault that is defined in section 5, can be modeled using Markov chain. The

system to be protected against transient faults have to contain some redundancy.

Papers presented in [52, 53] deal with the permanent and transient faults. These models and the models proposed in this thesis assume that a single transient fault can cause a failure of the system only when it is preceded with another fault, but there are several differences:

1. My models are focused on periodical systems (systems switching critical and non-critical parts of the calculation periodically) and I assume that the transient fault can cause the system failure only when it appears during the critical part of the calculation.

2. My models do not include any kind of system repair/recovery, because I assume that a single transient fault will not cause any error (the unaffected a critical part of a calculation) or a fault is masked by TMR (transient fault in a critical part of a calculation) will generate a correct result and the effect of the transient fault will be dissolved before another critical part starts).

DE Patent DE 10 2013 225 039 B4 [46] describes a detection and correction method intended for transient errors in the combinational circuits based on asynchronous C-elements and latches. Unfortunately, the patent does not provide any dependability model or calculations, thus I can not compare it with my approach directly.

Dependability Modelling Under the Changing Conditions

Analytical computations of dependability properties is possible only if the predefined conditions, e.g. failure rates of all components are known and constant. The method how to achieve applicable results under changing conditions is briefly described in [17]. The method is based on the construction of reliability models and their dependability assessment using a simulation tool available in UPPAAL SMC, see [54]. Stochastic timed automata and statistical model checking were used and first simple models and results were presented. The presentation was only short (poster type), but such timed stochastic behaviors over continuous time, dynamically manageable objects within the simulation process etc., could be interesting area of future research and some other type of model to include into my Heterogeneous Dependability Model (HDM), described in Chapter 3.

Chapter 3

Heterogeneous Dependability Model

The reliability modelling based on Reliability Block Diagrams and Fault Trees is described in this chapter. This proposed reliability model has been developed to provide clarity and nesting capability for other dependability models. This proposed dependability model has been published in [A.1, A.8, A.11, A.13] and [A.19], the last one is enclosed in App. A.

3.1 System Modelling

Most of safety systems is nowadays designed hierarchically, in layers. It means that every system can be divided into smaller components such as separate functional units. These units can be divided into logical functional blocks consisting of several printed circuit boards (PCBs). Finally, each PCB consists of many electronic parts. These smallest parts represent the basic level of each system. It is necessary to know the failure rate of each of these parts. The total failure rate of larger components can be calculated using failure rates of these individual parts. Then for the particular modules, we can calculate failure rates of each using the same approach, then for other modules, then for units, and finally for the whole system. This approach is shown in Fig. 3.1. A system can have up to n layers. These layers are only a logical representation of a specific level in the system hierarchy. The whole system is always on the top level and the elemental further indivisible or atomic parts are always on the lowest level. The schema of the system shown in Fig. 3.1 corresponds the most to a tree structure. For every designed system, operational demands are defined, for example maximal and minimal operational temperature, humidity, vibration, maximal stress, or current, etc. All these requirements are related to dependability, respectively to the reliability of the designed system.

I needed a tool that could unify all these requirements. I used the internal form of RBD which I have proposed in my Master thesis [A.18]. Thus, I have developed a *Heterogeneous Dependability Model* that was gradually improved. That Heterogeneous Dependability Model was published in these papers [A.1, A.8, A.11, A.13] (Note: the proposed model had a name: "Hierarchical Reliability Block Model" in these papers, but a more appropriate naming (used in this Thesis) is "Heterogeneous Dependability Model".). I have used this

proposed model to solve the prediction analyses of dependability [A.14, A.15]. These analyses are described in detail in the next Chapter 4.

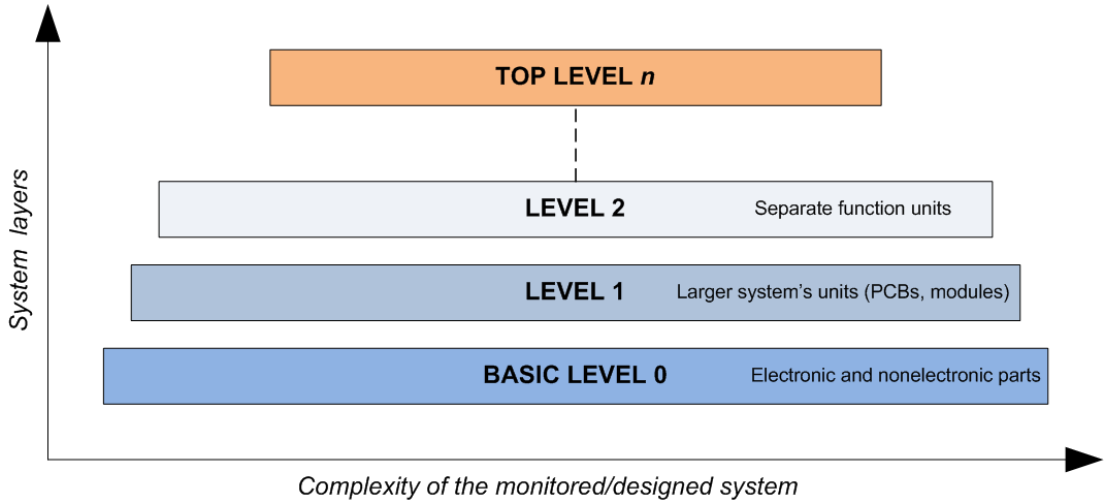

Figure 3.1: The diagram shows a system hierarchy model of a common electronic system.

3.2 Specification of the Heterogeneous Dependability Model

The proposed model is based on *Reliability Block Diagrams* and it is precisely related to contemporary system design methods. The basic idea is the level of abstraction, where the Heterogeneous Dependability Model allows for the possibility to imagine a large system model as a separate block. These models also have the property that other reliability models can nested them, for example, Markov chain. A direct relationship between the layers of the system and the layers of the Heterogeneous Dependability Model is shown in Fig. 3.2.

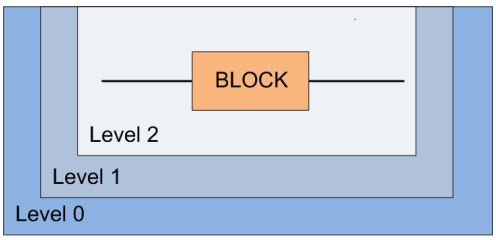

Figure 3.2: Layers of the Heterogeneous Dependability Model of a common system shown in Fig. 3.1.

3.2.1 Block Specifications

The Heterogeneous Dependability Model consists of common blocks such as reliability block diagrams. The difference is not only in the structure of whole model (which forms a tree structure), but also in the information or rules that the blocks hold. The RBD block contains a single value of *a total failure rate of an element* (and sometimes also a text description such as in SHARPE [4]).

An example block attributes that were used in the ABA-12 project [A.15] are given below:

- Title of the block – may be a system or a module name or a specific electronic part.
- Color of the block – may be the meaning for a specification of some important requirements.
- Failure rates:
  - Required failure rate.
  - Predicted failure rate according to the standard (MIL-HDBK-217, FIDES, IEC TR 62380).
  - Estimated failure rate according to the operational data.
- Operation conditions:
  - Maximal, minimal and expected operating temperature.
  - Humidity, vibrations etc.
  - Operating cycles – does the device work constantly or sometimes it shuts down?
  - Description of an operating environment.
- Description of the block – text notice.

The list mentioned above is not exhaustive. The block can be understood as a "white box" with a set of rules and attributes. Every reliability engineer can design and modify the block rules according to his needs.

3.2.2 Internal Form and Gradual Calculation

The need to the model the system layers can be best shown using the *tree structure*. With a closer look at serial models, parallel models, or combined models, it is evident that these models can be described by a tree structure. All RBDs (which are defined in Section 2.8.1), including their equivalent tree structures, are shown in figures below. No restrictions are defined for these considered systems. The sets of rules of each block are empty and each block has one attribute – λ_{Bi}. A constant failure rate is assumed (which involves exponential distribution, see Section 2.3).

Serial model

The series model and its equivalent in a tree form are shown in Fig. 3.3. The block S has been added to the tree structure, defining a serial model consisting of blocks B0 - B2. This new block also defines the top level of the whole system. The block S defines the reliability function as well as in the case of the classical serial model (defined in Section 2.8):

$$R_S(t) = R_{B0}(t) \times R_{B1}(t) \times R_{B2}(t) \tag{3.1}$$

$$R_S(t) = e^{\lambda_{B0}t} \times e^{\lambda_{B1}t} \times e^{\lambda_{B2}t}$$

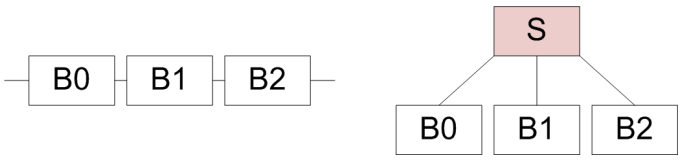

Figure 3.3: A basic example of the serial model and its equivalent tree form. The S block is a top-level block and it means the whole system.

Parallel model

The parallel model and its equivalent in a tree form are shown in Fig. 3.4. Similarly as in the previous case, the block P has been added to the tree structure, defining a parallel model consisting of blocks B0 – B2. This new block also defines the top level of the whole system. The block P defines the reliability function, as well as in the case of the classical parallel model (defined in Section 2.8):

$$R_P(t) = 1 - [1 - R_{B0}(t)][1 - R_{B1}(t)][1 - R_{B2}(t)] \tag{3.2}$$

$$R_P(t) = 1 - [1 - e^{\lambda_{B0}t}][1 - e^{\lambda_{B1}t}][1 - e^{\lambda_{B2}t}]$$

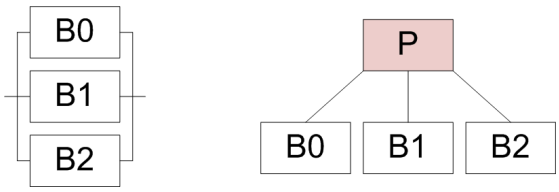

Figure 3.4: A basic example of the parallel model and its equivalent tree form. The P block is a top-level block and it means the whole system.

Combined model

The combined model and its equivalent in a tree form is shown in Fig. 3.5. Similarly to both previous cases, the two blocks P and S have been added to the tree structure, defining a combined model consisting of blocks B0 – B2 as the parallel part of the model and blocks P, B3 - B5 as the series part of the model. The new block S defines the top level of the whole system. The block P defines the reliability function as well as in the case of the classical parallel model and the block S defines the reliability function as well as in the case of the series model (defined in Section 2.8):

$$R_P(t) = 1 - [1 - R_{B0}(t)][1 - R_{B1}(t)][1 - R_{B2}(t)] \tag{3.3}$$

$$R_P(t) = 1 - [1 - e^{\lambda_{B0}t}][1 - e^{\lambda_{B1}t}][1 - e^{\lambda_{B2}t}]$$

$$R_S(t) = R_P(t) \times R_{B3}(t) \times R_{B4}(t) \times R_{B5}(t)$$

$$R_S(t) = (1 - [1 - e^{\lambda_{B0}t}][1 - e^{\lambda_{B1}t}][1 - e^{\lambda_{B2}t}]) \times e^{\lambda_{B3}t} \times e^{\lambda_{B4}t} \times e^{\lambda_{B5}t}$$

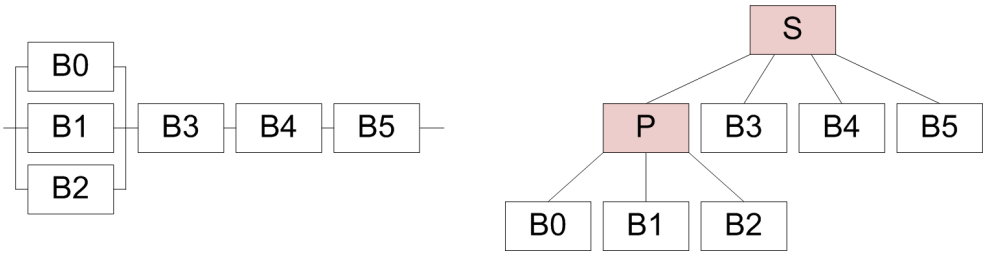

Figure 3.5: Basic example of a combined model and its equivalent tree form.

An Example HDM Containing Different Reliability Models

The proposed Heterogeneous Dependability Model can be used to describe a more complex system whose components can be modelled in various reliability models. In Fig. 3.6 there is an example such a system. The considered system is composed of one basic B0C block and other components which are shown in Fig. 3.7 and described using serial models, fault tree, and a Markov chain.

The considered equipment is an early warning system against a snow avalanche. The system consists of these components:

- B0 – block represents a basic block – some electronic parts (a bulb, a bulb socket, resistors, capacitors, integrated circuits, etc.).
- B0A – the block represents a unit of a light signalling of a danger.
- B0B – the block represents the acoustic signalling of a danger.
- B0C – the block represents the GSM early warning transmitter.

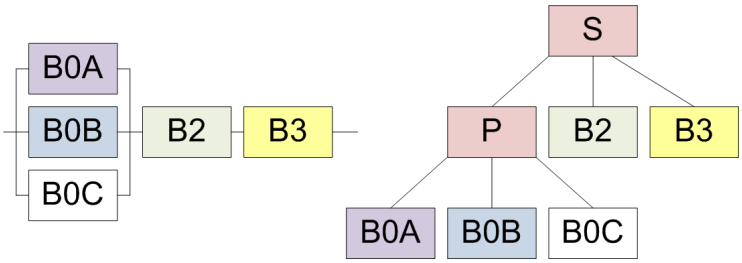

Figure 3.6: An example of a combined model and its tree form that includes other types of reliability models. The B0C block is an individual block, the B0A, B0B blocks contain series system, the B2 block contains a fault tree, and the B3 block contains a Markov chain.

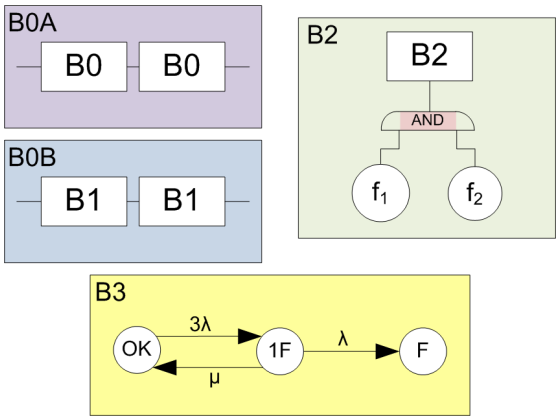

Figure 3.7: Composition of individual blocks (B0A, B0B, B2 and B3) from Fig. 3.6.

- B1 – block represents a basic block – some electronic part (a speaker, an alarm, etc.).
- B2 – the block represents the power supply.
- B3 – the block represents the complex redundancy system for assessing snow avalanche risks.

Each block of this model can have a set of conditions or requirements for its correct operation. For example:

1. The S block holds the attribute of minimum temperature set to a specific value. That means, that for the whole equipment, every electrical and non-electrical part of it has to meet this requirement. In other words, this attribute "runs through" from root to leaves.
2. The B3 block has an attribute set for a maintenance; a serviceman has to check all three evaluation modules and their voter every 5 000 hours.
3. The equipment does not work permanently, but only in case of a snow avalanche.

4. More and more requirements and rules which are placed on today's systems...

This considered system is not a functional device, but only an example how to combine reliability models. The calculation of the failure rate for this system can be executed according to the standard expressions mentioned in Section 2.

3.3 Summary

Looking at the three models above, it is clear that each of them can be described by a tree structure. The root of the tree will always represent the whole system – the top level. This block includes all known and available limitations and rules for the entire system. The tree leaves (the lowest system level) will always represent the elementary parts or a nested sub-model. Other internal nodes will always represent mathematical operations, requirements, and rules that are placed in blocks in lower levels. In other words, the internal form shows, that the most basic information is held in tree leaves. Any sub-root represents only the information about the operation, applied to its direct descendants or to the rest of the subtree.

Each block of the mentioned model has to hold the required set of attributes and rules, by which it is possible to generate the equations with the parameters required for calculations. In order for the system to generate the equation, each model must hold information on all its objects; they must take the hierarchical structure and nesting into account. For these calculations, it was necessary to design an internal representation that will actively change its response to model changes – the tree structure was the simplest one.

The advantage of this model is the possibility to show a system architecture in a tree form, such as shown in Fig. 3.1. Next advantages or disadvantages are described in Tab. 3.1.

From the point of view of predictive reliability analysis, the model can be included in the quantitative analysis shown in Fig. 2.6. Moreover, this model is also suitable for the early stages of analysis (functional and technical analysis, see Fig. 2.6), when it is necessary to collect information (attributes and rules) about the designed equipment and its operation.

Appendix A contains a conference paper [A.1] that describes an application of the proposed dependability model in practice. The Heterogeneous Dependability Model has been successfully used in the search for critical electronic parts on the track signalling equipment.

	Advantages
1	Simplicity & processing speed. At the beginning, it is possible to work with the RBD in a tree structure only.
2	Usability & universality – the model can be used for most of systems and the user can design his own system rules for a block.
3	Hierarchical model – individual blocks can be nested.
4	Critical parts of the system can be found very quickly.

	Disadvantages
1	Can not model system states. In this case, it is necessary to use a Markov chain, for example.
2	The time consumption of a model creation depends on the number of attributes stored in the blocks.
3	For computations it is necessary to use some programming and mathematical environment, for example Maple or Wolfram Mathematica. [5, 50].

Table 3.1: Advantages and disadvantages of Heterogeneous Dependability Model.

Chapter 4

Case Studies: Electronic Track Circuits & Eurobalise

This section describes two different case studies on the same topic. The first study [A.14] deals with predictive analysis of a parameter failure rate of track circuit systems (KOA) according to the standard MIL-HDBK-217 and according to the operation data. The second study [A.15] deals with predictive analysis of a parameter failure rate of Eurobalise (ABA-12) according to the same standard as the first one. The Hierarchical reliability block model is also applied in this section, defined in Chapter 3. Both analyses have identified possible problems with transient faults, these are described in detai in Chapter 5. Results of this chapter are published in these papers [A.5, A.9], the last one is enclosed in App. B.

4.1 Electronic Track Circuits

4.1.1 Cooperation with Industry

I supervised a project in 2014 – 2015 that dealt with a predictive analysis of reliability of an evaluation part of electronic track circuit systems (KOA) [55]. The project was based on cooperation between our university and the AŽD Praha company. This (contractual research) project gave me the opportunity to analyse real equipment. The manufacturer gave me **real data** gathered from ten years of equipment operation. The output from this project were three reports:

- *Summary of the project manager*
  This report has been determined for company managers and its content is a "business secret". The report contains simple outputs from the project, in the form of required information – failure rates, description of critical locations, recommendations to improve the reliability.

- *Detailed technical report*
  This report is also protected by "business secret", moreover, it contains detailed information about all calculations, assumptions, progresses, reliability models, results evaluation.

- *Comprehensive research report*
  This report contains a general description of the equipment, the used methodology, the reliability models and necessary assumptions resulting from the standards, internal directives and practical constraints. This report is publicly accessible and does not contain specific numerical values and results (predicted dependability parameters like MTBF) [A.14].

The first two reports serve only for business and development purposes. However, some important aspects of the calculations and assumptions are included in this section. Summaries of the third report are also contained in this section.

The resulting analysis followed these objectives:

- Predict the failure rate of the track circuit systems using the military standard MIL-HDBK-217F N2, using both methods (*Parts Count* and *Stress Part*).
- To estimate the failure rate of the track circuit system using operation data.
- Comparing the obtained failure rates and make the final assessment.
- To identify possible problems in these areas:
  - Data collecting and post-processing.
  - Localization of critical modules or electronic parts.
  - Determining fault types.
  - Determining unknown parameters of electronic parts according to the requirements of the standard MIL-HDBK-217 ("standard" unless otherwise stated).

The first three objectives are important primarily for AŽD. The remaining goals are important for my research. However, all the required goals have shown significant problems that need to be addressed.

4.1.2 Description of the Equipment

Electronic track circuits (or track circuit systems) are used to detect a train on rails. This is a very important system – the critical system for which the highest safety integrity level (SIL = 4) is required, according to the standard EN 50126 [39]. This device is in continuous operation. In the case of a fault, the device works in degraded mode and has to be repaired within 80 hours.

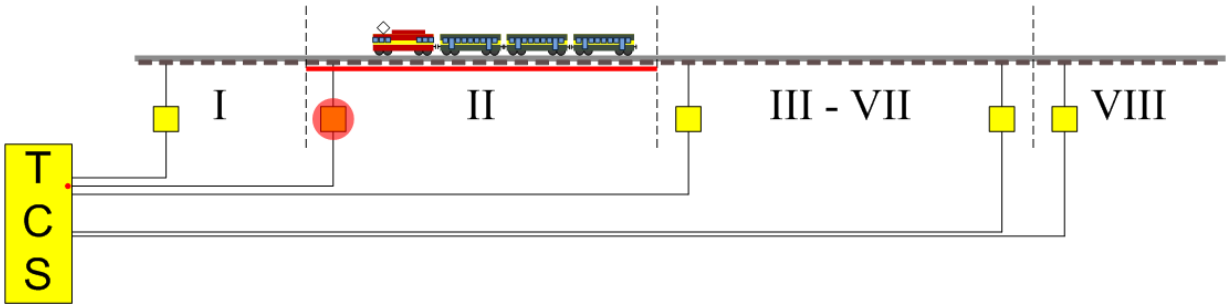

Figure 4.1: The electronic track circuit in a real operation. The figure shows the division of railway into 8 observed sections (marked with a Roman numeral). The detection part of electronic track circuit is under each railway section (small yellow box). The train occupies the second railway section. The box denoted TCS (big yellow box) is evaluation part of electronic track circuit.

A track circuit system provides information about the occupied and free track sections [55]. Fig. 4.1 shows a simplified model of an electronic track circuit. This system can be divided into two separate sets of parts – detection parts (it is possible to observe up to 8 sections) and evaluation ones (TCS). Each system can supervise up to eight track sections, see Fig. 4.1. This means that one evaluation unit monitors eight detection parts, see Fig. 4.1. The detection parts are close to the rails, while the evaluation part is in a railway building. Every evaluation part is located inside an air-conditioned rack. This rack can contain up to eight independent evaluation parts (TCSs) with one common power supply unit (PCB). It means that one rack can monitor up to 64 track sections. The aim of the project was to find required dependability parameters for **one evaluation part** only.

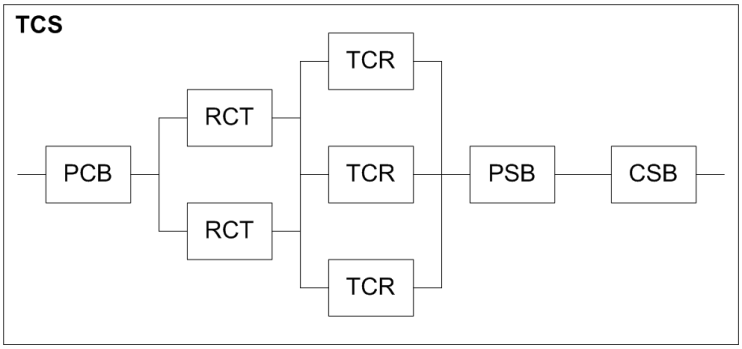

Figure 4.2: The block diagram of one evaluation part *Track Circuit System – TCS*. This block diagram contains only critical parts.

A block scheme of the TCS is shown in Fig. 4.2. The PCB module serves as mutual common part of all TCS units in a rack (up to 8 units). RCT modules are common for four

independent TCS units. The most complex unit is TCR, as this unit consists of several printed circuit boards. Description of the block model in Fig. 4.2:

- TCS – Track Circuit System.
- PCB[1] – Power and Circuit Breakers block represents power, circuit breakers, and other input ports of the equipment.
- RCT – Rectifier – these blocks are redundant and represent the next stage of power distribution and rectifiers.
- TCR – Track Circuit Receiver – these blocks are redundant (Two-out-of-Three redundancy – 2oo3 is used, see [42]) and they represent the most complex part of the whole system. This part consists of several sub-parts.
- PSB – Power Switch Board – this block represents power distribution within the TCS.
- CSB – Communication Switchboard – this block represents communication within the TCS.

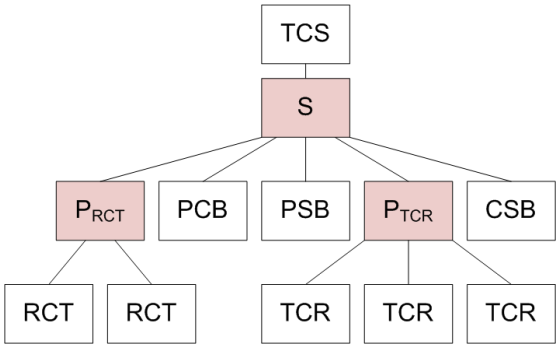

Figure 4.3: The hierarchical block diagram of TCS – level: n to $n-2$

The heterogeneous dependability model of the TCS is shown in Fig 4.3. All white blocks are the same as in Fig. 4.2. The red blocks are defined as:

- S – a serial system, failure of any module or unit (CSB, PCB, PSB, P_{RCT} and P_{TCR}) will cause the system failure.
- P_{RCT} – a classical parallel system of two identical units.

[1]PCB is usually used as an acronym for *Printed Circuit Board*. However, in this context, this abbreviation means *power supply unit and circuit breakers*. Most of modules contain printed circuit boards, but this module does not.

- P_{TCR} – 2oo3 system described by a Markov chain. This block has several attributes, (e.g., the repair rate – μ, failure rate of TCR – λ_{TCR}, maximum time to repair – $t_R = 80$ hours) and one rule in a form of a Markov chain 4.4.

Moreover, in this model the blocks contain additional hidden important attributes and rules. For example, the P_{RCT} block contains a Markov chain shown in Fig. 4.4.

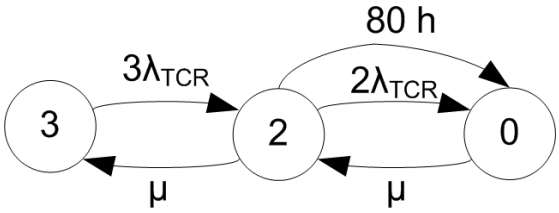

Figure 4.4: The Markov chain describes the degradation of computing modules TCRs.

4.1.3 Problems to Solve

This section is focused on problems which are not specified or solved in any standard. Nevertheless, they must be somehow solved. The track circuits system is a very complicated device, containing approximately 2 500 electronic parts. For each part it was necessary to predict a failure rate according to the standard. Even though I had a complete documentation of TCS, it was not always possible to determine each parameter (or a factor – defined in Section 2.6.1) according to the requirements of the standard. It means that some parameters for reliability calculation of a specific electronic part were unknown. In this case, I had to choose the most pessimistic value of the parameter from the offered options of standard. Therefore, I used both methods from the standard MIL-HDBK-217 the simpler one –*Parts Count* and the more advanced one – *Part Stress*, or I approximated or estimated an unknown parameter according to these other standards (FIDES, IEC TR 62380). I personally processed these key parts of the project:

Material Preparation

First, I had to collect all the data (electrical schemes, data-sheets of electronic parts, functional and non-functional requirements, internal directives, etc.) about the device. I created a Heterogeneous Dependability Model (see Chapter 3) of the whole TCS with respect to its system architecture. This step showed that Heterogeneous Dependability Model is a very effective tool for description of a system architecture with different conditions or rules.

Establishing Basic Assumptions

It was necessary to specify some parameters before the calculation of a failure rate of individual electronic parts, e.g., parts quality, operation environment, temperature.

These parameters are based on the standards used. However, I had to specify some others parameters or answer other questions, e.g.,

- How to replace faulty parts?
  Every faulty part is exchanged by a new one. Any fault does not cause a failure of a unit or a module. Certain faults may be not observed on the system functions, e.g. status diodes and their electronic accessories. Is it important to consider these parts?

- Is every fault permanent?
  All standards assume that every fault is permanent. This is one reason, why the used standard is very strict and pessimistic.

- Is the device continuously upgraded?
  Is the device improved or revised if a design deficiency is observed during real traffic.

- How to proceed if there is no or incomplete data?

  – No fault has occurred over 10 years of operation for some units.
  – Unintentional mistakes of maintenance process.
  – Different records of the same faults.

  Another interesting problem was specific custom-made or hand-made parts (little inductive parts, main transformers, relays). These parts are 100% reliable, and there are no fault records of such parts over 10 years of operation.

Fault Table and Operation Data

The observed devices have operated since 2006. The number of TCS deployed increased over time. With the increasing number of deployed systems, the number of operating hours (of the order of millions) and the number of different faults (of the order of hundreds) also increased. It was necessary to design an efficient observed data collecting and sorting system, for these observations. I created a fault table from the original service database. This database contains all records of operated devices, and initially it was not determined as a database for reliability purposes but only for maintenance (installation of new devices – date, time, location, number of devices). Each device has a specific identification code. The database also contains fault logs, related to specific devices. It was necessary to specify and to distinguish the types and origins of faults. The faults caused by the atmospheric effects (storms, lightning, floods etc.) could not be considered. I observed many records about transient faults in this database.

Comparison of the Results

A comparison of the results of analysis based on operation data and analysis based on the standard was done to choose a proper model. I used my proposed HDM (see Chaper 3) to be able to model the TCS system, including all conditions, rules, and requirements for its use.

The basic problem was to compare results obtained using different methods. The standard MIL-HDBK-217 provides two similar methods that are based on the same fundamentals and predicted failure rates from these methods were very similar. However, the results from the operating data were very different. The standard provides a failure rate – λ for each electronic part. Then, the failure rate of the whole system can be easily calculated. However, the observed operation data do not provide (or rarely when) information about specific parts. The observed data provided information about larger units or modules (PCB, RCT or components of TCR).

4.1.4 Predicting Failure Rate with Censored Data

The problem with incomplete observed data has led to the use of data censoring [56, 57]. The paper [A.5] shows an idea "how to get the maximum from using the censored data". A simple example "what is meant by censoring the observed data by time" is described here.

It was found that the resulting failure rate has decreasing trend from the observed data from 10 years of operation and using censoring. This decreasing tendency can be seen in Fig. 4.5. This can be caused by continuous devices recovery, when a fault was observed.

Then a method for nonparametric estimation from incomplete observation (*Kaplan-Meier estimate* [58]) has been used. We investigated the distribution of the observed data using this method. This estimate shown that the fault distribution describes *Log-normal* distribution the best, see in Fig. 4.6.

4.2 Eurobalise

4.2.1 Cooperation with Industry

I supervised a project in 2016 – 2017 that dealt with a predictive analysis of *Eurobalise*. Eurobalise or more simply *Balise* (it means "buoy" from French language) is a part of an *European Train Control System* – ETCS. The project had followed-up to a successful previous cooperation between our university and the AŽD Praha company. The project had the character of a contractual research. This ("contractual research") project gave me the opportunity to analyse real equipment. The output from this project were two reports:

- *Detailed technical report*
  This report designated for AŽD development department is a "business secret", and it contains outputs of the project, in the form of required information – failure rates, description of critical locations, and recommendations to improve the reliability.

- *Comprehensive research report*
  This report contains a general description of the equipment, the used methodology, the reliability models, and the performed assumptions. This report is publicly ac-

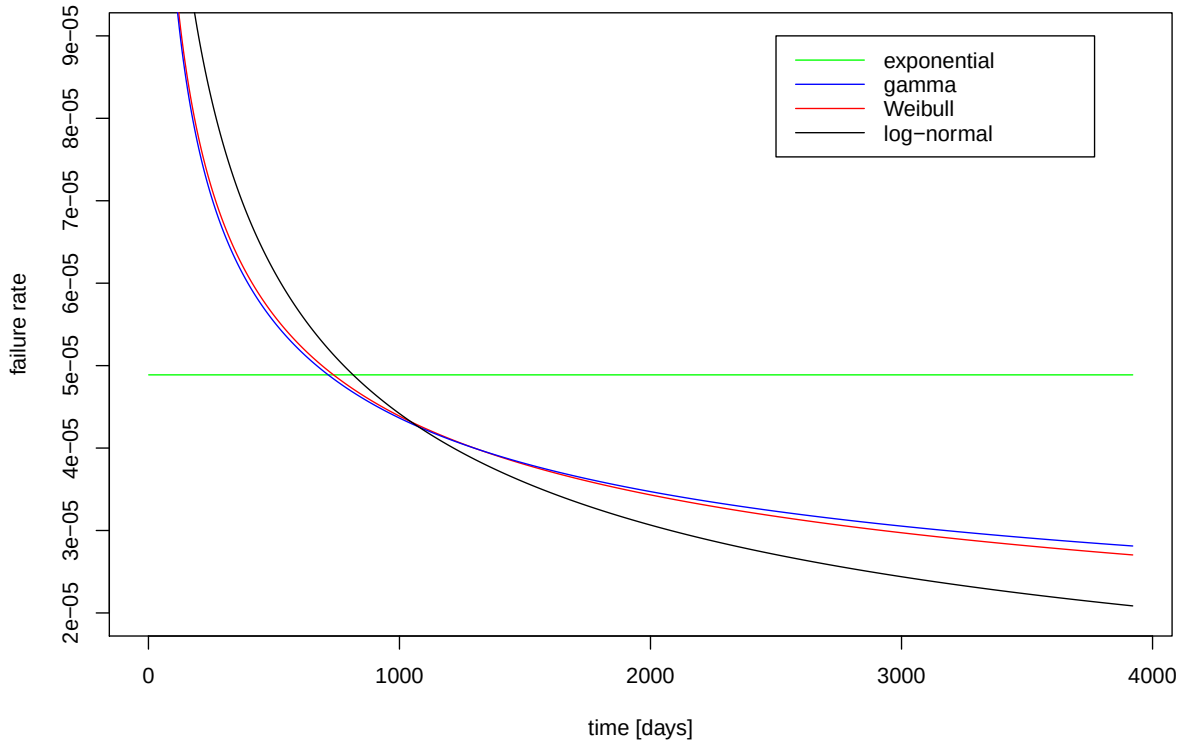

Figure 4.5: Estimated parametric failure rate for TCR only. This graph suggests that this could be the beginning of the bathtube curve. This figure is taken from [A.5].

cessible and does not contain specific numerical values and results (predicted dependability parameters like MTBF) [A.15].

The first report serves only for business and development purposes. However, some important aspects of the calculations and assumptions are included in this section.

4.2.2 Description of the Equipment

The function and placement of Balise is shown in Fig. 4.7. The device has a telegram (data packet) stored. The telegram contains information, like where on the track the train is, speed restriction, or other constraints for the train. A passing train exposes the device to the electromagnetic field. This causes that the device charges and starts working (Balise does not have its own power source). It means that Balise sends a telegram to a train. This action takes a few dozens microseconds – [μs]. The Balise is not classified as a safety critical

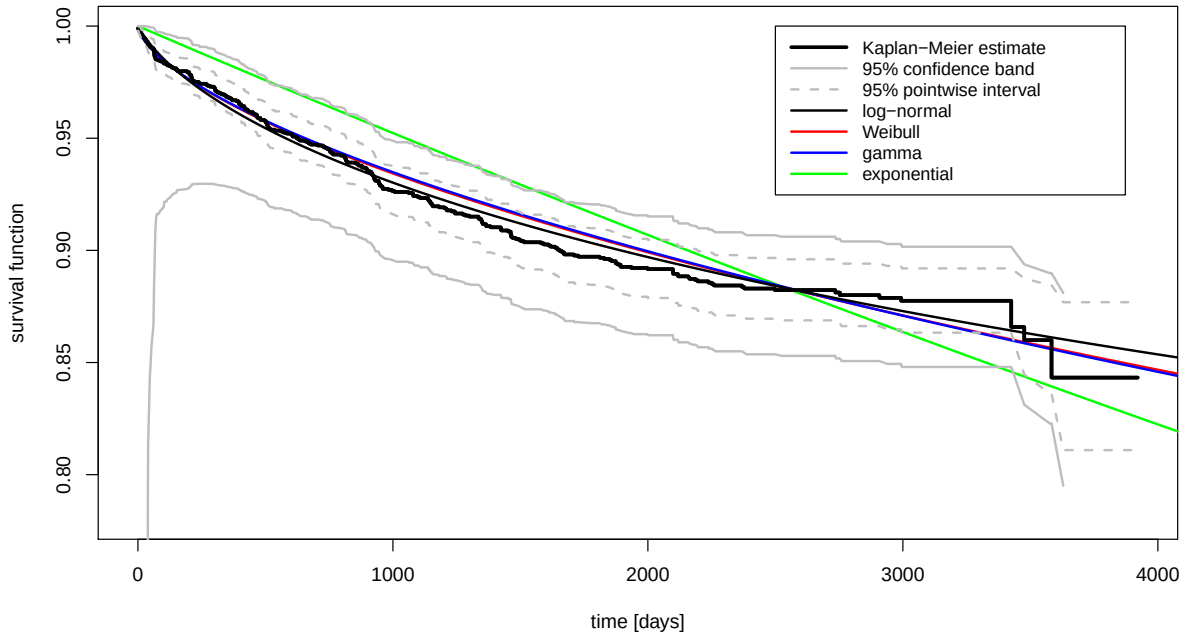

Figure 4.6: The result of Kaplan-Meier estimate of the reliability (survival) function for TCR only.

system such as track circuits. However, there may be a risk of derailing or colliding trains if more than several Balises in a row do not work. The *mission time* of this equipment is planned for 30 years.

The device consists of one printed circuit board. This board contains about 500 electronic parts and the whole system is embedded in an epoxy resin. The Balise failure is addressed by replacing it. In other words, the Balise is not developed as a renewable equipment. It is because of the resin.

4.2.3 Problems to Solve

The analysis of this device was a bit different because I could directly influence its design and development. Two versions of Balise have been created during the project ABA-12 [A.15]. The goal was not only to improve the reliability and availability but also to reduce the price of the product.

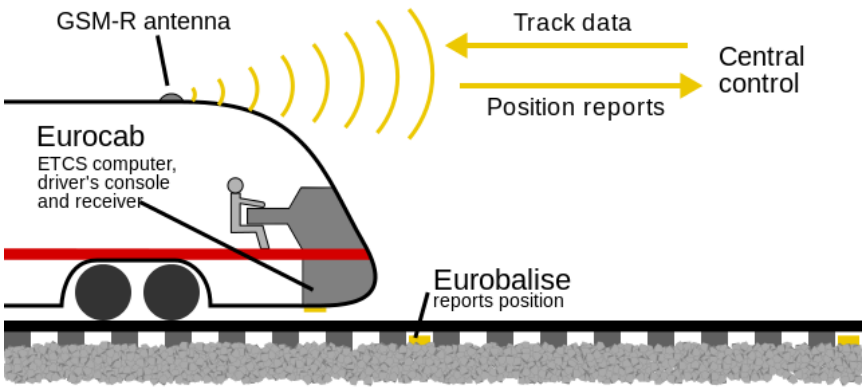

Figure 4.7: Placement of Balises. The Balise will send a telegram to the train. (European Train Control System – ETCS Level 3 schematic, taken from [12]).

Approaches to increase system-level reliability:

- System redundancy
  Two Balises always work side by side, such as in Fig. 4.7.
- A telegram contains information redundancy – CRC.
- Balise can use a temporal redundancy.
  A Balise unit is the computing module and the passing train contains a voter.

These approaches, mentioned above, are based directly on the definition of Balise requirements [12].

Approaches to increase component-level reliability:

- Increasing the quality of the used electronic parts. The technical report IEC TR 62380 has been used in the development and for reliability prediction, to predict a failure rate of the particular part.
- All parts have to work at a maximum of 50% of their rated power. It means that for their "Power Stress" (S) holds

  $$S = \frac{ActualPowerDissipation}{RatedPower}$$

  where

  $$S < 0.5$$

- Improving current design based on reliability analysis of the previous version of this device.

Alternate operation

Balise has a different use than the track circuits system. Balise is in off-mode in most of its mission time. Balise works only if some train passes above it. Total real operating time from the required mission time (30 years) may be less than one month. Consider the following hypothesis:

- A regular track with a frequency of 100 train passes per day.
- The assumption is that each day of the week is working day (no weekends and no holidays).
- One pass over the device takes 1 [s].
- Balise works for 100 [s] per one day, 700 [s] per week, 36 500 [s] per year and 1 095 000 [s] per 30 years.
- Balise has worked about 13 days in total in 30 years of operation.

The used standard MIL-HDBK-217 does not take this situation into account.

Different operation environment

The used standard allows choosing only one specific operating environment that holds on for whole mission time. This fact proved very restrictive, e.g.,

- Vibrations – the used standard does not consider the vibrations caused by "only" the passage of the train.
- Temperature range – the used standard cannot work with a temperature lower than 0° [C], and it does not even consider the changing of seasons.

These mentioned problems have helped to resolve the use of other standards, e.g. FIDES [15] or HDBK-217 [59] and also earlier experiences from the KOA project [A.14].

Comparing the results with another Eurobalises

The AŽD company is not the only company that manufactures this equipment. This equipment is manufactured by several other producers, e.g., Alstom, Ansaldo STS, Bombardier, Invensys, Siemens, Sigma-Digitek and Thales. Most of these companies use the availability instead of the MTBF parameter. If the MTBF parameter can be found, it is usually about 30 years (including various operating conditions). The Siemens company specifies the MTBF parameter that is calculated according to their own specific standard SN 29500 [60]. The MTBF parameter value is hardly to believable 800 years for a fixed type of Balise [61].

4.3 Summary

Both types of equipment (Balise and Track Circuit Systems) were developed by the same company and contained the same or very similar electronic parts. The same output reports were requested in the form of predictive analysis of dependability parameters. These analyses had been performed according to the same methodology – MIL-HDBK-217. The primary difference was that the second project (ABA-12) had no operating data. This was because they were the first prototypes to be deployed. This project was simpler than first one (KOA), in terms of the number of electronic parts. However, the research has shown that using of the required standard is not sufficient, see the problems above. Comparing the results with other manufacturers, on the contrary, showed that it is not possible to compare the MTBF parameter according to different methodologies.

The question again arises "Isn't the time to rethink it?" [34] What does this MTBF parameter say [62], if I do not know the assumptions under which the reliability calculation was performed? In my opinion, it is difficult to express the reliability of today's devices according to one parameter.

The most interesting problem for this dissertation thesis was discovery of the possible occurrence of transient faults. Problems with transient faults were observed in both projects. However, both projects have some type of redundancy, that could avoid negative effects caused by transient faults. The next Chapter 5 deals with predicting and modelling of the reliability of systems (mentioned above) with transient faults considered.

Chapter 5

Modelling the Effect of Common Transient Faults

This chapter describes the idea: "How to create a reliability model of a system with considered effects of transient faults? "In Chapter 2, methods for predicting reliability are mentioned. All these methods and industrial or military standards have one thing in common – they assume permanent faults only. The previous Chapter 4 describes two case studies [A.14, A.15] for different equipment, where transient fault effects have been observed. Both devices can be protected by different types of redundancy. In case of Track Circuit Systems, it is spatial, respectively triple modular redundancy, and in case of Balise, it is temporal redundancy. This section aims to show how the transient faults influence the reliability prediction using the Markov chains. The proposed methods have been published in this article [A.3] and these papers [A.2, A.6, A.10, A.16], the last one is enclosed in App. C.

5.1 Consideration of Transient Faults

The track circuit system uses spatial redundancy at several levels (duplex for power distribution and rectifiers and Triple Modular Redundancy (TMR) for track circuit receivers, see in 4). Track circuit receivers are very complex units, which contain diagnosis modules. In case of a fault, the system shuts down the faulty unit, and the diagnosis module records a report about the fault. The system runs in degraded mode, and maintenance intervention is necessary. However, if it has been affected by a transient fault only, the unit is not physically faulty. Nevertheless, the current system requires maintenance intervention (see Section 4.1).

The problem of dependability prediction with regards to transient faults is solved, see [42, 52, 53]. However, it is complicated to determine the failure rate – λ of specific

transient faults. Unfortunately, all sources mentioned above assume a knowledge of some repair rate – μ of these transient faults. This section aims to show the possible influence of transient faults in dependability prediction. The proposed method can be used for more extensive systems such as Track Circuit Systems or small systems that fit into one FPGA.

5.1.1 Transient Faults Modes

For purposes of this thesis, only two modes of transient faults will be distinguished, critical and non-critical. These modes of transient faults are shown in Fig. 5.1. The problem is not the transient fault itself, or its origin (a noise, radiation etc.). Their problem are possible negative effects on a critical part of a calculation. Information about the frequency of transient faults is available from previous case studies [A.14, A.15]. Sometimes, the duration of the particular transient fault has also been detected.

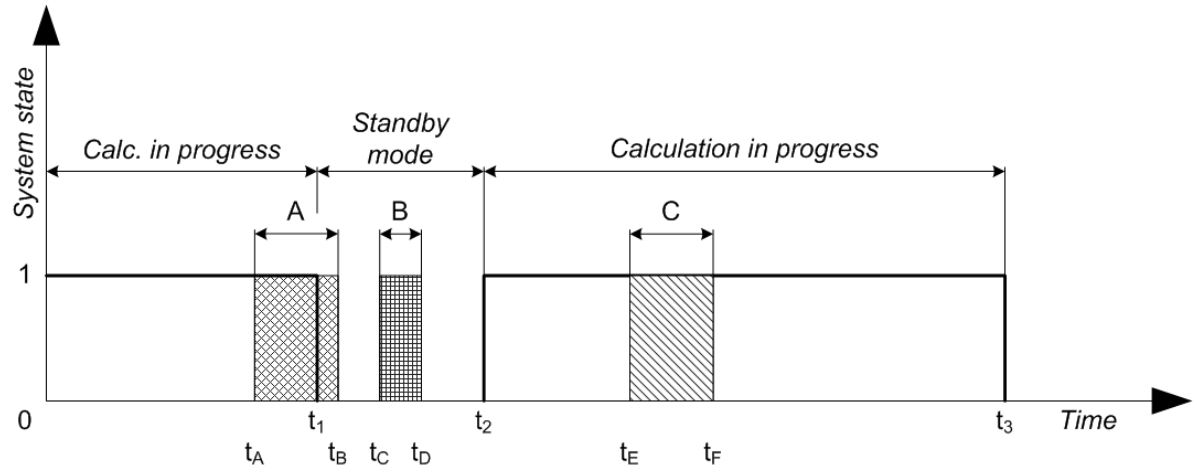

Figure 5.1: Modes of transient faults. The faults "A" and "C" are critical and fault "B" is non-critical.

Different modes of transient faults can occur during system operation. In general, two states of a calculation or a system can be distinguished. These states are indicated by the y axis, the *time* is on the x axis:

- State 0 – the non-critical phase of a calculation is in progress, or the system is temporarily off.
- State 1 – the system is on and the critical phase of calculation is in progress.

Transient faults can negatively affect only the system that is in operation, and only if the system performs a calculation, or if the system performs a critical part of calculation. Fig. 5.1 shows three independent transient faults, each of them has a different duration. Each of them can be observed in different parts of the calculation.

- Transient fault A occurred in an interval $(t_A - t_B)$, this fault is critical.

- Transient fault B occurred in an interval $(t_C - t_D)$, this fault is non-critical.
- Transient fault C occurred in an interval $(t_E - t_F)$, this fault is critical.

The calculation needs not take the same amount of time. Fig. 5.1 shows three differently long operation stages of a system.

- Interval $(0 - t_1)$ means a critical part of calculation.
- Interval $(t_1 - t_2)$ means a non-critical part of calculation.
- Interval $(t_2 - t_3)$ means a critical part of calculation.

For the next text in this thesis, it is assumed that the duration of a transient fault will not be longer than any stage of the critical or non-critical parts of the calculation. If the duration of a transient fault is longer than any stage of calculation, it can be considered a permanent fault, because it can also affect another part of the calculation. In case of Track circuit system would be faulty unit disconnected and deactivated (see Section 4.1).

5.2 Modelling Transient Faults in Spatial Redundancy

In the area of reliability and security, TMR is used to mask faults. Fig. 5.2 shows a block diagram of an embedded system. Implementation of the mentioned system is based on FPGA. The diagram consists of three equal modules and a simple voter. It is assumed that the voter is more than hundred times smaller than the module.

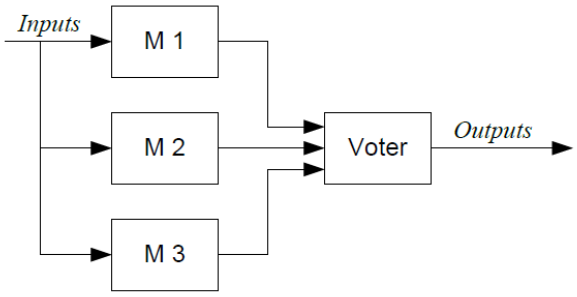

Figure 5.2: The TMR consists of three equal modules (Module 1, Module 2 and Module 3) and a simple voter.

The state diagram (Figure 5.3) represents a Markov chain of the mentioned equipment. It is consisted of three modules and a voter. The voter is based on the majority function. This is a classical Markov chain that describes the behavior of TMR in terms of reliability.

Description of the Markov chain in Fig. 5.3:

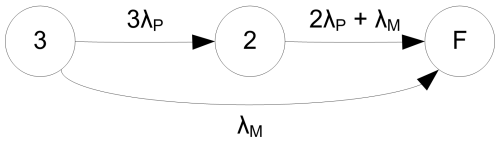

Figure 5.3: A simple Markov chain with absorbing state representing the TMR behavior.

- State 3 means that everything is alright. All three modules and voter are functional.
- State 2 means that one of the three modules is faulty.
- State F describes the (fatal) state where the system is no longer able to produce correct result (two out of three modules or the voter are faulty).
- λ_P – failure rate of any module.
- λ_M – failure rate of the voter.

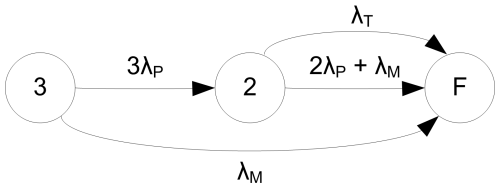

Figure 5.4: A simple Markov chain with transient faults effect.

The reliability model shown in Fig. 5.4 is not suitable for modelling transient faults. In general, the system has critical and non-critical phases of execution, see Fig. 5.1. The effect of a transient fault can be observed only during the critical phase.The difference between the Markov models described in Fig. 5.3 and Fig. 5.4 is that the second one (Fig. 5.4) is designed to model also the transient faults. The meaning of the states is identical to the previous model; the added edge leading from the state 2 to the state F describes the transient fault (λ_T). This fault can be modelled only in the state 2. Transient faults occurring in state 3 are not considered, because they are repaired automatically.

Fig. 5.5 describes two time-dependent stages of the mentioned system. The t axis describes the operational time; the S axis describes the stage (i.e., critical/non-critical stage of the operation labeled C and N). The critical stage has an average period of t_C and the non-critical stage (or inactivity of circuit) has an average period of t_N. This proposed approach is applicable only if all critical periods represented by t_{C1}, t_{C2} $\ldots t_{Cn}$ have the same or similar lengths. If the average time (e.g., t_C and t_N) is known, it is possible to determine the mean frequencies (α_C, α_N).

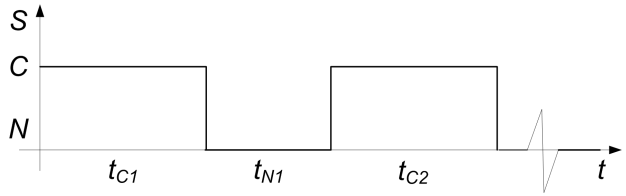

Figure 5.5: The system works periodically. The y-axis (S) indicates two stages of the system – C is the critical part of the calculation and N is the non-critical part. The x-axis (t) represents the time.

$$\alpha_C = \frac{1}{t_C}$$

$$\alpha_N = \frac{1}{t_N}$$

- α_C – represents the mean frequency of the critical part.
- α_N – represents the mean frequency of the non-critical part.

A more precise dependability prediction of the TMR has been achieved by including the periodicity of the calculation (see Fig. 5.5) and by including the effect of transient faults.

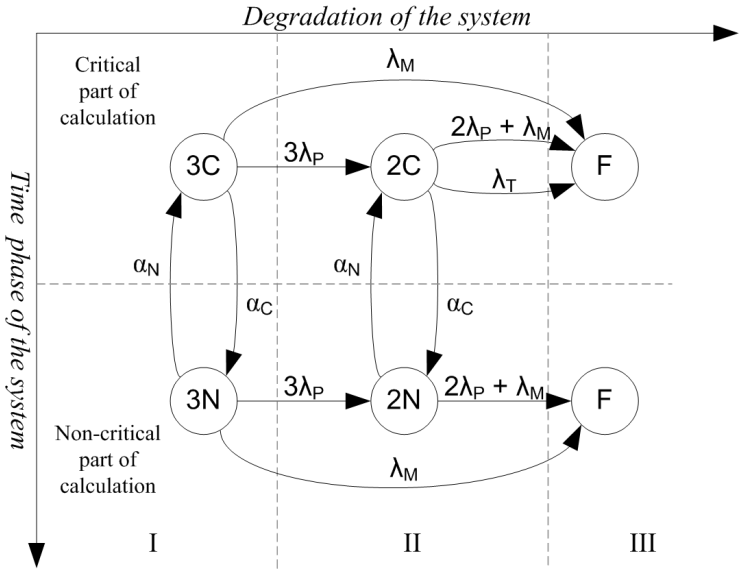

Figure 5.6: Detail of the extended Markov TMR (two stage TMR) model representing permanent and transient faults during the critical and non-critical phases of the execution.

The proposed extended Markov model of the mentioned system, shown in Fig. 5.6 in the form of 2-D grid, respects the two stages and respects the permanent and transient faults. In this case study the model is divided into the horizontal and vertical axes. The horizontal axis describes "the level of the system degradation" and the vertical axis describes "the level of the system stage activities".

- State $3C$ means that everything is alright. All the modules and the voter are functional in the stage of the critical calculation.
- State $3N$ means that everything is alright. All the modules and the voter are functional in the stage of the non-critical calculation.
- State $2C$ means that one of the three modules is faulty in the stage of the critical calculation.
- State $2N$ means that one of the three modules is faulty in the stage of the non-critical calculation.
- States F_C and F_{NC} mean that the system has failed (two out of the three modules or the voter is faulty), as both F_C and F_{NC} states lead to system failure.
- λ_P – permanent failure rate.
- λ_T – transient failure rate.
- λ_M – failure rate of the voter.

5.2.1 Conditions and Numerical Solutions

These mentioned parameters are merely illustrative. They reflect the experience from the field of dependability prediction of the train infrastructure safety systems [A.14, A.15]. The time length of the critical and non-critical calculation is approx. 25 $[ms]$ and 50 $[ms]$, respectively. The desired reliability parameters are the failure rates of the whole system respectively the Mean Time To Failure (MTTF), and the function $R(t)$.

$$\lambda_P = 3.4 \times 10^{-6}[h^{-1}]$$

$$\lambda_T = 2.9 \times 10^{-6}[h^{-1}]$$

$$\lambda_M = 6.8 \times 10^{-7}[h^{-1}]$$

$$\alpha_C = 144\ 000[h^{-1}]$$

$$\alpha_N = 72\ 000[h^{-1}]$$

Fig. 5.7 shows that the curves of the Classical TMR (blue dashed curve) and Extended TMR (red dotted curve) create the borders for two stage TMR (green curve). The blue

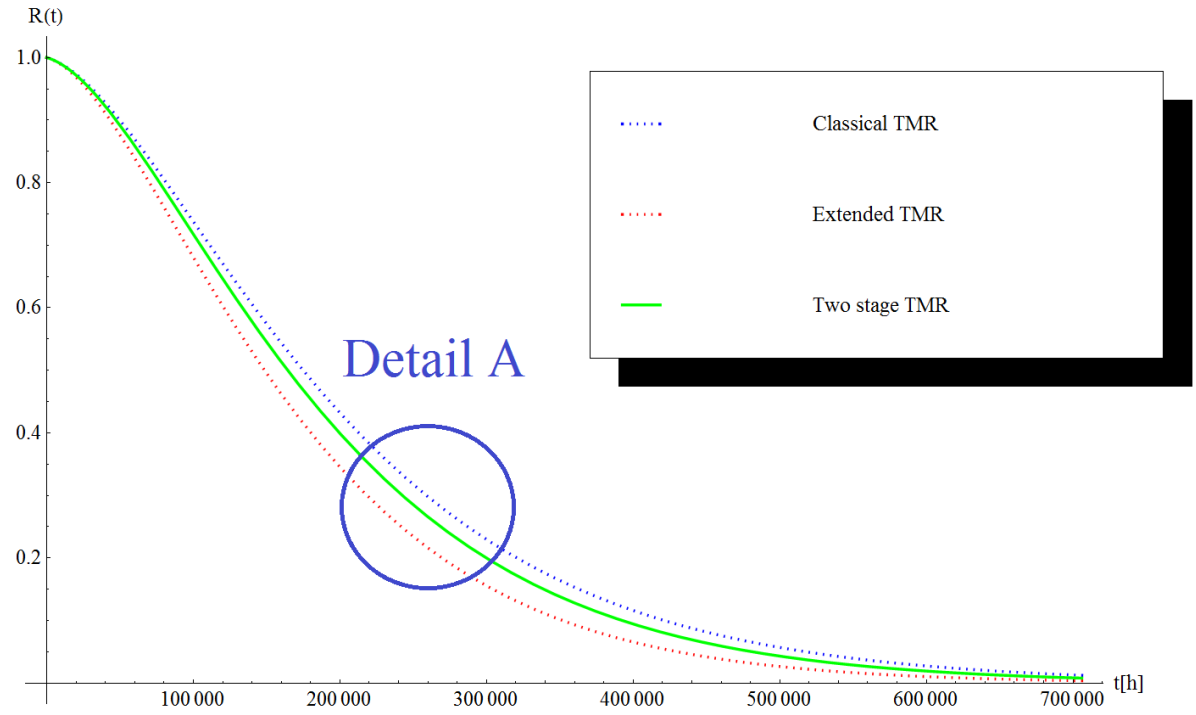

Figure 5.7: Comparison of the Markov models. Classical TMR is described in Fig. 5.3, Extended TMR is described in Fig. 5.4 and Two stage TMR is described in Fig. 5.6. The axis $R(t)$ is the reliability function and the axis t is time in hours. The graph was generated using Wolfram Mathematica [50].

curve is the best case and the red curve is the worst case of the reliability of the mentioned system.

The detail A of Fig. 5.7 is described in Fig. 5.8. The distance between the dashed and doted curve depends on the magnitude of the transient faults rate. The ratio of the values – α_C, α_N affects the position of the curve between the borders from the Classical TMR and Extended TMR. If α_C is greater than α_N, then the green curve gets closer to the doted red curve.

Markov models are valid assuming an exponential probability distribution of the time "in the appropriate even" (transition). This is acceptable for the permanent or transient faults (i.e., λ_P, λ_M, λ_T), but not for the events representing the termination stage activities (α_C, α_N). The model can be more accurate (in case of need) if every stage will be divided into sub-stages. Further details can be found in [63].

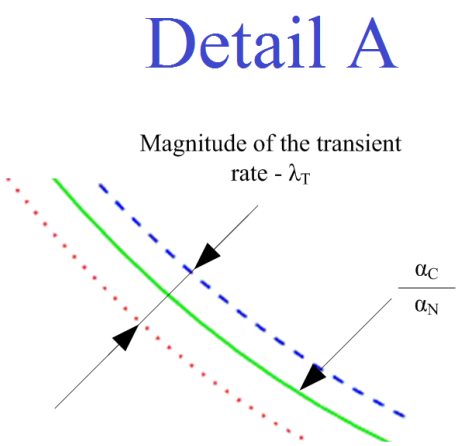

Figure 5.8: The detail A of Figure 5.7. The middle curve represents the Reliability function of the two-phases Markov chain (Two stage TMR).

5.3 Transient Faults Modelling in Temporal Redundancy

The basic operation of the temporal redundancy is shown in Fig. 5.9. There is only one module present, thus there is no area penalty. The temporal redundancy executes the operation of the module multiple times in order to eliminate the negative effect of transient faults. As the calculation proceeds, the intermediate result (e.g., the output of the module after its operation is finished) is stored in memory. After all the intermediate results are collected, the final output is voted upon, using the majority function. This mechanism allows to mask the negative effect of a transient fault in case its effect has a negative impact on operation of the module during one of the cycles. In case the majority of the cycles is affected by the negative effect of the transient fault or in case a permanent fault, the system as a whole leads to a failure.

If the average time (e.g., t_C and t_N) is known, it is possible to determine the mean frequencies (α_C, α_N).

$$\alpha_C = \frac{1}{t_C} = \frac{1}{t_{C_1}} + \frac{1}{t_{C_2}} + \frac{1}{t_{C_3}}$$

$$\alpha_N = \frac{1}{t_N}$$

- α_C – represents the mean frequency of the critical part.
- α_N – represents the mean frequency of the non-critical part.

Fig. 5.10 describes two time-dependent stages of the mentioned system. The t axis describes the operational time; the S axis describes the stage (e.g., critical/non-critical

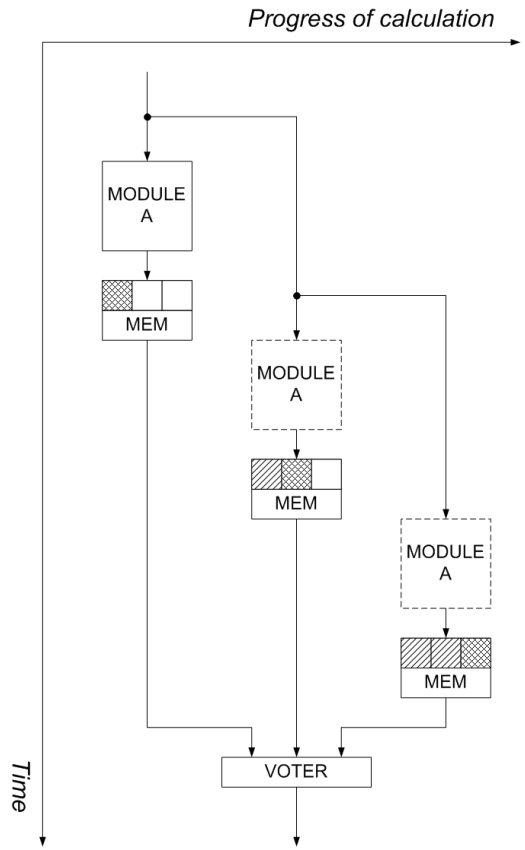

Figure 5.9: Temporal redundancy utilizes one operational module and executes the operation multiple times. In this example the operation is executed three times and every intermediate result is stored in memory. The output is finally voted using the majority function and the intermediate results.

stage of the operation labeled C and N). The critical stage has an average period of t_C, its subparts $(t_{C_1}, t_{C_2}, t_{C_3})$ respectively, and the non-critical stage (or inactivity of circuit) has an average period of t_N. This proposed solution is applicable only if all the periods represented by $(t_{C_1}, t_{C_2}, t_{C_3})$ have the same or similar length. It is assumed that the critical (respectively non-critical) calculation takes roughly the same time.

Fig. 5.11 describes the Markov chain model involving permanent faults only and the periodical behaviour (Fig. 5.10) as described in Section 5.2. States 1-3 belong to the set of states that are executed during the critical part of execution. This represents the duty cycle where the number of states represents the number of repetitions due to the implementation of the temporal redundancy. The remaining state N belongs to the non-critical part (e.g., the system is idle). Also α_C represents the transitions during the critical part of the execution while α_N represents the transitions during the non-critical part of execution. The permanent failure rate λ_P transitions lead to system failure (state F) in case a permanent fault is observed in any state.

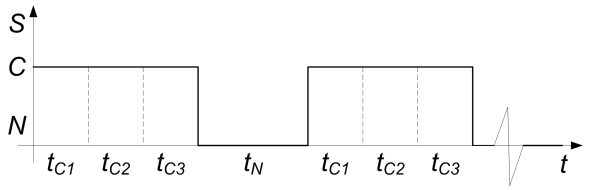

Figure 5.10: The system works periodically. The axis S represents two stages of the system, C is the critical part of the calculation and N is the non-critical part. The axis t represents time.

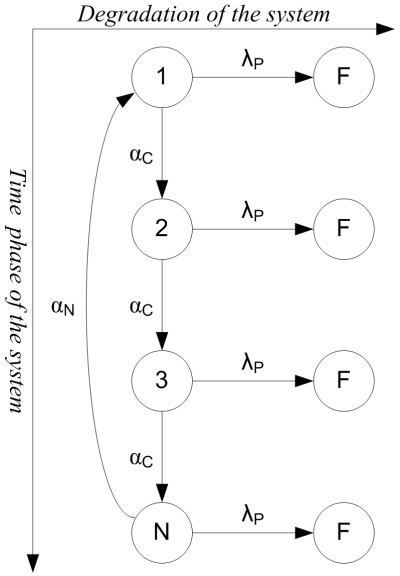

Figure 5.11: Basic Markov chain model for dependability prediction involving only permanent faults.

To summarize the description of the model (Fig. 5.11):

- States $1-3$ mean all the modules and the voter are functional in one of the three stages of the critical calculation.
- State N means that everything is alright. The module and the voter are functional in the stage of the non-critical calculation.
- States F mean that the system has failed. The module or the voter is faulty. Each state F leads to system failure.
- λ_P – permanent failure rate λ_M – permanent failure of the voter is included.
- α_C – represents the frequency of the critical part (the transition between critical parts of the system).

- α_N – represents the frequency of the non-critical part.

In previous Section 5.2 the parameter λ_M (failure rate of the voter) was included. In this case the parameter is not included in the model as it can be easily merged with the permanent failure rate λ_P.

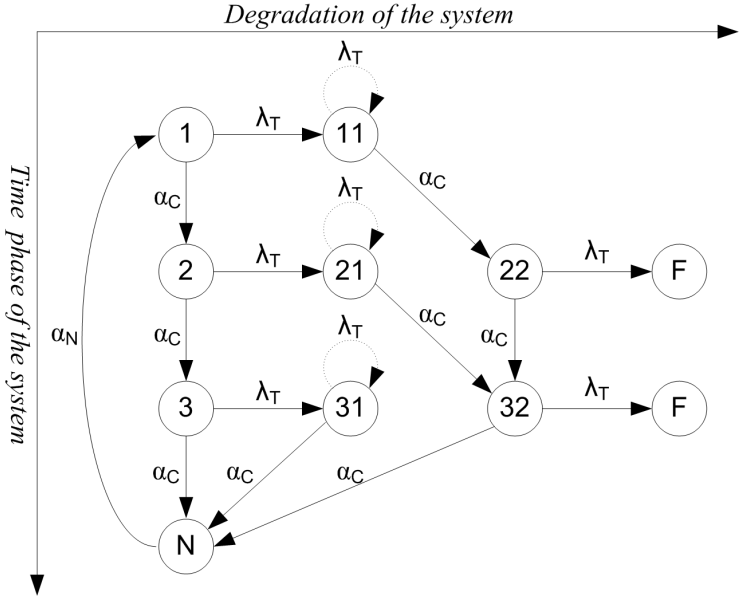

Figure 5.12: Markov chain model involving only transient faults.

Fig. 5.12 describes the initial Markov chain model including the λ_T parameter (i.e., the transient faults rate). States 11, 21 and 31 represent the states of degradation which means that a transient fault has been observed. Here more transient faults can occur but as the result is already faulty, any other transient fault does not have a negative impact on the output, as it is already considered to be invalid. States 22 and 32 represent next stage during the execution after a degradation has been detected. The result is a system failure in case another transient fault occurs in these states. In case of no transient fault observed, the calculation can end up successfully, as there will be a majority of valid intermediate results, thus the negative effect of the transient fault will be masked.

The Markov chains described in Fig. 5.12 can be further reduced. After the majority of valid results is obtained, the need to check for other transient faults is no longer necessary. The state 31 can be merged with state 3. The final model involving only transient faults is shown in Fig. 5.13.

As it was stated before, it is assumed that the observable effect of the transient fault is significantly lower than the operation cycle of the equipment. This means that the effect of one transient fault is not observed after the transition to the next state. This phenomenon

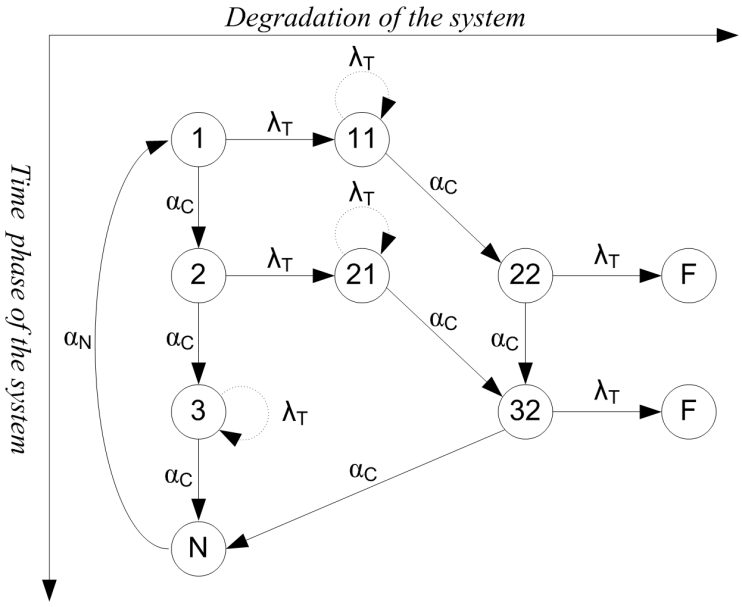

Figure 5.13: Simplified/reduced Markov chain model involving only transient faults.

would be considered as a permanent fault and would lead directly to system failure.

The described model considering only permanent faults (Fig. 5.11) and the model considering only transient faults (Fig. 5.13) were merged. Every state has a transition λ_P to a state F describing the system failure after the permanent fault has been observed. The final model is shown in Fig. 5.14.

To summarize the description of the models in Fig. 5.12, 5.13 and 5.14:

- States $1 - 3$ mean that all the modules and the voter are functional in one of the three stages of the critical calculation.
- States 11, 21, 31 mean that all the modules and the voter are functional, but transient fault(s) has been observed in one of the three stages of the critical calculation.
- States 22, 32 mean that all the modules and the voter are functional, but transient fault(s) has been observed in some previous stage of the critical calculation.
- State N means that everything is alright. The module and the voter are functional in the stage of the non-critical calculation.
- States F mean that the system has failed. The module or the voter is faulty. Each state F leads to system failure.
- λ_P – permanent failure rate λ_M – permanent failure of the voter is included.
- λ_T – transient failure rate.

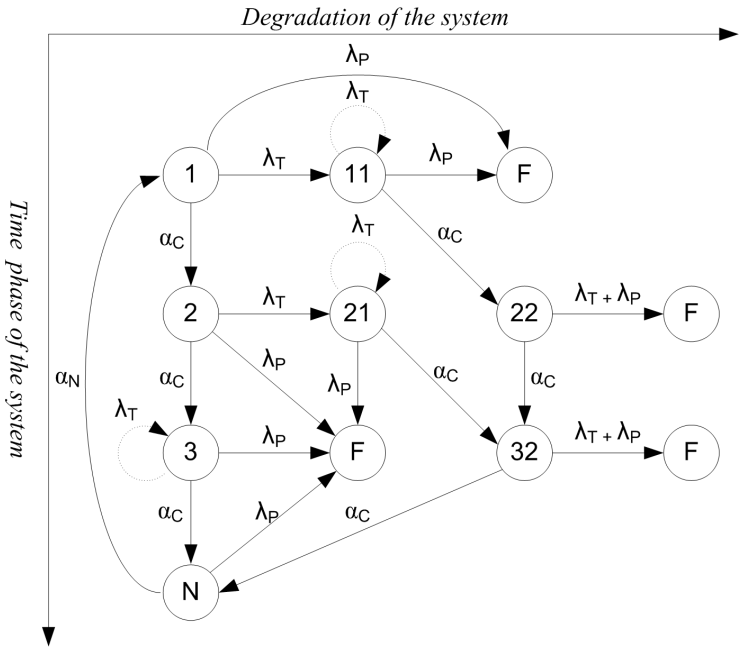

Figure 5.14: Final Markov chain model modelling the temporal redundancy considering both the stuck-at faults the the transient faults.

- α_C – means the frequency of the critical part (the transition between critical parts of the system).
- α_N – means the frequency of the non-critical part.

5.3.1 Conditions and Numerical Solutions

The numerical solutions refer to the previous Section 5.2.

$$\lambda_P = 3.4 \times 10^{-6}[h^{-1}]$$
$$\lambda_T = 2.9 \times 10^{-6}[h^{-1}]$$
$$\lambda_M = 6.8 \times 10^{-7}[h^{-1}]$$
$$\alpha_C = 144\ 000[h^{-1}]$$
$$\alpha_N = 72\ 000[h^{-1}]$$

Table 5.1 shows the MTTF values for the dependency of the transient failure rate (λ_T) on the permanent failure rate. This table was proposed in order to find the threshold where the λ_T parameter would start to have an impact to the actual MTTF values. As it is visible from the table, the values between 10^{-4} and 10^3 do not have any impact to the actual MTTF value. More significant changes to the MTTF values become visible when the the λ_T value is approx. four times greater than the λ_P. This is due to the fact that

the temporal redundancy is not resilient enough to the effect of a permanent fault that can occur in every state of the model (Fig. 5.14).

Table 5.1: Mean Time to Failure – MTTF values for the dependency of the transient failure rate (λ_T) on the permanent failure rate. (λ_P).

$k = \lambda_T/\lambda_P$	MTTF
10^{-4}	294 118
10^{-3}	294 178
10^{-2}	294 118
10^{-1}	294 188
10^{0}	294 118
10^{1}	294 118
10^{2}	294 118
10^{3}	294 114
10^{4}	293 701
10^{5}	257 622
10^{6}	187 736
10^{7}	129 284
10^{8}	64 761
10^{9}	37 036
10^{10}	207

Fig. 5.15 shows different results of the reliability function of the same system (Fig. 5.14). The resulting plot shows how the increasing transient failure rate λ_T can influence the reliability function.

On the other hand, the proposed model involving temporal redundancy is resilient to transient faults during the critical stages of the computation. This means that the transient failure rate λ_T must be significantly greater than the permanent fault rate in order to cause the system failure.

5.4 Summary

A new point of view on the interpretation of Markov chains used to predict the fault tolerant systems reliability parameters was proposed, in contrast to the traditional approach, where only permanent faults models were involved in the fault prediction.

Originally the transient faults were not included in dependability prediction of complex (safety-critical) systems – e.g., systems that need to guarantee a certain level of dependability. The reliability standards cannot take transient faults into account. Their failure rate and their duration is not known. These faults can occur based on environmental noise, the

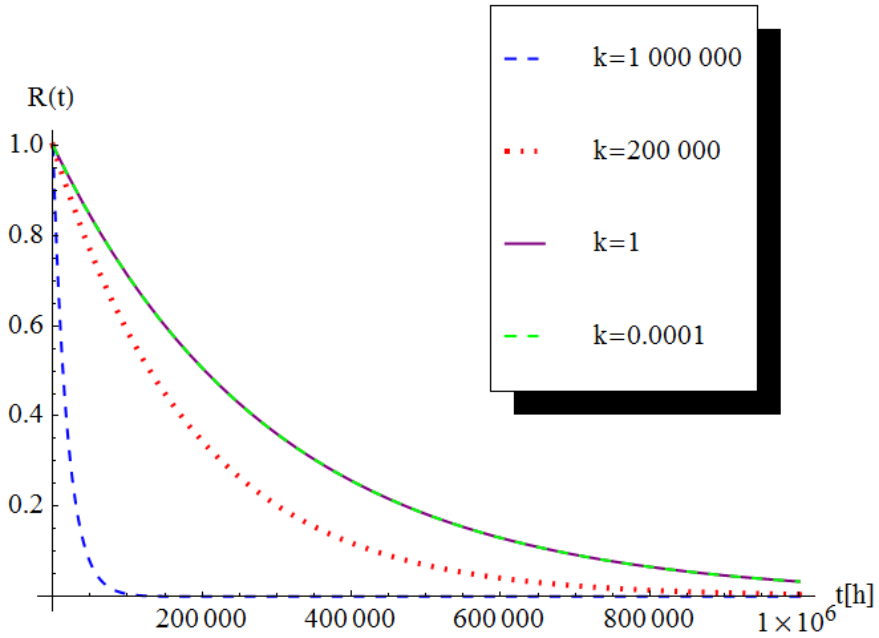

Figure 5.15: Comparison of different λ_T values used to calculate the reliability function of the proposed model in Fig. 5.14. Curves for $k > 10^3$ show a reliability prediction of a system where the transient failure rate λ_T is much higher than the permanent failure rate λ_P. The remaining curves on the other hand represent a reliability prediction for a system where the permanent failure rate λ_P is dominant. The graph was generated using Wolfram Mathematica [50].

overload stress of some parts, ionising radiation, etc.

For the purpose of this thesis, the assumption also includes the duration of the negative effect of transient faults. Safety-critical systems usually operate in an environment where the probability of fault occurrence is high [6]. For that purpose, the design of such systems include some form of redundancy (area/temporal/information) in order to detect and possibly mask the negative effect of permanent or transient faults. Due to the safety reasons, these systems also operate at low frequencies. This approach is time-proven and the system is then more resistant to faults generated by the hazardous environment [2]. For this reason it is assumed that the observable effect of transient faults is significantly lower than the operation cycle of the equipment.

Spatial Redundancy

The goal of this approach is to predict the dependability of complex systems that need to guarantee a certain level of dependability (safety-critical systems) including the effect of transient faults. The more precise the calculation is, the more accurate the dependability prediction can be. The resulting parameters of the prediction might be unnecessarily

pessimistic in case the Markov model does not take into account the periodic behaviour of the system. This would result in degradation of the guaranteed level of dependability. At the same time, a procedure to design a Markov model for a general fault-tolerant system consisting of n-redundant blocks and m-phases of execution has been shown.
The extended version of the proposed method is in App. *The Effect of the Transient Faults in Dependability Prediction* C. The enclosed article [A.3] contains a comparison with a similar method [52, 53] based on the knowledge of the repair rate – μ.

Temporal Redundancy

A basic example of a Markov chain model involving temporal redundancy has been proposed. This model takes the effect of both stuck-at and transient faults into consideration. The reliability function has been calculated using numerical values from the previous work. Multiple values of the transient failure rate λ_T have been proposed. The effect of these values on the resulting reliability function has been shown and discussed.

It is apparent from the presented results, that the proposed model is resilient to transient faults. In another words, the effect of transient faults can be neglected in case the transient failure rate $\lambda_T < 10^3 \times \lambda_P$.

Experimental results suggest that the state 3 shown in Fig. 5.14 is not necessary and might be removed from the model. This would lead to a duplex system architecture. The operation would be recalculated only in case the intermediate results do not match. This proposal might have the same results as the solution proposed in this paper and it will be considered for a future work in this research.

Chapter 6

Conclusions

6.1 Summary

This dissertation thesis is aimed at dependability issues: the methods for reliability, availability, and safety properties predictions. Valuable and usable results could have been obtained only due to construction of many real models and dependability computations based on real data obtained from industrial equipments during several years of their operation. A series of unreported or unresolved issues was encountered during the solving of these practical problems. This thesis tries to answer some of them (you can see their list in Section 1.2).

For successful answering these questions defined in Section 1.2 I was forced to study a lot; especially case studies with real equipment, real data and real problems have brought me important and interesting ideas. I had to go back in history, to understand the fundamentals of reliability. I noticed a simple relationship during my study. With the increasing complexity of the systems, the need to improve their reliability has grown. The important development milestones in the field of dependability (only from my point of view) are described in Section 2.1. If there was a problem of reliability, its solution has emerged within a certain period of time (about 10 years). It is interesting, that after 2000, when the complexity of systems began to grow sharply, techniques and methods from the 1980s and 1990s have been still used without major changes. Over time, reliability standards and handbooks were written to help to predict the reliability. Nowadays, there are countless different reliability standards, all of them are derived from the first one MIL-HDBK-217.

It was not in my power to study and compare all these standards (there are more than 30 standards of reliability in the Czech Republic only), therefore I started from historically the most used and world-recognized standards.

The real problems with using today standards, sometimes unclear terminology, and several experiments and case studies descriptions are presented [A.4].

Moreover, two important problems should be solved:

- *Transient faults* – reliability standards from their own nature cannot predict a system failure based on transient faults. The failure rate of transient faults is defined for no electronic part, because it is related to the operation environment, interactions between systems, and other dependencies.
- *Basic reliability models* – the standards cannot work with more complex or hierarchical models. The fault models of individual electronic parts are very complex, but the reliability model of the whole system is generally assumed to be serial.

The methods to overcome these shortcomings are presented in Chapter 3, whereas the Heterogeneous Dependability Model is presented in Chapter 5 with two papers that incorporate transient faults into dependability modeling and calculations. Chapter 4 presents the mathematical methods to collect operational data and evaluate the results and to estimate the reliability.

6.2 Contributions of the Dissertation Thesis

The main contributions of this thesis *Prediction and Analysis of Mission Critical Systems Dependability* can be emphasized as follows:

- In-depth studying and assessing the existing approaches to dependability parameters prediction. This study has shown the incorrect use of many obsolete standards and approaches, and their main shortcomings have been identified.
- The examples demonstrating that using such obsolete or inappropriately used standards can produce results far from reality (e.g. hundred years MTTF).
- Heterogeneous Dependability Model. The proposed model allows to hierarchically incorporate different model types: Markov chains, reliability block diagrams, Petri Nets, etc.
- Modelling of transient faults and using these faults in more realistic dependability parameters computations.
- Using mathematical methods to process a large amount of unordered and often missing data.
- Experimental evaluations of all proposed methods on real practical (industrial) problems, mostly of large size and based on data gathered from many years of equipment functioning.
- Denomination of other problems in this area to be solved and partial foreshadow how to do it (dynamical dependability database, coloured hierarchical model, optional choice of fault distribution, multiple faults modelling).

This thesis is not focused on a concrete field of electronic systems reliability, although all examples are based on Czech railways and rail transportation and using FPGAs in AŽD railways safety equipments. I firmly believe that my work can be used in different fields of all human activities, where the predefined dependability parameters level must be guaranteed. Proper and understandable dependability model has been designed with the aim to design a realizable system fulfilling predefined dependability constraints. I rather focused my research and the thesis on common electronic systems and their dependability problems; it does not matter whether it is a train transport or car transport, or perhaps a power plant, etc.

6.3 Future Work

Based on the interesting problems encountered in solving this dissertation, the author suggests to examine the following (first attempts to solve some of these problems have been made, some partial results were submitted to international conferences):

- *A database of dependability parameters*
  When I was proposing processes for collecting reliability data from the operation of railway equipment, I proposed a database of dependability parameters. This database allows to update a failure rate of each component, module, or the whole system. Particularly, the original failure rate of each component is calculated according to the standard, and then it is updated according to the operation data.

  Gradually it has been shown that the values from this database are very important for the design of new and similar equipment and also for maintenance.

- *Non-constant failure rate*
  Our research in this area has shown that the assumption of a constant failure rate may not always be correct. Some components get aging faster and wear out earlier. A curve of aging in operation can have a different shape for each type of electronic part. The proposed database can serve to track real measured data. There are two possibilities based on using this database: to use up-to-day data, it means to construct a dynamic database, or to allow incorporating different types of fault distributions into computation.

- *Include the software reliability into the proposed methodology*
  The whole thesis basically does not address the area of reliability of software. In the future, I consider it necessary to link these two areas. I believe that the overall reliability of the system should reflect possible software-based dependability-increasing methods.

- *Improve the Heterogeneous Colored Model*
  The time consumption of a precise dependability analysis is enormous. One of the problems is how to describe the designed equipment in terms of dependability simply.

Bibliography

[1] Vintr, Z. Základní Filozofie Průkazu Spolehlivosti a Bezpečnosti Technického Systému v Počátečních Etapách Životního Cyklu – only in Czech. *Česká Společnost pro Jakost*, 6 2009: pp. 1–8.

[2] Polian, I.; Hayes, J. P.; Kundu, S.; et al. Transient fault characterization in dynamic noisy environments. In *IEEE International Conference on Test*, Nov 2005, ISSN 1089-3539, pp. 1048–1058, doi:10.1109/TEST.2005.1584070.

[3] May, T. C.; Woods, M. H. A New Physical Mechanism for Soft Errors in Dynamic Memories. In *16th International Reliability Physics Symposium*, April 1978, ISSN 0735-0791, pp. 33–40, doi:10.1109/IRPS.1978.362815.

[4] Hirel, C. Symbolic Hierarchical Automated Reliability and Performance Evaluator. Duke University, Durham, USA, 2002, Available from: `http://sharpe.pratt.duke.edu`.

[5] Maplesoft. Maple – Symbolic and Numeric Computing Enviroment. Waterloo Maple, Canada, 2003, Available from: `http://www.maplesoft.com/products/Maple/`.

[6] Storey, N. R. *Safety Critical Computer Systems*. Inc. Boston, MA, USA: Addison-Wesley Longman Publishing Co., 1996, ISBN 0-201-42787-7.

[7] Geffroy, J.-C.; Motet, G. *Design of Dependable Computing Systems*. Institut National des Sciences Appliqués, Toulouse, France: Kluwer Academic Publishers, 2002, ISBN 1-4020-0437-0, 672 pp.

[8] IEC 61078:2016 Reliability Block Diagrams. 2016, Available from: `http://webstore.iec.ch/publication/25647`.

[9] Hlavička, J.; Racek, S.; Golan, P.; et al. *Číslicové systémy odolné proti poruchám*. Czech Republic: ČVUT v Praze, 1992, ISBN 80-01-00852-5.

[10] Vesely, W.; Dugan, J.; Fragola, J.; et al. Fault Tree Handbook with Aerospace Applications. 2002, Available from: http://elibrary.gsfc.nasa.gov/_assets/doclibBidder/tech_docs/25.NASA_Fault_Tree_Handbook_with_Aerospace_Applications-Copy.pdf.

[11] Petri, C. A. *Communication with automata*. Dissertation thesis, 1966, Available from: http://www.dtic.mil/dtic/tr/fulltext/u2/630125.pdf.

[12] Wikipedia.org. "European Train Control System – Eurobalise". 2017, Available from: http://en.wikipedia.org/wiki/European_Train_Control_System.

[13] Avizienis, A.; Laprie, J. C.; Randell, B.; et al. Basic concepts and taxonomy of dependable and secure computing. *IEEE Transactions on Dependable and Secure Computing*, volume 1, no. 1, Jan 2004: pp. 11–33, ISSN 1545-5971, doi:10.1109/TDSC.2004.2.

[14] Reliability Prediction of Electroic Equipment MIL-HDBK-217F. 1991, Available from: http://www.weibull.com/mil_std/mil_hdbk_217f.pdf.

[15] Reliability Methodology for Electronic Systems. 2004, Available from: http://www.fides-reliability.org.

[16] Reliability data handbook – Universal model for reliability prediction of electronic components, PCBs and equipment. 2004, Available from: http://webstore.iec.ch/publication/6946.

[17] Strnadel, J. On Dependability Assessment of Fault Tolerant Systems by Means of Statistical Model Checking. In *Proceedings of the 2017 20th Euromicro Conference on Digital System Design*, IEEE Computer Society, 2017, ISBN 978-1-5386-2146-2, pp. 352–355.

[18] Dictionary.com. Online Etymology Dictionary – "Dependability". 2017, Available from: http://www.dictionary.com/browse/dependability.

[19] Wikipedia.org. "Dependability". 2017, Available from: http://en.wikipedia.org/wiki/Dependability.

[20] Dictionary.com. Online Etymology Dictionary – "Reliability". 2017, Available from: http://www.dictionary.com/browse/reliability.

[21] IEC 60050-191:1990 International Electrotechnical Vocabulary. Chapter 191: Dependability and quality of service. 1990, Available from: http://webstore.iec.ch/publication/184.

[22] Bradley, E. *Reliability Engineering: A Life Cycle Approach*. CRC Press, 2016, ISBN 9781315367422, 370 pp.

[23] Barlow, R. E.; Proschan, F. *Mathematical Theory of Reliability*. SIAM, 1965, ISBN 9781611971194, 258 pp.

[24] Starý, I. *Spolehlivost Systémů*. Zikova 4, Prague, Czech Republic: ČVUT v Praze, 1998, ISBN 80-001-01756-7, 120 pp.

[25] DeVale, J. Traditional Reliability. Carnegie Mellon University, 1998, Available from: http://users.ece.cmu.edu/~koopman/des_s99/traditional_reliability/.

[26] Takahashi, Y. "Progress in the Electronic Components Industry in Japan after World War II". In *Technological Competitiveness: Contemporary and Historical Perspectives on Electrical, Electronics, and Computer Industries*, 1993, pp. 37–52.

[27] Technical Committee 56. 1965, Available from: http://tc56.iec.ch/about/about_tc56.htm.

[28] Gnedenko, B. V.; Beljajev, J. K.; Soloviev, A. D. *Mathematical Methods of Reliability Theory*. New York: Academic, 1969, 506 pp.

[29] Ziegler, J. F.; Lanford, W. A. Effect of Cosmic Rays on Computer Memories. *Science*, volume 206, no. 4420, 1979: pp. 776–788, ISSN 0036-8075, doi:10.1126/science.206.4420.776.

[30] Stroud, C. E. *Mathematical Methods of Reliability Theory*. Kluwer Academic Publishers, 2002, ISBN 1-4020-7050-0, 319 pp.

[31] Matsumoto, K.; Matsumoto, T.; Goto, Y. Reliability Analysis of Catalytic Converter as an Automotive Emission Control System. In *SAE Technical Paper*, SAE International, 1975, doi:10.4271/750178.

[32] Laprie, J. C. *Dependability: Basic Concepts and Terminology*. Vienna: Springer Vienna, 1992, ISBN 978-3-7091-9170-5, pp. 3–245, doi:10.1007/978-3-7091-9170-5_1.

[33] Electronic Reliability Design Handbook MIL-HDBK-338B. 1998, available from: http://www.weibull.com/mil_std/mil_hdbk_338b.pdf.

[34] Leonard, C. MIL-HDBK-217: it's time to rethink it. *Electronic Design*, 1991: pp. 79–82.

[35] Windchill. Relex – Reliability Management Software. 1999, Available from: http://www.crimsonquality.com.

[36] Quanterion. RIAC – The Reliability Information Analysis Center. 2005, Available from: http://www.quanterion.com.

[37] Gipper, J. VITA 51 and the Reliability Community ease reliability prediction challenges. *VITA Technologies*, Dec 2012, Available from: http://vita.mil-embedded.com/articles/vita-and-reliability-reliability-prediction-challenges/.

[38] Novák, M.; Šebesta, V.; Votruba, Z. *Bezpečnost a Spolehlivost Systémů*. Zikova 4, Prague, Czech Republic: ČVUT v Praze, 2003, ISBN 80-01-02807-0, 160 pp.

[39] European Standards EN 50126:2001 Railway application – The specification and demonstration of Reliability, Availability, Maintainability and Safety (RAMS). 2001, international Industrial Standard.

[40] IEEE 90 – Institute of Electrical and Electronics Engineers. IEEE Standard Computer Dictionary: A Compilation of IEEE Standard Computer Glossaries. 1990, New York, NY.

[41] Kohlík, M. *Hierarchical Dependability Models Basen on Markov Chains*. Dissertation thesis, Faculty of Information Technology, Czech Technical University in Prague, 2015.

[42] Dobiáš, R. *Methodology of Fail-safe and Fault Tolerant System Design*. Dissertation thesis, Faculty of Electrical Engineering, Czech Technical University in Prague, 2010.

[43] Kirrmann, H. Fault Tolerant Computing in Industrial Automation, Second edition. 2005.

[44] Vaňát, T. *Physical Fault Injection and Monitoring Methods for Programmable Devices*. Dissertation thesis, Faculty of Information Technology, Czech Technical University in Prague, 2017.

[45] Habing, D. H. The Use of Lasers to Simulate Radiation-Induced Transients in Semiconductor Devices and Circuits. *IEEE Transactions on Nuclear Science*, volume 12, no. 5, Oct 1965: pp. 91–100, ISSN 0018-9499.

[46] Krstic, M.; Schoof, G.; Petrovic, V.; et al. DE Patent DE 10 2013 225 039 B4 The system for detection and correction of transient errors in the combinational circuits. Technical report, Deutsches Patent- und Markenamt, 5 2016.

[47] Sogomonyan, E. S.; Weidling, S.; Goessel, M. A new method for correcting time and soft errors in combinational circuits. In *2013 IEEE 16th International Symposium on Design and Diagnostics of Electronic Circuits Systems (DDECS)*, April 2013, pp. 283–286, doi:10.1109/DDECS.2013.6549835.

[48] IEC 60812:2006 Analysis techniques for system reliability - Procedure for failure mode and effects analysis (FMEA). 2006, Available from: `http://webstore.iec.ch/preview/info_iec60812%7Bed2.0%7Den_d.pdf`.

[49] CEI IEC 1025:1990 Fault tree analysis (FTA). 1990, Available from: `http://webstore.iec.ch/p-preview/info_iec61025%7Bed1.0%7Db.img.pdf`.

[50] Wolfram. Mathematica. 2017, Available from: `http://www.wolfram.com/mathematica/`.

[51] European Standards EN 50129:2003 Railway applications - Communication, signalling and processing systems - Safety-related electronic systems for signalling. Dec 2003.

[52] Scharoba, S.; Schölzel, M.; Koal, T.; et al. On reliability estimation for combined transient and permanent fault handling. In *14th Biennial Baltic Electronic Conference (BEC)*, Tallinn, Estonia, 2014, pp. 73–76.

[53] Scharoba, S.; Koal, T.; Vierhaus, H. T. Estimating the effect of TMR on lifetime considering transient and permanent faults. In *Doctoral Workschop ICTDS*, Tallinn, Estonia, 2014.

[54] David, A.; Larsen, K.; Legay, A.; et al. Uppaal SMC Tutorial. *International Journal on Software Tools for Technology Transfer*, volume 17, no. 4, 2015: pp. 397–415, doi: 10.1007/s10009-014-0361-y., Available from: `http://vbn.aau.dk/files/207763747/main.pdf`.

[55] Electronic Track Circuits Type KOA1. Standard, Apr. 2016, Available from: `http://www.azd.cz/admin/files/Dokumenty/pdf/Produkty/Kolejove/30-KOA-1-ENG.pdf`.

[56] Cox, D. R.; Oakes, D. *Analysis of Survival Data*. CRC Press, Jun. 1984, ISBN 9780412244902, 208 pp., google-Books-ID:Y4pdM2soP4IC.

[57] Kalbfleisch, J. D.; Prentice, R. L. *The statistical analysis of failure time data*, volume 360. John Wiley & Sons, 2011.

[58] Kaplan, E. L.; Meier, P. Nonparametric Estimation from Incomplete Observations. *Journal of the American Statistical Association*, volume 53. no. 282, 1958: pp. 457 – 481.

[59] Handbook of 217Plus^{TM} – Reliability Prediction Models. 2015, Available from: `http://www.quanterion.com/product/publications/hdbk-217plus-2015-notice-1/`.

[60] Standard for the reliability prediction of electronic and electromechanical components. 2015.

[61] Trainguard Eurobalise S21 and S22 – central component for ETCS. 2014, Available from: `http://www.mobility.siemens.com/mobility/global/SiteCollectionDocuments/en/rail-solutions/rail-automation/train-control-systems/trainguard-eurobalise-s21-s22-en.pdf`.

[62] Torell, W.; Avelar, V. Mean Time Between Failure: Explanation and Standards. 2004: p. 10.

[63] Vais, V.; Racek, S. Experimental evaluation of regular events occurence in continuous time markov models. In *Proceedings of the Eleventh International Conference on Informatics*, Košice, Slovakia, 2011, pp. 143–146.

Reviewed Publications of the Author Relevant to the Thesis

[A.1] Daňhel, M.; Dobiáš, R.; Kubátová, H. Predictive Analysis of Mission Critical Systems Dependability. In: *Proceedings of 16th Euromicro Conference on Digital System Design*, pp. 561-566, Santander, Spain, 2013.

The paper has been cited in:

- Fauser, J; Schmidthuysen, M; Scheffold, B. The Prediction of Success in Project Management – Predictive Project Analytics, 2016.
  "Available from: `http://www.bdu.de/media/177649/predictive-project-analytics_artikel_gpm.pdf`"

[A.2] Daňhel, M.; Štepánek, F.; Kubátová, H. The Effect of the Transient Faults in Dependability Prediction. In: *Proceedings of 19th Euromicro Conference on Digital System Design*, pp 9-13, Limassol, Cyprus, 2016.

[A.3] Daňhel, M.; Štepánek, F.; Kubátová, H. The Effect of the Transient Faults in Dependability Prediction. In: *Journal of Microprocessors and Microsystems - Embedded Hardware Design, vol: 52*, pp. 498-504, 2017.

[A.4] Daňhel, M.; Kubátová, H. Dependability or Reliability in the Real World, History, Terminology, Prediction In: *6thMediterranean Conference on Embeded Computing including 5th Workshop on Embedded and Cyber-Physical Systems.* pp. 4, Bar, Montenegro, 2017.

[A.5] Novák, P.; Daňhel, M.; Blažek R.; Kohlík, M.; Kubátová, H. Predicting the Life Expectancy of Railway Fail-Safe Signaling Systems Using Dynamic Models with Censoring. In: *2017 IEEE International Conference on Software Quality, Reliability and Security (QRS).* pp. 329-339, Prague, Czech Republic, 2017.

[A.6] Daňhel, M.; Štepánek, F.; Kubátová, H. Dependability Prediction Involving Temporal Redundancy and the Effect of Transient Faults. In: *Proceedings of 20th Euromicro Conference on Digital System Design.* pp 360-363 Vienna, Austria, 2017.

Remaining Publications of the Author Relevant to the Thesis

[A.7] Daňhel, M. *Reliability of Digital Systems.* Ph.D. Thesis Report, Faculty of Information Technology, CTU in Prague, Czech Republic, 2013.

[A.8] Daňhel, M. Hierarchical Reliability Block Diagrams in the Program SHAMAP. In: *15th International Student Conference on Electrical Engineering POSTER 2011*, pp 5, Prague, Czech Republic, 2011.

[A.9] Daňhel, M. The Determination of Operational Reliability and Predictive Analysis of Reliability of the Railway Signaling Systems. In: *19th International Student Conference on Electrical Engineering POSTER 2015*, pp 5, Prague, Czech Republic, 2015.

The paper has been awarded as the best paper.

[A.10] Daňhel, M. The Effect of the Transient Faults in Dependability Prediction. In: *20th International Student Conference on Electrical Engineering POSTER 2016*, Prague, Czech Republic, 2016.

[A.11] Daňhel, M. Hierarchické Blokové Modely. In: *Počítacové Architektury a Diagnostika (Czech only)*, p , Stará Lesná, Slovak Republic, 2011.

[A.12] Daňhel, M. Predikce a Analýza Spolehlivosti Kritických Systémů. In: *Počítacové Architektury a Diagnostika (Czech only)*, p. 69-74, Teplá, Czech Republic, 2013.

[A.13] Daňhel, M.; Kubátová, H. *Methods of Hierarchical Reliability Block Diagrams in the Program SHAMAP.* In: *Proceedings of 14th Euromicro Conference on Digital System Design - WiP*, pages 31-32, Oulu, Finland, 2011.

[A.14] Daňhel, M. Spolehlivostní Analýza KOA1M. *Comprehensive Research Report RRR-FIT-15-02 (Czech only).* Technical Report for FIT CTU in Prague, pp 12, Praha, Czech Republic, 2015.

[A.15] Daňhel, M. Spolehlivostní Analýza ABA-12. *Comprehensive Research Report RRR-FIT-17-03 (Czech only).* Technical Report for FIT CTU in Prague, pp 12, Praha, Czech Republic, 2017.

[A.16] Daňhel, M.; Štepánek, F.; Kubátová, H. Relaibility Model of TMR System Considering Transient Faults. In: *Workshop on Trustworthy Manufacturing and Utilization of Secure Devices*, pp 5, Dresden, Germany, 2016.

Remaining Publications of the Author

[A.17] Daňhel, M. Využití programu MAPLE při výpočtech spolehlivostních parametrů. *Bachelor Thesis (Czech only), Faculty of Electrical Engeneering*, p. 67, Praha, Czech Republic, 2007.

[A.18] Daňhel, M. Využití programu MAPLE při výpočtech spolehlivostních parametrů. *Master Thesis (Czech only), Faculty of Electrical Engineering*, p. 139, Praha, Czech Republic, 2011.

[A.19] Daňhel, M.; Kubátová, H. Modelling the Reliability and Safety of the System as a Whole and Its Partial Calculation. *Biannual European - Latin American Summer School on Design, Test and Reliability*, p. 2, Rotterdam, The Netherlands, 2017.

[A.20] Daňhel, M. The Determination of Operational Reliability and Predictive Analysis of Reliability of the Railway Signaling Systems. In: *Vienna-Bratislava-Brno-Prague – Joint Research Seminar for PhD Students*. pp 1, Bratislava, Slovak Republic, 2015.

Appendix A

Predictive Analysis of Mission Critical Systems Dependability

This paper was published at the *Euromicro Conference on Digital System Design* in Spain in 2013. The paper has been cited:

- Fauser, J; Schmidthuysen, M; Scheffold, B. The Prediction of Success in Project Management – Predictive Project Analytics, 2016.
  Available from:
  `http://www.bdu.de/media/177649/predictive-project-analytics_artikel_gpm.pdf`

2013 16th Euromicro Conference on Digital System Design

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.

`/13 $26.00 © 2013 IEEE
DOI 10.1109/DSD.2013.66

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.

Listed methods or standards for calculation of reliability parameters are mostly alternatives. If we compare the reliability parameters similar (competing) equipment, we calculate according to the same metrics (standards). Our methodology is built on the basis of MIL-HDBK-217F because this standard is suitable for computing the reliability of railway signalling equipment.

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.

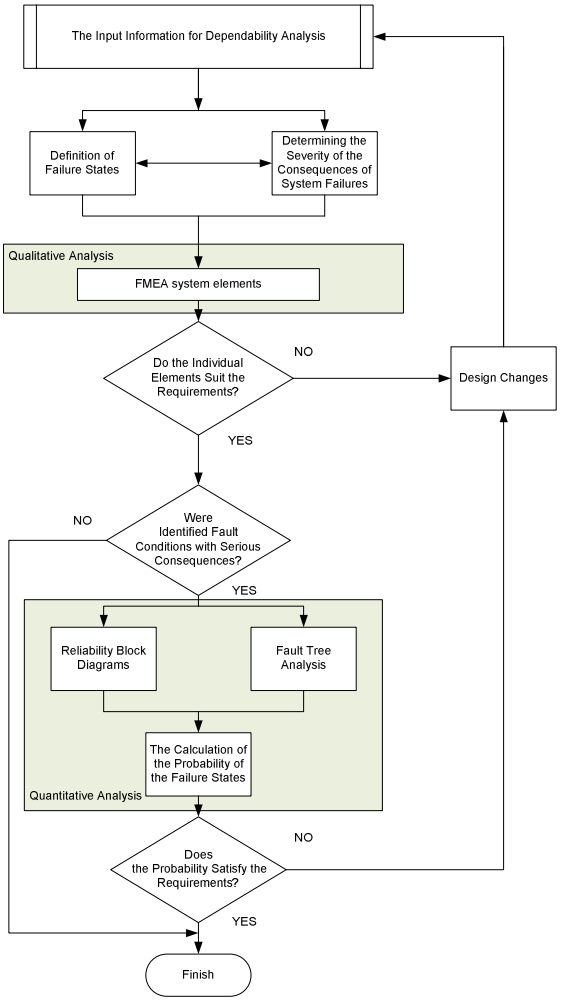

Figure 1.The process of predictive dependability analysis

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.

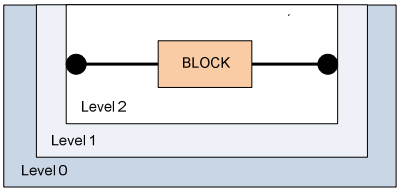

Figure 2.The process of predictive dependability analysis

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.

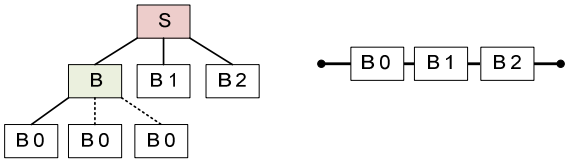

Figure 3.Hierarchical model with backup

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 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.

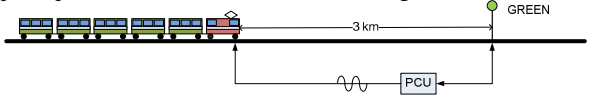

Figure 4.There is a train on rails before the signaling equipment. The signaling equipment indicates free passage. The *PCU* emit a signal into rails. This frequency means that everything is in order.

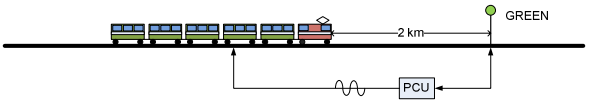

Figure 5.Here is the critical limit, where the train can stop before the signaling equipment.

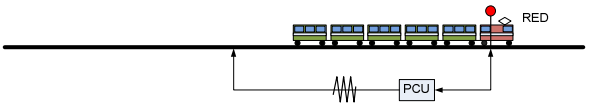

Figure 6.The train passed signaling equipment. At this moment the signal has changed to STOP. But this information was given train only using *PCU*.

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. In the Figure 7 is the underlined bad result.

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.

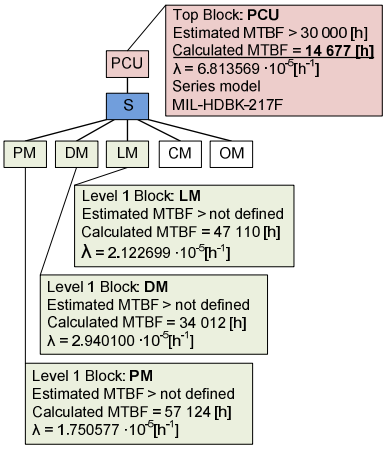

Figure 7.The process of predictive dependability analysis

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.

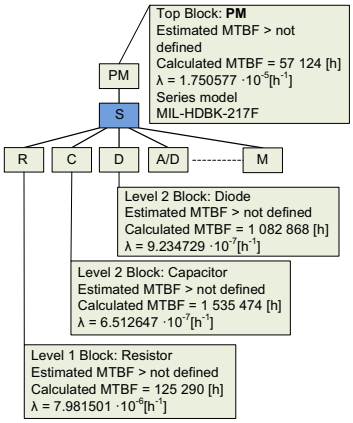

Figure 8.Screenshot from SHAMAP - Hierarchical model of the module *PM* with associated information

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.

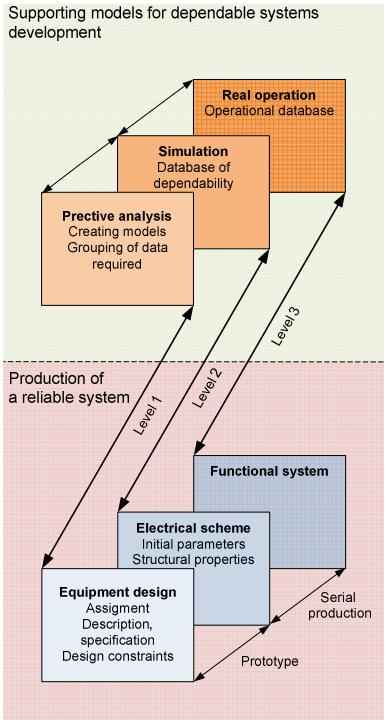

Figure 9.Reliable system development methodology roofed by hierarchical UML models

The phases of the real system development are described in Figure 9. The development of 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 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 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.

Appendix B

Predicting the Life Expectancy of Railway Fail-safe Signaling Systems Using Dynamic Models with Censoring

This paper was published at the*2017 IEEE International Conference on Software Quality, Reliability and Security (QRS)* in Czech Republic in 2017.

My main contribution was collecting and preparing observed data. I was also involved in the subsequent evaluation of the results.

2017 IEEE International Conference on Software Quality, Reliability and Security

Predicting the Life Expectancy of Railway Fail-safe Signaling Systems Using Dynamic Models with Censoring

Petr Novák, Martin Daňhel, Rudolf B. Blažek‡, Martin Kohlík, and Hana Kubátová*
Statistics & Probability Research Group, Faculty of Information Technology
Czech Technical University in Prague, 160 00 Prague 6, the Czech Republic
Email: petr.novak@fit.cvut.cz, martin.danhel@fit.cvut.cz, rudolf.blazek@boxtrap.net
martin.kohlik@fit.cvut.cz, hana.kubatova@fit.cvut.cz
‡Affiliated also with Boxtrap Research, Prague, the Czech Republic
*IEEE Senior Member

***Abstract*—In the presented work we predict the life expectancy of multi-part railway fail-safe signaling systems. The monitored electronic track circuits detect train locations and movement in real time, and issue alerts and warnings to prevent collisions. Based on 10 years of failure reports from the manufacturer of systems used by Railway Infrastructure Administration in the Czech Republic, we establish estimates of time-to-failure distributions of their components. We modify and apply survival models for censored data with various parameters for which we propose and compare new estimators. Both left and right time-based censoring of the data is considered. This approach allows us to include in the analysis components that were in operation before the study started, as well as components that were functional after the end of the study. Special attention is paid to the correct treatment of missing and incomplete data in the analyzed reports. We compare models with constant and variable failure rates. Hypotheses testing methodology is used to select a model with the best fit for the analyzed data.**

I. Introduction and Motivation

Requirements for predefined levels of reliability and safety parameters become recently an inseparable part of technical requirements for modern technical systems. The development and design methods of any technical system will not be successful without clearly defined requirements for reliability and safety aspects. These requirements are usually formulated by a future user of the designed system, mainly when the system is developed for a specific user, or by a manufacturer – especially for systems intended for serial production. For systems whose failures could lead to health or human life hazard, or to large material losses, the requirements for reliability and safety are often laid down by mandatory regulation, such as laws, notices, directives, standards, etc. (see [1], [2]).

There are also requirements to predict a requested level of reliability before proceeding to actual manufacturing or before the construction of a prototype. These requirements follow from the experience that every forced change of the system structure implemented before preproduction phases is considerably simpler and cheaper than in the following phases. Practically, a customer requires a proof, that the developed system will meet his requirements for reliability and safety levels in the starting phases of the system's lifecycle. This proof is obligatory, and in the case of a later system failure, there is a possibility of serious sanctions for the manufacturer. These results are accepted and mainly used as the proof of prediction analyses of reliability and safety issues (see [1], [3]).

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. This study is focused on *quantitative analysis*.

The calculation (or estimation) of quantitative (numerical) values of appropriately selected reliability indicators is performed under the terms of the quantitative analysis. The numerical values of a probability of a phenomenon can be obtained from the reliability model. Quantitative analysis can be generally done "by hand" if the systems are simple and not too large. Otherwise it is obtained using specialized software tools.

II. Description of the Problem

A. Dependability Terminology

Dependability of a system is the ability to avoid service failures that would be more frequent and more severe than acceptable. Service failures correspond to situations where the behaviour of the system deviates from the correct behaviour. Dependability is a concept that integrates four dependability parameters called RAMS standards (see [4]):

- **Reliability** is the probability of the correct function of a component 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.

978-1-5386-0592-9/17 $31.00 © 2017 IEEE
DOI 10.1109/QRS.2017.43

These dependability parameters have been introduced in the Electronic Reliability Design Handbook MIL-HDBK-338B (see [5]). This study focuses primarily on the first (Reliability) and last (Safety) items. Generally there is a trade off – with higher safety levels smaller reliability of the equipment can be achieved.

Next we describe the most common reliability related metrics. The mean time to failure (MTTF) describes the expected time to failure for a *non-repairable system*. MTTF is derived from basic statistical theory as follows:

$$MTTF = \int_0^\infty R(t)\,dt,$$

where ***R(t)*** is the reliability function, i.e. the probability of a system not failing prior to some time *t*. In the following sections of this work the reliability function will also be denoted as the *survival* function ***S(t)***.

On the other hand, the mean time between failures (MTBF) is the predicted elapsed time between failures of a *repairable system*.

The average rate at which failures occur in a time interval from t_1 to t_2, the failure rate $\lambda(t)$, is defined as the ratio of probability that failure occurs in the interval, given that it has not occurred prior to t_1, the start of the interval, divided by the interval length. Thus,

$$\lambda(t) = \frac{S(t) - S(t + \Delta t)}{\Delta t\, S(t)},$$

where $t = t_1$ and $t_2 = t + \Delta t$. The hazard rate $h(t)$, or instantaneous failure rate, is defined as the limit of the failure rate as the interval length approaches zero, or

$$h(t) = \frac{f(t)}{S(t)},$$

where f is the density function for S. See the discussion of equation (9) in Section III-B8 for more details.

Hazard rate according to the EN 50126 (see [4]) is hazard defined as a state that can lead to accidents or a situation that can lead to injury of people. This meaning of *hazard rate* is not considered further in this study.

B. Description of the Equipment

In the past the safety related functionality in railway applications was always based on gravitational attraction (e.g. by relays) for the stop-signals, and on a mechanical pull, or on a large value of the electrical current for the permit signal.

Nowadays electronic 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, 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 is one method for showing its high dependability parameters in such cases.

In the Czech Republic and other countries in Central and Eastern Europe, Track Circuit Systems (TCS) are used to detect a train on rails. This is a very important system known as the critical system for which the highest safety integrity level (SIL = 4) is required, according to the standard EN 50126 (see [4]). The company AZD Praha produces these safety signaling systems.

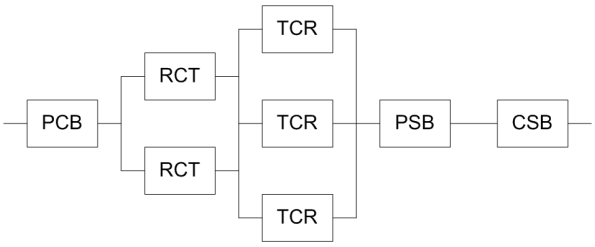

Fig. 1. The reliability block diagram of Track Circuit System developed of the company AZD Praha. Block diagram contains only critical parts.

This manufacturer provided detailed electrical scheme of TCS for this study and also maintenance data of TCS from the past 10 years of operation. Required life time of these equipment is 20 years.

Description of the block model in Fig. 1:

- **PCB** – Power and Circuit Breakers block represents power, circuit breakers and other input ports of the equipment.
- **RCT** – Rectifier – these blocks are redundant and represent the next stage of power distribution and rectifiers.
- **TCR** – Track Circuit Receiver – these blocks are redundant and represent the most complex part of the whole system. This part consists of several sub-parts. (For the purposes of this study it is not necessary to further subdivide this part).
- **PSB** – Power Switchboard – this block represents power distribution within the Track Circuit System.
- **CSB** – Communications Switchboard – this block represents communication within the Track Circuit System.

Some parts of the equipment are based on independent hot-swap modules. Due to high safety, the TCS is constantly under the control of the master system supervising the proper functionality of TCS. The rectifiers are two independent hot-swap modules. Each rectifier provides power to all switchboards. The failure of a single rectifier does not cause the failure of the equipment. The TCSs are three independent boards. Each board performs the same calculations independently of the other boards, but the results are compared to each other. Two fully functional boards are required to keep the equipment operational.

C. Description of the Data

The company AZD Praha owns a database of failures for TCS (the service database). This database stores information on the order of several thousand records on TCS. Faults are distinguished at the module level (according to the Fig. 1). The supplied data are a business secret of the manufacturer. Therefore, the data presented in this study have been slightly

modified by randomization. The aim of this study is not to prove dependability of Track Circuit Systems, but to demonstrate the use of methods for censored data in the field of dependability.

Each fault corresponds to the replacement of the faulty part by a new one. The manufacturer collects information on every fault or regularly scheduled maintenance. The large-scale utilization of TCS has started in early 2006. Since then, their numbers have been increasing. The mentioned equipment consists of approximately 2,500 electronic parts. The parts level is the smallest possible resolution which is required by the reliability standards i.e. MIL-HDBK-217 or FIDES (see [6], [7]). If the observed failure data are not available, using these standards-based reliability prediction methods becomes the best available approach, but such method may be inaccurate due to outdated standards, different environmental/performance conditions, etc.

Sometimes, a fault of some component does not necessarily mean a total failure. Some faults cannot have an effect, therefore these faults cannot be recorded. On the other hand, there are faults that cannot be controlled, for example atmospheric effects. Thus there may be situations where a fault is recorded, but is not proved in any way. It was necessary to remove these false faults from the measurements. Because the database is maintained purely for service purposes, it was necessary to identify faults concerning device functions.

For individual blocks (shown in Fig. 1) we distinguish among the following faults:

- **PCB**
  - *Transformer failure*
  - *Fault of connector*
  - *Circuit breaker failure*
- **RCT**
  - *Fault of internal components*
  - *Rectifier failure*
  - *Connector fault*
- **TCR**
  - *Fault of internal components*
  - *Faulty CPU*
  - *Faulty memory*
  - *Faulty connector*
  - *Faulty crystal*
  - *Faulty relay*
  - *Faulty diagnostics*
  - *Software error*
- **PSB**
  - *Fault of internal power distribution*
  - *Connector fault*
- **CSB**
  - *Communication error*
  - *Connector fault*

In each mentioned block, two additional failure types may occur:

- *Manufacturing defect*
- *Unknown cause*

Faults not considered by the calculation:

- *Fault or failure of an other device responsible for TCS*
- *Incorrect calibration*
- *Atmospheric effects.*

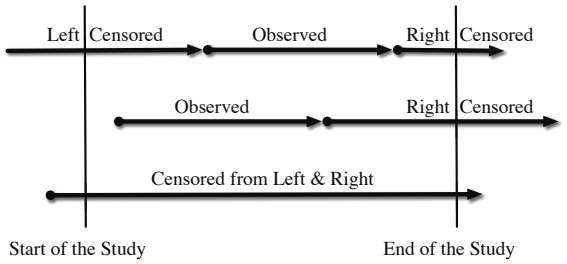

Fig. 2. Observed service times for devices in the study may be censored by time either from the left, right, or both. The service times are independent.

III. Methodology

In this study we use survival analysis with *time-censored* observed failure data. We will first discuss what is meant by censoring observed data by time. Then we will introduce the main ideas of the methodology in a discrete-time example. It is much easier to understand than the general continuous-time survival model that we utilized in the study, and describe last.

A. Time-Censored Failure Data

Consider a device that is deployed at several service locations. The devices can fail over time and are replaced by a new one after a failure. In order to analyze the reliability of the device, we start recording the failure times of the deployed devices. We will assume that the failure times are independent between locations and after replacing a defective device.

As shown in Fig. 2, some of the devices were in operation before we started the study. And most devices, if not all, were operational when the study finished. We only know exact failure data for devices that were put in service and also failed during the course of the study. Either after replacing a failed device, or at a new location.

For devices that were functional before we started observing them, we do not know the left starting point of their service times. We call these observed service times to be *censored by time from the left*. Similarly, devices functional at the end of the study have service times *censored by time from the right*.

For a right-censored service time we only know that a failure did not happen yet, and the actual service time is longer than the observed value. The good part is that we also know the actual age of the device during the study, therefore we know how the failure rate of the device changed due to aging.

Unfortunately we do not know the age of a device that was operational before the study. This is a complication that can only be addressed if we assume at least some properties of the aging process, or the shape of the failure rate function as it changes over time.

TABLE I
REPLACED OR NEWLY INSTALLED DEVICES

	Before	2003		
Month	2003	Jan	Feb	Mar
Devices	30	10	20	10

In the basic models, and in the discrete-time example below, we will assume that the devices have a constant failure rate and hence do not age. This assumption leads to a survival model with random failure times with exponential distribution [8], [9]. We also discuss more general models in Section III-D.

Constant failure rates will allow us to treat left-censored failure times the same way as the right-censored failure times. For both cases we will only utilize the information that the actual service time was longer than observed, disregarding the age of the observed devices.

B. Motivational Discrete-time Example

The goal of the following example is to intuitively illustrate the reasoning why survival analysis uses "hazards" to estimate the distribution of failure times of a device. Simply put, hazards utilize the *censored* data in a "smarter" way compared to other "natural" or classical choices of estimators. For this purpose we will temporarily assume that we deal with device failures that can occur at discrete times, at the level of months.

Consider a service shop that has in 2003 replaced broken or installed new devices by month as listed in Tab. I. The devices that were installed before 2003 are considered censored by time from the left.

Tab. II shows numbers of devices that have failed during the first few months of 2003. They are listed separately for each month when the devices were installed so that we can determine their ages at the time when they fail. The number of devices installed each month is listed in parentheses.

1) Information from the Observed Failures: The equipment is assumed to be inspected, replaced, and newly installed always on the *first day* of each month. If a device fails during a given month, the failure is considered to have occurred immediately before the inspection the next month. Therefore the device is considered to have aged the whole month. As a result, failures can happen only at integer ages, with the first possible failure at age 1.

Let T_i denote the age of the i-th observed device at the time when it fails. This age is called the *time-to-failure*. In our data set we have observed 70 devices of the same type, with $i = 1, \ldots, 70$. Notice that for the left-censored data in the first row, we are unable to determine the exact failure ages of the devices because we do not know when this equipment has been put in service. Similarly, in the last column with the right-censored data we only know that the equipment has not yet failed when the study ended.

Information about the observed failures in Tab. II corresponds to observed frequencies for events of the form $\{T_i = t\}$ and $\{T_i \geq t\}$ for device ages t calculated from the failure times. These events are listed in Tab. III, and their observed frequencies are listed in the corresponding cells of Tab. II.

TABLE II
OBSERVED EQUIPMENT FAILURES

Installed	Failures Observed in 2003						Censored	
Before	(30)	2	2	4	2	3	30	17
Jan		(10)	1	2	3	1	0	3
Feb			(20)	2	1	5	0	12
Mar				(10)	1	2	0	7
		Jan	Feb	Mar	Apr	May	Left	Right

TABLE III
CORRESPONDING OBSERVED EVENTS

Installed	Information about Failure Times						Censored
Before	(30)	$T_i \geq 1$	$T_i \geq 2$	$T_i \geq 3$	$T_i \geq 4$	$T_i \geq 5$	$T_i \geq 6$
Jan		(10)	$T_i = 1$	$T_i = 2$	$T_i = 3$	$T_i = 4$	$T_i \geq 5$
Feb			(20)	$T_i = 1$	$T_i = 2$	$T_i = 3$	$T_i \geq 4$
Mar				(10)	$T_i = 1$	$T_i = 2$	$T_i \geq 3$
		Jan	Feb	Mar	Apr	May	Left Right

2) Estimating the Time-to-Failure Probabilities: We assume that the failure times are independent and identically distributed (i.i.d.). They have the same distribution function $F(t) = P(T_i \leq t)$, where $t = 1, 2, \ldots$ is the device age in months. The independence is presumed to hold for devices across different locations, as well as for devices replaced at the same location.

Our goal is to estimate the cumulative distribution function F based on the information gathered. For the sake of simplicity, let us temporarily exclude the left-censored data and focus on the the last 3 rows of Tab. II and III. We will come back to left-censoring in Section III-B4 below.

We will first estimate $P(T = t)$. For example, the events $\{T_i = 1\}$ and $\{T_i = 2\}$ have been observed 4 and 5 times, respectively, among 40 devices in the last 3 rows of Tab. II and III. Thus, for a failure time T of a general device of the observed type, we can estimate

$$\hat{P}(T = 1) = \frac{4}{40}, \qquad \hat{P}(T = 2) = \frac{5}{40}.$$

Therefore we get estimates of F for $t = 1, 2$ as

$$\hat{F}(1) = \hat{P}(T \leq 1) = \frac{4}{40}, \qquad \hat{F}(2) = \hat{P}(T \leq 2) = \frac{9}{40}.$$

Notice, however, that for estimation of $P(T = 3)$ we will have to reduce the set of considered devices because of censoring in the last row. There we were *unable to observe* any events $\{T_i = 3\}$. We did observe these events in the first two rows 8 times among 30 devices, therefore if we use the same direct approach for $t = 3$, we estimate

$$\hat{P}(T = 3) = \frac{8}{30}.$$

TABLE IV
OBSERVED EQUIPMENT FAILURES IN TERMS OF DEVICE AGES

Age t	Age at Least t	In the Study	Devices at Risk	Failed Devices	Censored L	Censored R
0	70	40	40	0	2	0
1	70	40	40	4	2	0
2	64	40	36	5	4	7
3	57	30	24	8	2	12
4	38	10	4	1	3	3
5	23	0	0	0	0	17

3) Including Right-censored Data: The next step is *absolutely crucial*. In the last row of Tab. II and III, we have observed 7 times the events $\{T_i \geq 3\}$. We can utilize this information if we rewrite the failure probability as

$$P(T = t) = P(T = t \,|\, T \geq t)\; P(T \geq t). \tag{1}$$

We can now include the right-censored data from the last row in the estimate of $P(T \geq 3)$. First, notice that in the first two rows with 30 devices, there are 6 devices with $T_i \leq 2$. Similarly, there are 9 devices with $T_i \leq 2$ among all 40 observed devices (recall $\hat{F}(2)$ above). Therefore we can estimate

$$\hat{P}(T = 3 \,|\, T \geq 3) = \frac{8}{30 - 6}, \qquad \hat{P}(T \geq 3) = \frac{40 - 9}{40}.$$

These estimates use 30 and 40 observations, respectively. Finally, we estimate

$$\hat{P}(T = 2) = \frac{8}{24} \times \frac{31}{40}.$$

If we only used the first 2 rows also for $\hat{P}(T \geq 3)$, we would would get $(30 - 6)/30$ which would yield our old undesired estimate $\hat{P}(T = 3) = 8/30$ that only uses 30 observations.

4) Including Left-censored Data: Recall that we have excluded data in the first row of Tab. II and III, because for the left-censored data there we are unable to calculate the exact ages of the devices when they fail.

Consider a device that was put in service before the study started, and denote its time-to-failure as S. If we knew that the device was in service exactly k months, then the remaining time-to-failure would be $S - k$. In addition we know that the device did not fail yet, i.e. that $S > k$.

For simplicity we will assume that the remaining time-to-failure $S - k$ has conditional distribution, given the event $\{S > k\}$, identical to the distribution of the original time-to-failure S. We will assume that it holds for any age k. This condition is called the "lack-of-memory property". It holds only for the discrete geometric and continuous exponential distribution. This assumption is quite common in simple survival analysis models [8], [9].

The consequence of this assumption is that we can treat the left-censored data as if they were right-censored. As an illustration, for $t = 2$ we only have used 40 devices from the last three rows of Tab. II and III to estimate

$$\hat{P}(T = 2) = \frac{5}{40}.$$

Using equation (1), we can utilize the left-censored data in the first row as follows:

$$\hat{P}(T = 2 \,|\, T \geq 2) = \frac{5}{40 - 4}, \qquad \hat{P}(T \geq 2) = \frac{70 - 6}{70},$$

and finally

$$\hat{P}(T = 2) = \frac{5}{36} \times \frac{64}{70}.$$

These two terms in the estimate use 40 and 70 observations, respectively. This is again an improvement over the original estimate $\hat{P}(T = 2) = 5/40$ which is only based on 40 observations.

5) Hazards and Devices at Risk: We have seen that we are able to utilize more information from the observed data when we use equation (1) to estimate the failure probabilities from censored data. Notice that we can rewrite it as a recursive formula

$$\begin{aligned} P(T = t) &= P(T = t \,|\, T \geq t)\; (1 - P(T \leq t - 1)) \\ &= P(T = t \,|\, T \geq t)\; (1 - F(t - 1)), \end{aligned} \tag{2}$$

where $F(t - 1)$ is assumed to have been already estimated in the previous step. Therefore in each step we only have to estimate $P(T = t \,|\, T \geq t)$.

In survival analysis literature, these conditional probabilities are referred to as *hazards*. They are denoted by

$$\lambda_t = P(T = t \,|\, T \geq t). \tag{3}$$

Hazards are estimated as

$$\hat{\lambda}_t = \frac{\text{Number of failures at age } t}{\text{Number of devices at risk at age } t}. \tag{4}$$

The term "*devices at risk* at age t" refers to devices that did not fail before age t, and stayed in the study at age t. The important detail is that if they fail at age t, we will observe the failure. More precisely, for these devices we know $T_i \geq t$, which is for discrete integer-valued time the same as $T_i > t - 1$. We also know if they failed at age t, i.e. if $T_i = t$ or not.

Our first step before estimating the hazards will be to rewrite the observed data in terms of device ages and devices at risk. But we have to take into account that the devices are censored at different ages from the left and right (at the beginning and end of the study).

The data is summarized in Tab. IV. The device categories used in the table are as follows:

In the Study:
Devices observed at age t. We know if $T_i = s$ or not for $s = 1, \ldots, t$.

Age at Least *t*:
Devices did not fail before age t; may or may not have departed the study at age $t - 1$. We know that $T_i > t - 1$, i.e. $T_i \geq t$. We **may or may not** know if $T_i = t$ or not.

Devices at Risk:
Devices did not fail before age t; observed in the study at age t. We know that $T_i > t - 1$, i.e. $T_i \geq t$. We also **do** know if $T_i = t$ or not.

Censored from the Right:
Devices did not fail *at or before* age t with status unknown *after* age t. We know that $T_i > t$, i.e. $T_i \geq t+1$. We **do not** know if $T_i = t+1$ or not.

Censored from the Left:
Devices did fail at time $t+1$ *after the beginning* of the study. Their previous service time k is *unknown*. We know that $T_i = t+1+k$ with unknown $k \geq 0$. If the devices do not age (rate failures do not change), we use this information as $T_i \geq t+1$, i.e. $T_i > t$.

In general, right-censored devices exit the study at age t without failing, and their status is unknown *after* age t. We do not know whether they did or did not fail later. If the i-th device is right-censored at time t, we only know that $T_i > t$, where T_i is the time when the i-th device fails. The consequence is that when considering which devices of age t are "at risk" of failing, we sometimes have to exclude devices for which we do not know whether they failed at age t or not. Depending on whether we need to estimate conditional or unconditional probabilities (see equations (4) and (5)).

6) Survival Models and Kaplan-Meier Estimators: We can rewrite the formula (2) using the hazards λ_t from (3) as

$$P(T = t) = \lambda_t \, (1 - F(t-1)).$$

Thus, it is reasonable to devise an estimator of $P(T = t)$ based on the hazard estimators $\hat{\lambda}_t$ in (4)

$$\hat{P}(T = t) = \hat{\lambda}_t \, \hat{P}(T \geq t) = \hat{\lambda}_t \, (1 - \hat{F}(t-1)), \qquad (5)$$

and estimate the cumulative failure probabilities as

$$\hat{F}(t) = \hat{P}(T \leq t) = \sum_{s \leq t} \hat{P}(T = s). \qquad (6)$$

In survival analysis literature, for the case of discrete integer-valued data, an equivalent relationship based on

$$1 - \lambda_t = P(T > t \,|\, T \geq t) = P(T \geq t+1 \,|\, T \geq t)$$

provides a useful recursion

$$\begin{aligned} P(T \geq t+1) &= P(T \geq t+1 \,|\, T \geq t) \; P(T \geq t) \\ &= (1 - \lambda_t) \; P(T \geq t). \end{aligned}$$

It is more convenient to rewrite the equation in terms of $P(T \geq t)$ as

$$\begin{aligned} &P(T \geq t) = (1 - \lambda_{t-1}) \; P(T \geq t-1) \\ &P(T \geq t) = \prod_{i=0}^{t-1} (1 - \lambda_i), \quad t = 1, 2, \ldots, \text{ with } \lambda_0 = 0. \end{aligned} \qquad (7)$$

The above expression represents one of the basic tools used in survival analysis, and the probability $P(T \geq t)$ as a function of age is usually called the *survivor function*. Its estimator based on $\hat{\lambda}_t$ from (4) is called the Kaplan-Meier estimator:

$$\hat{P}(T \geq t) = \prod_{i=0}^{t-1} (1 - \hat{\lambda}_i), \quad t = 1, 2, \ldots, \text{ with } \hat{\lambda}_0 = 0. \quad (8)$$

7) Remarks on Rigorous Proofs: First, it is important to notice, that the estimators for the survivor function $P(T \geq t)$ and for the cumulative failure probability function $P(T \leq t)$ obtained here are undefined for t bigger than the maximum observed age. This complication represents a common situation in the analysis of censored data.

Secondly, our explanation of estimating the survivor function $P(T \geq t)$ by considering relative frequencies of devices in data subsets dependent on t is only intuitive. The arguments can be made more rigorous by introducing the events

$$K_t = \{\text{device status is known up to and including age } t\},$$

for $t = 1, 2, \ldots$, and considering the following probabilities as estimates that correspond to (1):

$$\begin{aligned} \hat{P}^*(T = t) &= P(T = t \,|\, K_t) \\ &= P(T = t \,|\, T \geq t, K_t) \; P(T \geq t \,|\, K_t) \text{ , and} \\ \hat{P}(T = t) &= P(T = t \,|\, T \geq t, K_t) \; P(T \geq t \,|\, K_{t-1}). \end{aligned}$$

The argument can then be made that $P(T \geq t \,|\, K_{t-1})$ is able to utilize more data than $P(T \geq t \,|\, K_t)$, because for the age $t-1$ there is less censored (excluded) data than for age t.

8) Continuous Survival Models: For continuous-time data, the hazard functions are usually defined in the literature as

$$\lambda(t) = \lim_{\Delta t \to 0} \frac{P(t \leq T < t + \Delta t \,|\, T \geq t)}{\Delta t}. \qquad (9)$$

They are viewed as the instantaneous rate of device failures (or other "death" events appropriate for the study at hand). Estimates for the survivor functions become more complicated, but are driven by similar ideas as in this example.

Most importantly, the survivor function estimator (8) used here has been derived rigorously by Kaplan and Meier in 1958 as a generalized non-parametric maximum-likelihood estimator for both, discrete and continuous-time survival data. A more detailed discussion of the estimator can be found in the literature, e.g. in [8], [9], [10]. We utilize these estimators in Section III-D.

C. Observed Data and Missing Information Treatment from the Survival Analysis Viewpoint

The data at hand represents the service records of components of the Track Circuit Systems from 130 locations. In each system, several components of each type were in operation and the times and types of their failures were recorded. Non-functioning components were being replaced by new ones, therefore we regard the times between their failures as independent and identically distributed random variables. The failure times are reported rounded to days. However, without a significant loss in accuracy, we treat the data as having a continuous distribution. We aim to estimate this distribution based on the methods described in the previous part.

Each component is considered separately, as their failures generally do not influence each other. For each device we considered several failure types as described in section II-C. However, we did not distinguish between them as we are interested in the time to the first failure, regardless of which

kind of failure it may be. If needed, it would be possible to utilize the competing risks models (see [11]) to differentiate between them.

Possibly due to the lack of unified guidelines for the record-keeping, the data is incomplete at some points. Therefore the models had to be adjusted accordingly:

1. For several stations, the start of operation was not recorded. The age of the device when the first failure occurred was therefore not clear and needed to be included in the model by means of left censoring.

2. Some failure records were not correctly assigned to a station, but to a track section between two stations, with no indication in which of the two stations the failure actually occurred. In this case, we decided to assign the failures to both stations, but with a probability of one half to each.

3. If there were multiple parallel devices of the same type at one station, it was generally not recorded which of them has failed at a given time. Therefore it was not possible to distinguish e.g. whether only devices in one slot kept failing or whether devices among all slots were failing at a similar rate. For this case the failures were assigned to the possible devices at random.

In the next section we use this methods to establish an estimating procedure.

D. Likehood-based Survival Model for Incomplete Data

The estimation of the time-to-failure distribution is performed using the maximum likelihood approach, maximizing the joint probability density of the observed data modified for censoring.

Using the extensions of the survival modeling techniques from above, we want to establish a likelihood function which would describe the data well and estimate its components.

We observe N stations with n devices altogether. For each device, n_i failures were observed occuring at times t_{ij}, $i = 1, ..., n$, $j = 1, ..., n_i$. Because the parts are replaced after a failure, the times between failures $T_{ij} = t_{ij} - t_{i,j-1}$ form a random sample from a non-negative distribution with a distribution function F, density function f and survival function $S = 1-F$. Denote Δ_{ij} the right-censoring indicators, with $\Delta_{ij} = 1$ if the j-th observation of the i-th device is an uncensored failure and $\Delta_{ij} = 0$ if it is a censored observation.

For our data, the last time-point for each device, t_{i,n_i}, corresponds to the closing of the study on December 31, 2016. At this point all devices were operational, and thus we consider the last observed time as right-censored.

If no missing data were present, the likelihood could then be obtained as a product of densities at the uncensored time points and survival functions for censoring (see [9]):

$$\begin{aligned} L &= \prod_{ij:\Delta_{ij}=1} f(T_{ij}) \prod_{ij:\Delta_{ij}=0} S(T_{ij}) \\ &= \prod_{i=1}^{n} \prod_{j=1}^{n_i} f(T_{ij})^{\Delta_{ij}} S(T_{ij})^{1-\Delta_{ij}}. \end{aligned} \tag{10}$$

There are two approaches for estimation possible. The distribution may be either parametrized and its parameters estimated by directly maximizing L, or the distribution may be estimated nonparametrically using the Kaplan-Meier estimator (8) introduced in the last section (see [10]).

We need to adjust the likelihood to accomodate for the missing data using approaches from above:

1) Missing starting times: Suppose that the first failure of the i-th device occurs at t_{i1}. If we did not know the time when the corresponding station was put into operation, we searched the data for a first recorded failure of any kind occurring at the station. Denote its time point as t^a_{i0}. If it was of a different type, the device surely was in operation before the first failure for longer than $t_{i1} - t^a_{i0}$, which represents left-censoring. Moreover, the device was in operation for a shorter time than $t_{i1} - t^0_{i0}$. Here t^0_{i0} corresponds to January 01, 2006, before which there were no devices in operation. Thus the likelihood contribution of the first observation at a station amounts to $f(t_{i1} - t_{i0})$ if the starting time t_{i0} is known, $F(t_{i1} - t^0_{i0}) - F(t_{i1} - t^a_{i0})$ if the starting time is unknown but there was a different previous failure and $F(t_{i1} - t^0_{i0})$ if there was not.

Even if a previous recorded failure time was available, the age of the device at t^a_{i0} is impossible to determine, we just know that it was operating for at least $t_{i1} - t^a_{i0}$ hours before failing. The corresponding likelihood part provides a conservative estimate, considering the device as new at t^a_{i0}. If the distribution of the data is exponential and therefore memory-less, we can view this as a case of right censoring because the age does not depend on the direction of the time obseravtion.

2) Unclear assignment of a failure to station: When the failures were reported to a track section instead of a station, we assigned them with a probability of 1/2 to each station at the section endpoints. Suppose that such a misreported failure occurred as j-th on the device i. The likelihood contribution of the j-th and j+1-th failure is then

$$\frac{1}{2} f(t_{ij} - t_{i,j-1}) f(t_{i,j+1} - t_{ij}) + \frac{1}{2} f(t_{i,j+1} - t_{i,j-1}),$$

because we do not know, if the device failed and was replaced at t_{ij}, or if it was actually functioning for the whole time from $t_{i,j-1}$ to $t_{i,j+1}$.

3) Multiple devices per station: The service records did not make a distinction between multiple parallel devices installed at one station. For instance, there were three TCR units for each system and at some larger stations, there were several independent track circuit systems. One way to deal with this would be to establish all possibilities of assigning failures to the devices as above, and include their likelihood contributions using probabilities. This proved computationally unfeasible, as distributing n failures among r devices provides r^n possibilities. Instead, we assign the failures to devices at random at the beginning of the computation. Because the results are dependent on the assignment, we repeat the procedure 100 times and take the average outcomes.

Using this modifications, we establish the likelihood function, which, when inserting a parametrized density and distribution function, could be maximized to obtain parameter estimates. Under certain regularity conditions, the estimates have desirable properties such as consistency and asymptotic normality [9].

If additional information on the parts was available, such as train frequency on the monitored track section or the mean temperature and precipitation in the region, we could use survival regression models to study the dependence of the time to failure on such explanatory variables (see [12] or [13]). If the parts were not replaced by new components after a failure, but were instead repaired and put to use again, it would be possible to employ models for incomplete repairs and maintenance actions. It was suggested (see [14]), that after each subsequent failure or maintenance, the failure rate may increase or decrease and therefore the device can be respectively more or less prone to subsequent breakdowns. Similarly, the device may also start internally aging slower or faster after each breakdown, see [15]. The influence of failures and possible maintenances then can be incorporated into the likelihood and their extent estimated.

The nonparametric estimator of the survival function (8) is not available outright under these modifications. For interval-censored data, the Kaplan-Meier estimator generalization was considered by [16]. The random assignment of stations to track segments and failures among devices can be viewed as an application of the Expectation-minimization algorithm [17], producing a consistent estimate when taking an average of multiple assignment possibilities. The proper establishment of asymptotic properties and uniform convergence requires a more in-depth approach using counting process theory, see [18]. For comparison, we obtain the estimate when disregarding the problematic starting points and assigning the stations to track segments randomly.

The variance of the Kaplan-Meier estimator can be found using the Greenwood's formula [9]:

$$\mathrm{var}\hat{S}(t) = (\hat{S}(t))^2 \sum_{T_i \leq t} \frac{\hat{\lambda}_i}{r_i(1-\hat{\lambda}_i)},$$

where d_i is the number of failures at time T_i, r_i is the number of devices at risk at T_i and $\hat{\lambda}_i = \frac{d_i}{r_i}$. The corresponding $(1-\alpha)\%$ confidence interval is then $\hat{S}(t) \pm 1.96 \cdot \sqrt{\mathrm{var}\hat{S}(t)}$. The uniform confidence band around $\hat{S}(t)$ can be obtained using a Hall-Wellner type approach [8] and can be then used or testing of the shape of the distribution.

In the next part, we show the results when fitting most commonly used survival distributons.

IV. Results of Data Analysis

We focused on critical parts of the signaling system as described in section II-B: PCB (power circuit breaker), RCT (rectifier), TCR (track circuit receiver), PSB (power switchboard) and CSB (communications switchboard). There were other parts involved in the system, but no failures were recorded during the study and their life-time distribution could not be reasonably estimated.

The number of device installations in the study along with the number of failures and censored observations can be seen in Tab. V. Some devices were present from the beginning of the study and some were put into operation later. We see that there are not many actual noncensored failures for some parts, which can make the results of the estimation inaccurate.

TABLE V
NUMBER OF DEVICES, FAILURES AND CENSORING TYPES FOR EACH PART

		number of occurrences of censoring types			
part	devices	noncens.	left	interval	right
PCB	165	4	1	33	132
RCT	472	2	1	69	403
TCR	2073	268	14	88	1994
PSB	691	32	0	35	656
CSB	691	15	1	34	657

A. Parametric analysis

The likelihood function constructed in the last section was used to obtain estimates of parametric models. The logarithm of L was used, because it turns products into sums, which are more computationaly feasible.

Beside the density and distribution or survival functions, the *failure rate* (intensity) or *hazard rate* $\lambda(t)$ (see section II-A) is explored, because it determines the immediate limit probability of failure.

We compared the exponential, Weibull, gamma and log-normal distributions. Their densities $f(t)$, survival functions $S(t)$ and failure rates $\lambda(t)$ can be seen in Tab. VI, where ϕ and Φ denote the density and distibution functions of the standard normal distribution, $\Gamma(a)$ is the gamma function and $\Gamma(a, \lambda t)$ its upper incomplete variant.

TABLE VI
CHARACTERISTICS OF THE USED PARAMETRIC DISTRIBUTIONS

distribution	density	survival function	intensity
exponential	$\lambda e^{-\lambda t}$	$e^{-\lambda t}$	λ
Weibull	$a\lambda^a t^{a-1} e^{-(\lambda t)^a}$	$e^{-(\lambda t)^a}$	$a\lambda^a t^{a-1}$
gamma	$\frac{\lambda^a}{\Gamma(a)} t^{a-1} e^{-\lambda t}$	$\frac{\Gamma(a,\lambda t)}{\Gamma(a)}$	nonsimple
log-normal	$\frac{1}{\sigma}\phi(\frac{1}{\sigma}\frac{\log t-\mu}{\sigma})$	$1-\Phi(\frac{\log t-\mu}{\sigma})$	nonsimple

The Weibull and gamma distributions can be viewed as generalizations of the exponential distribution, as the Weibull density has an additional shape parameter a in the exponent and the gamma density in a polynomial multiplicative part. Both distributions equal to the exponential for $a = 1$. The failure rates are then increasing with time when $a > 1$ or decreasing with $a < 1$. The log-normal distribution can be viewed as $\exp(Z)$, where Z has the normal (Gaussian) distribution with mean μ and variance σ^2.

After obtaining the parameter estimates for Weibull or gamma distributions, it is also possible to perform a statistical test of the hypothesis whether $a = 1$ or whether it differs significantly. We use the likelihood ratio approach. If we observe

the log-likelihood $l = \ln L$ at the estimated parameters, then under certain the regularity assumptions it holds that

$$-2 \cdot \Big(\ln\, L(\hat{\lambda}, 1) - \ln\, L(\hat{\lambda}, \hat{a}) \Big) \overset{n\to\infty}{\longrightarrow} \chi^2_1.$$

Thus if the term at the left-hand side is larger than the $1-\alpha$ quantile of the chi-square distribution with one degree of freedom, we can reject the hypothesis on the level of significance α and conclude that the parameter a provides a significant improvement of the fit over the exponential distribution. The output of the test is then the p-value, determining the smalles α for which we could reject the hypothesis with given data. The results can be seen in Tab. VII.

TABLE VII
PARAMETRIC ESTIMATES OF TIME-TO-FAILURE DISTRIBUTIONS

part	dist	log-lik	$\hat{\lambda}$	$\hat{a}$	p-val
PCB	ex	-49.77	1.07e-05	–	–
	wb	-48.34	2.49e-07	0.49	0.091
	ga	-48.33	1.83e-07	0.49	0.090
	ln	-48.53	$\hat{\mu} = 19.22$	$\hat{\sigma} = 5.85$	–
RCT	ex	-33.55	2.6106e-06	–	–
	wb	-32.18	1e-09	0.39	0.097
	ga	-32.18	7e-10	0.39	0.098
	ln	-32.11	$\hat{\mu} = 26.56$	$\hat{\sigma} = 7.57$	–
TCR	ex	-2827.95	4.84e-05	–	–
	wb	-2786.89	1.25e-05	0.61	< 0.001
	ga	-2787.57	8.63e-06	0.59	< 0.001
	ln	-2783.46	$\hat{\mu} = 11.93$	$\hat{\sigma} = 3.42$	–
PSB	ex	-382.44	1.75e-05	–	–
	wb	-377.12	2.83e-06	0.62	0.001
	ga	-377.14	2.23e-06	0.61	0.001
	ln	-377.14	$\hat{\mu} = 14.83$	$\hat{\sigma} = 4.11$	–
CSB	ex	-154.58	6.58e-06	–	–
	wb	-148.89	5.30e-08	0.43	0.001
	ga	-148.9	3.87e-08	0.43	0.001
	ln	-148.5	$\hat{\mu} = 20.83$	$\hat{\sigma} = 6.15$	–

For each component we see the achieved log-likelihood, the parameter estimates for the fitted distributions and the p-value of the test for $a = 1$ for Weibull and gamma distributions. For PCB the and PSB, the Weibull and gamma distribution provided the best fit, whereas for CSB, RCT and TCR the log-normal distribution achieved the largest likelihood. The parameters a of the Weibull and gamma distributions were smaller than one, suggesting, that the failure rate decreases with time. This will be later discussed. For PSB, CSB and TCR, the parameters a are even statistically significantly different from one, because the corresponding p-value of the test is smaller than 0.05. For parts PCB, CSB and RCT, the estimates may not be reliable because of a small number of actual observed failures. The intensities of used distributions with estimated parameters for TCR can be seen on Fig. 3.

In Tab. VIII, we see the main characteristics of the estimated distributions measured in days. The distributions are defined on the non-negative region and are rather heavy tailed, the life expectancy is larger than the median. As the failure rate is decreasing ($\hat{a} < 1$ for Weibull and gamma distributions), the expected time to failure is larger than for the exponential disitribution. Because only a small percentage of the devices were observed to have a failure during the 11 years of study

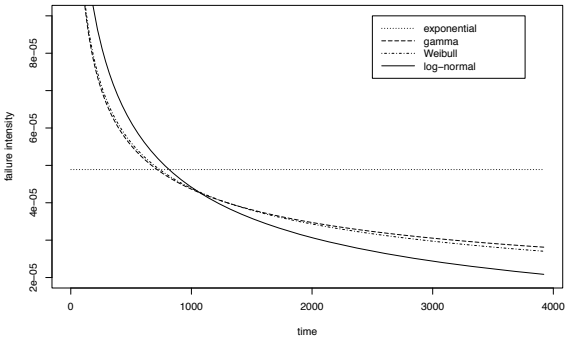

Fig. 3. Estimated parametric failure rates for TCR

TABLE VIII
ESTIMATES OF CHARACTERISTICS OF THE TIME-TO-FAILURE DISTRIBUTIONS IN DAYS

part	dist	expectation	median	95%crit.val
PCB	ex	93181	64588	4780
	wb	8.28e6*	1.91e6*	9625
	ga	2.68e6*	1.19e6*	9415
	ln	5.84e15*	2.21e8*	14758
RCT	ex	383047	265508	19648
	wb	3.68e9*	3.97e8*	487647*
	ga	5.56e8*	1.95e8*	465950*
	ln	9.24e23*	3.43e11*	1.35e6*
TCR	ex	20671	14328	1060
	wb	117859	43632	603
	ga	68627	35787	612
	ln	5.30e7*	152350*	546
PSB	ex	57020	39523	2925
	wb	515409	194494	2810
	ga	273147	145122	2725
	ln	1.27e10*	2.76e6*	3209
CSB	ex	152072	105408	7800
	wb	5.01e7*	8.10e6*	19959
	ga	1.11e7*	4.38e6*	18711
	ln	1.77e17*	1.12e9*	45564

(see Tab. V), the prediction beyond this bounds is only model based and **cannot be validated** by any means. The expectation and the median are therefore rather inaccurate estimates and **should not be regarded as applicable**. As such, they are marked by an asterisk (*) in Tab. VIII. We can, however, estimate the probabilities of the device not failing until time t, or reversely, finding points before which the devices will not fail with a large probability. In Tab. VIII, we thus also give the time point, which the devices will survive with a 95% probability. Clearly, the TCR is the most prone to failure among all observed parts.

B. Estimating the Survival Function

The survival function $S(t) = P(T > t)$ can be estimated either by inserting the likelihood estimates into a parametric model or nonparametrically by means of the Kaplan-Meier estimator. This way we can obtain the probabilities that the studied device will survive beyond any point t in the observed

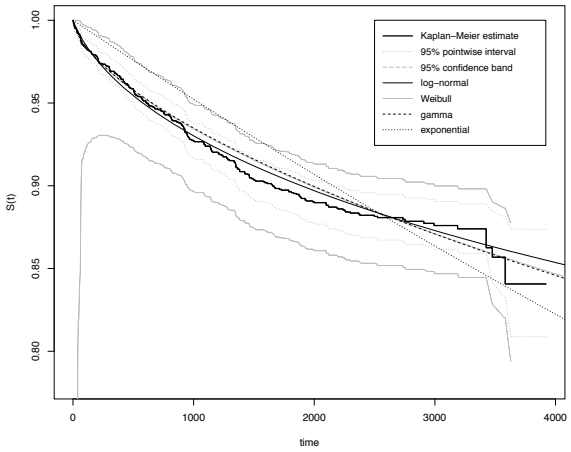

Fig. 4. Kaplan-Meier estimate of the survival function for TCR

time frame. We can construct its confidence intervals and bands using the approaches from section III-D.

The estimated survival function at 1000, 2000, 3000 and 4000 days is displayed in Tab. IX. For other parts than TCR, the probability that the device will be in operation for more than 1000 days before a failure does not drop below 95%. After that, the estimates for some parts are unavailable, because of no observed failures beyond certain time point.

TABLE IX
SURVIVAL PROBABILITIES OF OBSERVED DEVICES

	Probability of surviving for more than			
part	1000 days	2000 days	3000 days	4000 days
PCB	98.7%	97.9%	96.8%	–
RCT	99.6%	–	–	–
TCR	92.8%	88.9%	87.6%	84.4%
PSB	97.5%	95.6%	95.2%	–
CSB	98.0%	97.7%	–	–

On Fig. 4, we see the Kaplan-Meier estimator of the survival function for the TCR units, along with 95% pointwise confidence intervals and uniform confidence bands. The fitted parametric distributions are also displayed for comparison.

We see that the log-normal distribution gives the best fit as their curves are closest to the nonparametric estimate. The exponential survival function is larger at the start of the observation and becomes smaller with increasing time, while the opposite is true for the other survival functions. Because the estimated survival function does not lie in the confidence bounds at all time points, the commonly used **exponential distribution does not provide a sufficiently precise fit** for the data.

In accordance with Tab. VIII, with a 95% probability, a TCR device will survive for more than approximately 600 days. The sudden decrease near the end of observation corresponds to an increase in the failure rate when the age of the parts is nearing 11 years.

C. Discussion of the results

As the majority of the devices did not fail in the observed time frame, we do not have means to accurately predict their life expectancy beyond certain time. We compared several commonly used parametric models, which provided a reasonably good fit on the observed interval, but the applicability of the models outside of this interval cannot be validated. So far there were no similar studies performed, which could be used to compare the results and the estimation performance of the models. It is also not possible to use the non-censored data as a benchmark for validation, because not using censored observations would bring a considerable bias in the results.

Because the failure rate at the observed interval appeared to be decreasing except for at the end, one could suspect that a bath-tub shaped intensity may actually be applicable. This would mean that after some future time point, the number of failures would again rise. This may be hinted at by the decrease of the survival function near the end of the observation. As the data was relatively recent at the time of current analysis, an other possibility is that there was a change in failure recording methodology or other inconsistencies, which must be further investigated. Further behavior will be possible to detect when more data becomes available as an update to the study, or if an accelerated life testing experiment was performed (see [19]).

V. CONCLUSION

In this work we have studied the electronic railway safety signaling devices and explored the ways how to model their reliability. Statistical analysis of the service records of the track control system devices concerning 11 years of operation was performed. We used and extended methods of reliability and survival analysis, which are suitable for dealing with data which is incomplete because of censoring. We compared the results of parametric models of failure rates and nonparametric estimation of the survival function. We were able to find the distribution of the time-to-failure in the observed time frame, therefore when a new device is put into operation, it is possible to predict its behavior in the first 11 years. Beyond that age, due to modeling limitations and lack of relevant data, reasonable statistically confirmable predictions are not available. The early trend in the data suggests that the failure rate decreases with time, but in the last two of the observed eleven years, there may be a reverse tendency, possibly producing a bathtub failure rate. These concerns should be further investigated, so that that measures could be taken to prevent unexpected failures of the devices.

ACKNOWLEDGMENT

This research has been partially supported by the grants: SGS17/213/OHK3/3T/18 (CTU), LG15012 (MSMT) and GA16-05179S (GACR).

REFERENCES

[1] M. Daňhel, H. Kubátová, and R. Dobiáš, "Predictive analysis of mission critical systems dependability," in *2013 Euromicro Conference on Digital System Design*, Sept 2013, pp. 561–566.

[2] Z. Vintr, D. Vališ, M. Vintr, and J. Hlinka, *Analysis of Reliability and Safety in Practice*. CSJ Brno, 2009.

[3] I. Koren and C. Krishna, *Fault-Tolerant Systems*. Elsevier Science, 2010.

[4] "EN 50126 – railway applications – the specification and demonstration of reliability, availability, maintainability and safety (RAMS)," European Commitee for Electrotechnical Standardization, Tech. Rep., 1999.

[5] *Electronic Reliability Design Handbook – MIL-HDBK-338B*. US Department of Defense, 1998. [Online]. Available: http://www.weibull.com/mil_std/mil_hdbk_338b.pdf

[6] *Reliability Prediction of Electronic Equipment – MIL-HDBK-217F Notice 2*. US Department of Defense, 1995. [Online]. Available: http://www.weibull.com/mil_std/mil_hdbk_217f_2.pdf

[7] *FIDES: general presentation*. [Online]. Available: https://cct.cnes.fr/system/files/cnes_cct/459-mce/public/07__FidesEurocalce.pdf

[8] J. D. Kalbfleisch and R. L. Prentice, *The statistical analysis of failure time data*. John Wiley & Sons, 2011, vol. 360.

[9] D. R. Cox and D. Oakes, *Analysis of Survival Data*. CRC Press, Jun. 1984, google-Books-ID: Y4pdM2soP4IC.

[10] E. L. Kaplan and P. Meier, "Nonparametric Estimation from Incomplete Observations," *Journal of the American Statistical Association*, vol. 53, no. 282, pp. 457–481, Jun. 1958.

[11] A. Tsiatis, "A nonidentifiability aspect of the problem of competing risks." *Proceedings of the National Academy of Sciences of the United States of America*, vol. 72, no. 1, pp. 20–22, Jan. 1975.

[12] D. R. Cox, "Regression Models and Life-Tables," *Journal of the Royal Statistical Society. Series B (Methodological)*, vol. 34, no. 2, pp. 187–220, 1972.

[13] J. Buckley and I. James, "Linear Regression with Censored Data," *Biometrika*, vol. 66, no. 3, pp. 429–436, 1979.

[14] D. F. Percy and B. M. Alkali, "Generalized proportional intensities models for repairable systems," *IMA Journal of Management Mathematics*, Jul. 2005.

[15] P. Novák, "Regression Models for Repairable Systems," *Methodology and Computing in Applied Probability*, vol. 17, no. 4, pp. 963–972, Dec. 2015.

[16] J. Huang and J. A. Wellner, "Interval Censored Survival Data: A Review of Recent Progress," in *Proceedings of the First Seattle Symposium in Biostatistics*. Springer, New York, NY, 1997, pp. 123–169, dOI: 10.1007/978-1-4684-6316-3_8.

[17] A. P. Dempster, N. M. Laird, and D. B. Rubin, "Maximum Likelihood from Incomplete Data via the EM Algorithm," *Journal of the Royal Statistical Society. Series B (Methodological)*, vol. 39, no. 1, pp. 1–38, 1977.

[18] T. R. Fleming and D. P. Harrington, *Counting Processes and Survival Analysis*, 2nd ed. Hoboken, N.J: Wiley, Aug. 2013.

[19] W. Nelson, "Accelerated Life Testing - Step-Stress Models and Data Analyses," *IEEE Transactions on Reliability*, vol. R-29, no. 2, pp. 103–108, Jun. 1980.

Appendix C

The Effect of the Transient Faults in Dependability Prediction

This article was published in the *Journal of Microprocessors and Microsystems Embedded Hardware Design* in 2017. This article is extended version of the paper on the same topic published at the *Euromicro Conference on Digital System Design* in Cyprus in 2016.

Microprocessors and Microsystems 52 (2017) 498–504

Contents lists available at ScienceDirect

Microprocessors and Microsystems

journal homepage: www.elsevier.com/locate/micpro

The effect of the transient faults in dependability prediction

Martin Daňhel*, Filip Štěpánek, Hana Kubátová

Czech Technical University in Prague, Faculty of Information Technology, Thákurova 9, 160 00 Prague, Czech Republic

ARTICLE INFO

Article history:
Received 11 January 2017
Accepted 6 May 2017
Available online 10 May 2017

Keywords:
Markov models
Permanent fault
Reliability
Transient fault
Triple modular redundancy

ABSTRACT

Markov chain models are used to evaluate the dependability properties (reliability, safety, availability, maintainability etc.) of the mission-critical systems. Dependability models are often focused only on the basic stuck-at faults. On the other hand the transient faults are present in the operational environment but not included in the dependability prediction. The aim of this paper is to show how the transient faults influence the dependability prediction using the Markov chain model. In this paper basic TMR Markov chain model using stuck-at faults is compared to our extended TMR model considering both the stuck-at and transient faults. The main focus is given on the calculation of the dependability parameter lambda (i.e. the failure rate of the system).

1. Introduction

Fault tolerant operation is a top priority in the field of the safety-critical systems. Such systems require correct behaviour in spite of faults generated by the environment to ensure the quality of the service and the safe operation to prevent undesired injuries or damage to the property.

These systems implement redundancy to detect (or possibly correct) the negative effects of faults caused by the hostile environment. According to the implementation, the redundancy can be divided into area, information or temporal redundancy.

Area redundancy is used in situations, where the design is not constrained by the area requirements. This approach duplicates HW parts of the system and then uses voting mechanism to detect or even correct faults (duplex approach, TMR – Triple Modular Redundancy approach). By adding parity bits or by using some kind of error-detection-codes an information redundancy is achieved. This type of implementation might have lower area requirements but may also lower fault-detection properties.

In case the area redundancy cannot be used (for example by the high area constraints), temporal redundancy can be used instead. Temporal redundancy calculates the operation multiple times using the same input and afterwards votes for the correct result by using some kind of voting mechanism.

Fault tolerant systems aim at protecting their operation against faults caused by the environment. Therefore it is presumed, that the fault is generated randomly due to the ageing of the system or by the mentioned environment. On the other hand, during the fault injection attacks the faults are inserted intentionally. Although the maliciously inserted fault is not in scope of this paper, the idea on its generation/creation was influenced by such intentions. In the field of embedded security this is refereed to as fault attack. But the effects of the transient faults can be observed in hazardous environment as well. Even the first fault injections in microprocessors were unintentional, as radioactive particles produced by elements present in packing materials of the microprocessors caused faults [1]. Later the influence of cosmic rays and upper atmosphere was studied on airborne systems [2] and in 1992 faults were inserted by physical means using the laser beam [3].

The malicious faults are mostly inserted by radiation, EM-field or by using the laser beam. These faults are characterized by time and place of the injection; therefore we are speaking in the context of fault attacks about transient faults. Countermeasures presume that the attacker is able to insert multiple faults (higher order fault attacks) and at any time and at any place in the system. For example – the attacker can modify the processed information and later insert fault into the voting mechanism so he can bypass the fault detection mechanism. Countermeasures against fault attacks are inspired by the fault tolerant practices (e.g., by using area/information/temporal redundancy).

The transient fault is not included in dependability prediction of complex (safety-critical) systems – e.g., systems that need to guarantee a certain level of dependability. Selection of mathematical techniques is required to provide a dependability prediction. Analysis may also be performed using other techniques, such as Markov models. These models use stuck-at faults to model system behaviour [4]. At the same time the more precise calculation is achieved the more accurate the dependability prediction can be.

* Corresponding author.
E-mail addresses: martin.danhel@fit.cvut.cz (M. Daňhel), filip.stepanek@fit.cvut.cz (F. Štěpánek), hana.kubatova@fit.cvut.cz (H. Kubátová).

http://dx.doi.org/10.1016/j.micpro.2017.05.004
0141-9331/

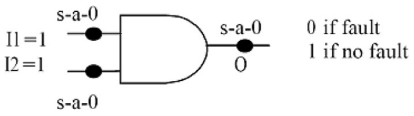

Fig. 1. A simple example of stuck-at zero. The fault this observed for example when both inputs are set to logical 1. Taken from http://nptel.ac.in.

Despite the effect of transient fault is known its influence on the system behaviour is not taken into account in the dependability models. The aim of this paper is to discuss the possible influence of transient faults in dependability prediction used in the field of the safety-critical systems.

2. Dependability assessment

The dependability is a complex property and consists of several terms [5]:

- Reliability
- Availability
- Maintainability
- Testability
- Safety
- Security

This article is primarily focused on the first one (Reliability) and the last two (Safety, Security) terms from the list. The reliability and safety are defined according to the RAMS [6] standard as: Reliability is the probability of a correct component function over a given period of time under a given set of operating conditions. Safety is a property of the system that it will not endanger human life or environment [7]. Or safety is the probability that the product will not have failures belonging to unacceptable seriousness classes, between the initial time and the given time *t*. Security is the next attribute of dependability with regard to the prevention of unauthorized access and/or handling information [5].

The flow above described the different assumptions of the system properties (reliability, safety, security), that cause the requirements to be vastly different. For example: "if the system fails, it must end in a safe state" is in direct contradiction with the fact that someone might attack the system. The system rather destroys itself as it does not want to provide any sensitive information to the attacker. Denial of service is not desirable from the viewpoint of safety.

2.1. Modelling of the reliability

Reliability models used in this paper are constructed assuming that any two different faults will never occur at the same time. Random failures are often modelled using the simple exponential distribution [8]. In contrast, the security must assume multiple failures (attacks) at the same time. In this article we suppose only permanent and transient faults based on classical reliability models.

One of the earliest, and also one of the most widely used fault models, is the single-stuck-at model (shown in Fig. 1). This makes no attempt to model the internal structure of a module but simply proposes that any failing module can be characterized by its external behaviour. The model assumes that a fault within a module will cause it to respond as if one of its inputs or output is stuck at a logic 1 or logic 0. It also assumes that the basic functionality of the circuit is otherwise unaffected and that the fault is permanent. The stuck-at model cannot accurately represent all fault conditions. Indeed, it cannot represent transient or intermittent faults. In this article the transient fault is specified as a fault that has a short lifetime (the effect of the transient fault passes over time), thus there is no need to introduce the repair rate. However, it does permit a large number of faults to be modelled in a simple manner [7]. Since the stuck-at model cannot represent transient faults, the reliability model has to use additional fault model to cover this kind of faults.

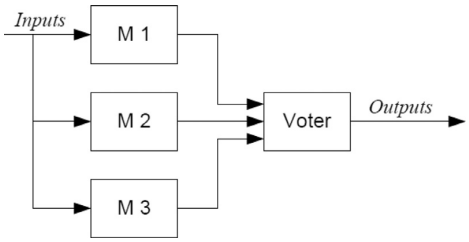

Fig. 2. The TMR consists of three same modules (Module 1, Module 2 and Module 3) and simple voter.

Markov modelling processes are stochastic processes using random variables to describe the states of the process, transition probabilities for changes of state and time or event parameters for measuring the process. A stochastic process is said to be a Markov property if the conditional probability of any future events, given any past events and the present state, is independent of the past events and depends only on the present state of the process. The advantages for using Markov modelling methods include the flexibility in expressing dynamic system behaviour.

The Markov models are widely used to estimate the indicators of the reliability and performance. These models can also be used to represent both kinds of mentioned faults. There are two basic categories of Markov models. First category contains models with one or more absorbing states. It is apparent that these models have "limited time of life". This type of model is solved using a set of differential equations of the first order. The second category contains models without absorbing state. These models can be solved using a set of linear algebraic equations. The analysed case used in this article represents the first mentioned category (e.g., models with one or more absorbing states). Description of Markov models utilization in the area of computer science can be found e.g. in [9].

3. Case study: reliable and secure equipment based on the TMR

Most of the early fault-tolerant systems used duplicated hardware modules. This meant that failure of an individual module would not normally result in a failure of the system. An example of such a system is the triple modular redundancy (TMR). In TMR modules receive identical input signals and therefore should produce identical outputs. A voting mechanism (voter) compares the outputs from all the modules and using the majority function safeguards the correct output. If the output of one of the units (blocks) differs from those of its neighbours as a result of a single fault, the voter will produce an output corresponding to the majority voting scheme. Therefore TMR is able to masks a failure of any single module.

3.1. Basic assumptions for a designed system

In the area of reliability and security TMR is used to mask failures. Fig. 2 shows the block diagram of the embedded system (e.g., encryption equipment). Implementation of the mentioned system is based on FPGA. The diagram consists of the same three modules and a simple voter. It is assumed that the complexity of the voter is more than hundredfold simpler than complexity of the module. Fig. 4 shows that the system works cyclically (repeatedly evaluates the input data and calculates the results).

The following faults are assumed for the mentioned system:

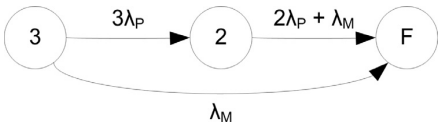

Fig. 3. A simple Markov model with absorbing state representing behavior of the mentioned equipment (TMR).

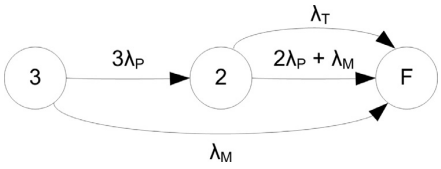

Fig. 4. A simple Markov model with transient fault.

- Permanent fault – stuck-at fault that can occur during a critical part or non-critical part of the calculation.
- Transient fault – single event upset, i.e., fault that can affect memories; it can occur only in a critical part of the calculation.

3.2. Classical TMR model

The state diagram (Fig. 3) represents the Markov model of the mentioned equipment. It is consisted of three modules and a voter. The voter is based on the majority function. This is a classic Markov model that describes the behavior of TMR in terms of reliability.

Description of the Markov model in Fig. 3:

- State 3 means that everything is in order. All three modules and voter are functional.
- State 2 means that one of the three modules is faulty.
- State *F* describes the (fatal) state where the system is no longer able to produce correct result (two out of three modules or the voter is faulty).
- λ_P – failure intensity rate of any module.
- λ_M – failure intensity rate of the voter.

3.3. Extended TMR model

The difference between the Markov models described in Figs. 3 and4 is that the second one (Fig. 4) is designed to model also the transient faults. Model in Fig. 3 does not have this property. However, this model is not accurate, because it does not describe the dependence of transient faults on system status (the considered system works cyclically). The meaning of the states is identical to the previous model; added edge leading from the state 2 to the state *F* emphasizes the added transient fault (λ_T). This fault can be modelled only in the state 2. The transient faults are not taken into account in state 3, because they are repaired automatically.

In this case study the reliability model (shown in Fig. 4) is not suitable for modelling transient faults. In general, the system has critical and non-critical phase of the execution. The effect of the transient fault can be observed only during the critical phase. Therefore the model itself should reflect this fact. The system has two calculation stages. The transient fault does not affect the non-critical part of the calculation.

3.4. Detail of the extended TMR model

The following graph (Fig. 5) describes two time-dependent stages of the mentioned system. The *t* axis describes the operational time; the *S* axis describes the stage (e.g., critical/non-critical

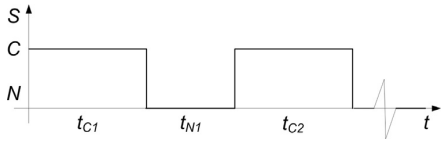

Fig. 5. The system works periodically. The axis *S* means two stages of the system, *C* is critical part of the calculation and *N* is non-critical part of the calculation. The axis *t* means time.

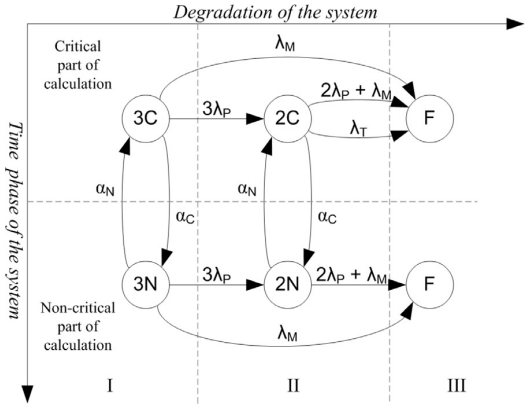

Fig. 6. Detail of the extended Markov TMR model represents permanent and transient faults during the critical and non-critical phase of the execution.

stage of the operation labelled *C* and *N*). The critical stage takes an average period of t_C and the non-critical stage (or inactivity of circuit) takes an average period of t_N. This proposed solution is applicable only if all the periods represented by t_1 (resp. t_2) have the same or similar length. It is assumed that the critical calculation takes roughly the same time.

If the average time (e.g., t_C and t_N) is known, it is possible to determine the mean frequencies (α_C, α_N).

$$\alpha_C = \frac{1}{t_C} \tag{1}$$

$$\alpha_N = \frac{1}{t_N} \tag{2}$$

- α_C – mean frequency of the critical part.
- α_N – mean frequency of the non-critical part.

The proposed extended Markov model of the mentioned system, shown in Fig. 6 in the form of 2D grid, respects the two stages and respects the permanent and the transient faults. In this case study the model is divided into the horizontal and vertical axes. The horizontal axis describes “the level of the system degradation” and the vertical axis describes “the level of the system stage activities”.

Description of the extended Markov model in Fig. 6:

- State 3*C* means that everything is in order. All the modules and the voter are functional in the stage of the critical calculation.
- State 3*N* means that everything is in order. All the modules and the voter are functional in the stage of the non-critical calculation.
- State 2*C* means that one of the three modules is faulty in the stage of the critical calculation.
- State 2*N* means that one of the three modules is faulty in the stage of the non-critical calculation.
- States F_C & F_{NC} mean that the system has failed (two out of the three modules or the voter is faulty). As both F_C & F_{NC} states lead to system failure.

- λ_P – permanent failure intensity rate of any module.
- λ_T – transient failure intensity rate.
- λ_M – failure intensity rate of the voter.

4. Adding states for transient fault

The following issues need to be resolved when including the transient fault into the reliability prediction:

- The final computional complexity.
- The effect of transient fault between the transition.
- The recovery rate - μ.

4.1. The final computational complexity

It is crucial how to insert the transient fault at the beginning of the reliability prediction as this will influence the future estimation/calculation of the Markov chain model for the whole system. At first there was an idea to propose a redundant state for the effect of the transient fault. This was later rejected as this would have significant impact on the complexity of the proposed model. Also due to the operation periods of the system as shown in Fig. 5. The computational complexity is influenced not only by the number of states but also by the number of transitions in the model. It is the goal to keep the final model as simple as possible in order to reduce the complexity.

4.2. The recovery rate – μ and the effect of transient fault between the transition

Another problem is the uncertainty of the recovery rate μ – hard to define in big picture (global overview). This parameter is influenced by specifications and operational requirements of the proposed system. The μ parameter is usually strictly defined by government or industry requirements [9–11]. The μ parameter is known in advance in case it is related to stuck-at faults – usually is defined by technical requirements or government standards. In case of transient faults the μ parameter is hard to define as the behaviour of the transient fault is hard to predict. Regarding the transient fault this parameter is influenced by specific hardware and operational environment. Although μ can be estimated for general purpose models, still it can be omitted. It is presumed that the effect of the transient fault in reliability prediction can be observed when the system is already in degraded stage of execution (Fig. 6). In case a transient fault would emerge in the TMR system in a state where no other fault is observed the negative effect would be masked by the rest of the modules using the majority function. Thus it is presumed that the negative effect would not have any impact on the prediction as it will be recovered by itself in a finite time. Therefore the negative impact of the transient fault is taken into account during the transition from the degraded stage of execution to the failure of the system. In this state (system failure) the recovery rate μ is no longer necessary.

Omitting the parameter μ simplifies the overall prediction and reduces the final computational complexity.

In recent work [12] a similar approach is proposed including the parameter μ (e.g., the recovery rate of the transient fault). Our approach does not include parameter μ as it is not necessary for the calculation of reliability prediction due to the level of abstraction. We do not anticipate 100% workload thus we include periodicity in the model. Due to this only non periodic models (Figs. 4 and 7) are compared. The following items describe the differences between the solution proposed by this paper and similar approach [12].

- Our solution contains less states and edges.

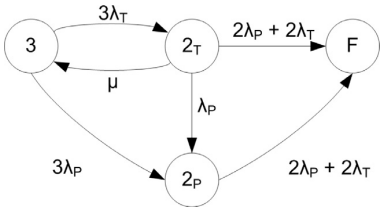

Fig. 7. A Markov model including transient fault according to the [12]. This model also include the recovery parameter μ. The parameter λ_T – is supposed to affect single TMR module only.

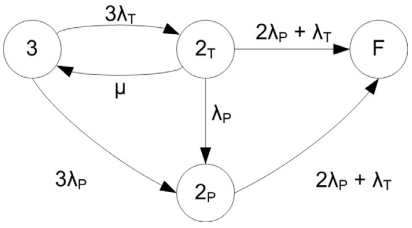

Fig. 8. A Markov model including transient fault according to the [12]. This model has been adjusted so it can be used for comparison with our results. The parameter λ_T – is supposed to affect the whole equipment.

- Our solution takes into account the λ_M – failure intensity rate of the voter.
- In our solution the recovery rate (parameter μ) has been eliminated by simplifying the model. In general this parameter is hard to estimate and can have negative impact on the final calculation.
- Taking into account periodicity in the prediction.
- The transient fault in our solution is related to the equipment as a whole. The solution described in [12] considers λ_T for every single module.

As indicated by the items the difference in the other solution is the usage of parameter μ (omitted by the solution presented in this paper) and the periodicity of the system – the solution presented by [12] supposes 100% system load. Also the cited model described in Fig. 7 has been adjusted so the effect of the transient fault is related to the equipment as a whole. The final model used for comparison is shown in Fig. 8. This approach to the same problem results in comparable results later discussed in Section 5. The authors of this paper emphasized the simplicity of the model in order to propose a reliability prediction with high level of scalability for concrete systems.

Description of the extended Markov model in Fig. 7:

- State 3 means that everything is in order. All the modules are functional.
- State 2*T* means that the present fault is temporary.
- State 2*P* indicates a permanently faulty unit.
- State *F* means that the system has failed.

5. Conditions and numerical solutions

This chapter shows a graphic comparison for all the mentioned Markov models. The system described above has the following parameters:

$$\lambda_P = 3.4 * 10^{-6}[h^{-1}] \quad (3)$$

$$\lambda_T = 2.9 * 10^{-6}[h^{-1}] \quad (4)$$

$$\lambda_M = 6.8 * 10^{-7}[h^{-1}] \quad (5)$$

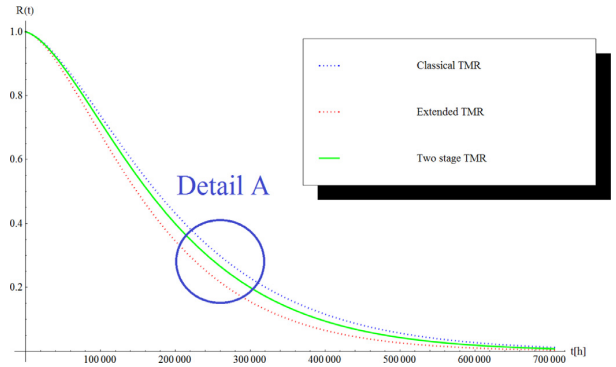

Fig. 9. Comparison of the Markov models. Classical TMR is described in a Section 3.2, Extended TMR is described in a Section 3.3 and Two stage TMR. The axis $R(t)$ is reliability function and the axis t is time in hours. The graph was generated using the Wolfram Mathematica [14].

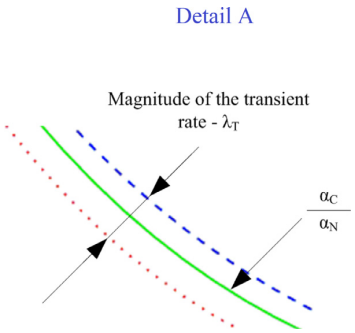

Fig. 10. The detail A of the Fig. 9. The middle curve represents the Reliability function of the two-phases Markov model.

$$\alpha_C = 144,000[h^{-1}] \tag{6}$$

$$\alpha_N = 72,000[h^{-1}] \tag{7}$$

These parameters are merely illustrative. They reflect the existing experiences from the field of dependability prediction of the train infrastructure safety systems [10,13]. The time length of the critical/non-critical calculation is approx. 25 respectively 50 ms. The desired reliability parameters are the failure rate of the whole system respectively the Mean Time To Failure (MTTF) and the course of the function $R(t)$.

Markov models are valid assuming an exponential probability distribution of the time "in the appropriate event" (transition). This is acceptable for the permanent or transient faults (i.e., λ_P, λ_M, λ_T), but not for the events representing the termination stage activities (α_C, α_N). Model can be more accurate (in case of need) if it will divide every stage into the sub-stages. Further details can be found in [11].

Fig. 9 shows that the curves of the Classical TMR (blue dashed curve) and Extended TMR (red dotted curve) create the borders for two stages TMR (green curve). Blue curve is the best case and red curve is the worst case of the reliability mentioned system.

In Fig. 10 is described the detail A of the Fig. 9. The distance between dashed and doted curves depends on the magnitude of the transient rate. The ratio of the values – α_C, α_N affects the position the curve between global extremes. If α_C is greater than α_N then the green curve get closer to the doted red curve.

Similar numerical solution has been performed for a model described in [12]. This model shown in Fig. 7 has been adjusted

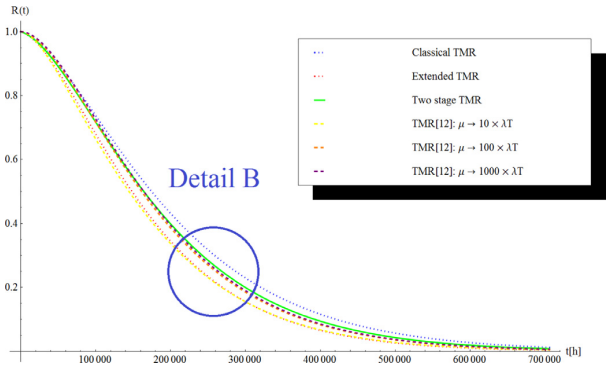

Fig. 11. Comparison of Markov models described in Fig. 9. Numerical solution has been performed for TMR model including transient faults taken from [12].

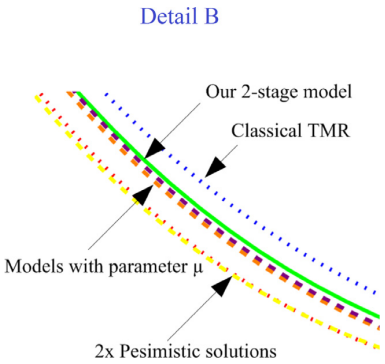

Fig. 12. The detail B of the Fig. 11.

(shown in Fig. 8) so the results are comparable. In order to solve the numerical solutions the parameters described above have been used. Also the recovery parameter μ has been added to the list of used values. The exact value of the parameter is taken from [12]. The result is shown in Fig. 11.

Fig. 12 shows detail B. The solution proposed by this paper is slightly more optimistic. Our most pesimistic solution is comparable with the model proposed by [12] for $\mu = 10 * \lambda_T$. Other cited solutions are more optimistic but more pesimistic than our two staged TMR model that takes into account periodicity of the operation.

6. Conclusion and future work

This paper proposed a new point of view on the interpretation of the Markov model used to predict the reliability of the fault tolerant systems. Traditional approach involved only stuck-at faults models involved in the fault prediction.

The goal of this approach is to predict the dependability of complex systems that need to guarantee a certain level of dependability (safety-critical systems) including the effect of transient fault. The more precise the calculation is the more accurate the dependability prediction can be. The resulting parameters of the prediction might be unnecessarily pessimistic in case the Markov model does not take into account the periodic behaviour of the system. This would result in degradation of the guaranteed level of dependability. At the same time a procedure has been shown on how to design a Markov model for general fault tolerant system consisting of n-redundant blocks and m-phases of execution.

Due to the findings involving the fault attacks authors propose the usage of the transient fault in the fault prediction mod-

els. Ideas presented in this paper will be later used to evaluate the reliability of the architectures used as countermeasures to the fault attacks. Such architectures involve the use of the temporal/information redundancy to prevent the focused intentional attacks on the implementation of the encryption algorithms.

Apart from the mentioned evaluation of the secure architectures the ideas presented might be used to evaluate the temporal redundancy. This redundancy although used in the industry is not widely seen in the reliability calculations.

Acknowledgement

This research has been partially supported by CTU grants SGS16/042/OHK3/1T/18 and GAČR 16-05179S. We would particular like to thank prof. S. Racek for his comments and assistance.

References

[1] T.C. May, M.H. Woods, A new physical mechanism for soft errors in dynamic memories, in: Reliability Physics Symposium, 1978. 16th Annual, IEEE, 1978, pp. 33–40.
[2] J.F. Ziegler, W. Lanford, Effect of cosmic rays on computer memories, Science 206 (4420) (1979) 776–788.
[3] D.H. Habing, The use of lasers to simulate radiation-induced transients in semiconductor devices and circuits, Nucl. Sci. IEEE Trans. 12 (5) (1965) 91–100.
[4] M. Daňhel, Hierarchical reliability block diagrams in the program shamap, in: In POSTER 2011 - 15th International Student Conference on Electrical Engineering, 2011, pp. 25–29.
[5] J.-C. Geffroy, G. Motet, Design of Dependable Computing Systems, Springer Science & Business Media, 2013.
[6] En 50126:2001 railway applications – the specification and demonstration of reliability, availability, maintainability and safety (rams), 2001.
[7] N.R. Storey, Safety Critical Computer Systems, Addison-Wesley Longman Publishing Co., Inc., Boston, MA, USA, 1996.
[8] M. Handbook, Mil-hdbk-338b, US Dpt. Def. 1 (1998).
[9] J. Hlavička, Číslicové systémy odolné proti poruchám, ČVUT, 1992.
[10] Electronic track circuits type koa1, 2016AZD Praha s.r.o. [Online]. Available: https://www.azd.cz/admin/files/Dokumenty/pdf/Produkty/Kolejove/30-KOA-1-ENG.pdf.
[11] V. Vais, S. Racek, Experimental evaluation of regular events occurrence in continuous time markov models, in: Proceedings of the Eleventh International Conference on Informatics, Košice, Slovakia, 2011, pp. 143–146.
[12] S. Scharoba, M. Schölzel, T. Koal, H.T. Vierhaus, On reliability estimation for combined transient and permanent fault handling, in: 14th Biennial Baltic Electronics Conference, Tallinn, Estonia, 2014, pp. 73–76.
[13] M. Daňhel, H. Kubátová, R. Dobiáš, Predictive analysis of mission critical systems dependability, in: Digital System Design (DSD), 2013 Euromicro Conference on, IEEE, 2013, pp. 561–566.
[14] Wolfram mathematica web page., 2016. [Online]. Available: http://www.wolfram.com/mathematica/