**Review of Ph. D. dissertation**

Author: *Ing. Martin Daňhel*

Title of the thesis: *Prediction and Analysis of Mission Critical Systems Dependability*

University: *Czech Technical University in Prague, Faculty of Information Technology and Engineering*

The topic of the thesis is the dependability issue: how to evaluate reliability, availability and safety properties of a designed industrial mission critical computer-based system before proceeding to the manufacturing process or before the construction of the system prototype. The described and developed methods are inspired by up-to-date real world problems and they are based on industrial standards. Therefore the main contribution of the thesis can be declared as an effort how to overcome insufficiency of currently used standards within the process of development of real devices with increased requests concerning their dependability.

An evaluation with respect to the prescribed CVUT/FIT template follows:

1/ Up-to-dateness of the dissertation

The theme of methods, architectures and algorithms aimed to evaluate and to improve reliability and dependability of electronic devices is a subject of scientific research worldwide. The thesis contributes to the state of the art, namely in the area of understanding of general dependability concepts and evaluation methods in the real engineering environment.

2/ Formal structure and organization of the dissertation

The thesis is structured as follows: Chapter 1 - *Introduction* contains author’s motivation and an overview of his previous research in the given area. In the chapter 2 named *Background and State-of-the-Art* basic terms and used models from the dependability area are explained especially in the context of reliability requirements. Chapter 3 – *Heterogeneous Dependability Model* brings author’s original approach how to connect and to evaluate reliability models of various kinds. This approach was published and the key article [A.1] is attached to the thesis as appendix A. The chapter 4 – *Case Studies* contains a description of two different industrial case studies and the problems arising from these studies are discussed. Again the key ideas were published in several articles and the main article [A.5] is attached via appendix B. Chapter 5 – *Modeling of Effect of General Transient Faults* concludes author’s work with the development and evaluation of more realistic models which enable to consider an influence of transient faults and/or time redundancy as a possible tool how to manage transient faults. Author’s approach was published in journal article [A.2] (2017), the full text of this article is attached in appendix C. Chapter 6 – *Conclusion* summarizes the results and suggests possible objectives for further research.

The formal level of the thesis is very good, especially it is necessary to appreciate formal level of figures. There are very little formal mistakes, follows one of them. For a reader is rather confusing the reference on the list of related author’s publications at the beginning of Chap.3, Chap.4 and Chap.5 – there should be … the first (item of the list) is enclosed in App. xx (instead …the last).

3/ Completion of the dissertation objectives
The thesis brings new ideas and practically usable scientific knowledge. Unfortunately the thesis objectives are not explicitly declared within the text of the thesis. But from the part 1.2. (Problem Statement) it is possible to derive the main goal of the thesis as to improve reliability modeling and models evaluation for electronic devices used in the mission critical industrial applications respecting industrial standards. This goal of the thesis can be considered as appropriately satisfied.

4/ Assessment of the methods used in the dissertation

From the scientific methodology point of view it is necessary to appreciate utilization of exact reliability models, which enable further generalization and modification for another similar architectures of mission critical computer based industrial devices. As a formal tool, author mostly uses Markov models, because this kind of models enables to cover an influence of transient faults as well as an influence of periodical activity of the designed electronic module. The validity and usefulness of the developed methods is documented using several examples which use realistic input parameters chosen with regard to author’s previous experience concerning the design of reliable railway control systems.

5/ Evaluation of the results and contributions of the dissertation

The main contribution of the thesis is critical evaluation of the up-to-date used methods for the reliability evaluation of electronic devices aimed for industrial safety-critical applications respecting used industrial standards. Author offers new methods which respect transient faults influence and the possibility to utilize time redundancy (i.e. repeated computation) to mask a transient fault effect. Author’s contribution is more realistic model of a device activity, i.e. his models assume periodical activity of the device with the cycle divided into critical and non-critical parts. Author uses experience obtained during his work upon referenced real industrial projects.

6/ Remarks, objections, notes and questions for the defense

- Due to the fact, that the objectives of the thesis were not explicitly defined and critically evaluated within the text, it should be done during the thesis defense.
- Terminological note: naming of the (three) models used in the section 5.2 is rather confusing – first level (the most simple) model is named either simple (fig. 5.3) or classical (fig 5.7), the second level model is named either simple with transient fault effect (fig. 5.4) or extended (fig 5.7) and the third level model is named either extended (fig 5.6) or two stage (fig 5.7). It should be improved within the presentation or discussed during the defense.
- The considered and modeled system works periodically (fig.5.5). The resultant effect of transient faults on reliability parameters values like R(t) will then depend on the ratio ts/tc. This dependence should be discussed during the defense.
- Two system architectures and corresponding models are analyzed in sections 5.2. and 5.3. Basic input parameters are the same (5.2.1, 5.3.1). My recommendation is to do a cross comparison (and corresponding discussion) during the defense, i.e. either to add one more column for MTTF in the table 5.1 or to merge curves for R(t) from the fig.5.7 and the fig.5.15 within one comparing figure.
7/ The overall evaluation of the dissertation – an overview

The thesis reflects state of the arts in the given area of computer science and it brings new results and outcomes in the form of usable methods presented in valuable scientific publications. The submitted thesis fulfills the requirements for a Ph.D. scientific work and general requirements stated by the law 111/1998 Sb. to award the Ph.D. title. I do recommend this dissertation for the Ph.D. defense.

In Pilsen, 30.5.2018

Stanislav Racek, Associate Professor
Univ.of West Bohemia in Pilsen
Faculty of Applied Sciences,
Univerzitní 22, 30614 Plzeň
Review Report

For the PhD Thesis “Prediction and Analysis of Mission Critical Systems Dependability”

by Martin Daňhel, Czech Technical University in Prague

The topic of Martin Daňhel’s dissertation, dependability analysis, is highly timely. The emerging technologies applied in nanoelectronic devices are increasingly vulnerable and prone to effects such as aging and radiation. To that end, the proposal in this thesis to extend the traditional dependability analysis approaches towards transient faults has significant value.

The dissertation report is written on 84 pages. It includes Introduction, Background and State of the Art and three sections presenting the author’s contribution. Three publications are attached as appendixes to the thesis report.

Section 1 presents the Introduction. It is written with a personal viewpoint. Subsections include titles such as “My Motivation”, “Progress of My Research”. While one could expect something more general and motivation to the society etc, I found the fact that the author has provided his personal history and motivation in such a detail quite useful.

Section 2 of the thesis includes a detailed overview of the background. It serves as a tutorial on dependability concepts, definitions and terminology. It is followed by a very thorough overview of existing standards and methodologies. An overview of related works, in a classical sense, is missing. Subsection 2.9 presents “Previous Results and Related Works”. Unfortunately, it is mostly constrained by the works from the same research group.

Sections 3-5 present the main contribution of the thesis. Section 3 briefly introduces Heterogeneous Dependability Model proposed by the thesis. Section 4 presents two case studies, the Electronic Track Circuit and Eurobalise. It shows that the author has deep knowledge in the standards and practices of dependability field in industry, having worked in several projects with companies. Finally, Section 5 presents the authors contribution in including the effect of transient faults to the dependability analysis. An interesting observation is that transient faults can be neglected if the transient failure rate is less than 1000 times greater than that of permanent failures.

During reading the thesis report, some questions, remarks emerged:

1) Problem statement (Section 1.2) includes a question “Is it possible to use current standards mostly used in industry?”
   What is the question? Industry is using them?
2) Page 12: MTBF is not Mean Time To Failure
3) Figure 2.4, what is the difference between Objective and Intent?
4) Table 2.4 Why isn’t FMEA/FMECA included to the table?
5) Page 37, “Combined systems”. Why isn’t R(t) simply a product of R012, R3, R4 and R5? It is a serial system!
6) Heterogeneous Dependability Model is one of the core contributions of the thesis. However, it is unclear to the reader why is the model called 'heterogeneous'? What is shown in Section 3 is mostly the hierarchical aspect of the model. Where does the heterogeneity come to play?

7) The first sentence of 3.2.2 does not seem to make sense.

8) It is mentioned that some “important aspects and assumptions” from confidential reports are included to the thesis. How was the confidentiality guaranteed?

9) Lines in Figure 4.5 are extremely difficult to differentiate.

10) The last sentence of Section 5.1.1 does not seem to make sense.

To conclude, the author of the dissertation proved the ability to conduct research and achieve scientific results at a high level. In accordance to that I recommend the thesis for the presentation and defense with the aim of receiving the PhD degree.

in Tallinn, June 3, 2018

Prof. Jaan Raik, Tallinn University of Technology
Subject: Ph.D./Dissertation Thesis Review

I made this review upon a request from the Czech Technical University in Prague, Faculty of Information Technology, Department of Digital Design. The request originated from the document with the reference number 68/18/18924, dated on March 12, 2018. The subject of the requested review was the Ph.D./Dissertation Thesis by Ing. Martin Darheli, entitled “Prediction and Analysis of Mission Critical Systems Dependability”.

I structured my review, according to the request, as follows:

1. **Up-to-dateness of the dissertation**: The problem solved in the thesis is clearly defined, is topical and it calls for recent solutions in both academia and industry. As the problem is constantly being solved by various authors/teams worldwide, there is no doubt that the **thesis is up to date**.

2. **Formal structure and organization of the dissertation**: The thesis is well structured/organized. This makes it, along with its thorough writing/presentation style, highly readable. The number of language and other lacks (such as the double definition of MTTF on p. 15.37 or undefined “k” in Fig. 5.15, p. 79) in thesis is negligible and is defeated by a high number of accompanying illustrations/examples, by giving the reasons for assertions stated in the thesis etc. Though I **appreciate** a detailed and readable introduction to key dependability aspects in chapter 2 of the thesis, I **miss** there information about further types of reliability models, such as state-space models (e.g., Markov Reward Models, Semi Markov Processes, Markov Regenerative Processes) and hybrid models (e.g., Dynamic Fault Trees, Dynamic Reliability Block Diagrams, Boolean Driven Markov Processes, Stochastic Petri Nets, Stochastic Activity Networks, Adaptive Transition Systems). Also, I **would welcome** a paragraph discussing analytical and simulation based approaches to the dependability assessment problem.

3. **Completion of the dissertation objectives**: Unfortunately, objectives of the thesis are hidden in the research questions posed in sect. 1.2 “Problem Statement”. A reader of the thesis is expected to deduce the objectives from the questions, the result of which may be ambiguous. In the thesis, I **would welcome to present a hypothesis** that should (or should not) be supported by the objectives. It is a pity, but **neither objectives nor a hypothesis are explicitly stated** in the thesis. With the hope that my deduction was correct, I have come to the conclusion that the objectives were completed.

4. **Assessment of the methods used in the dissertation**: Chosen methods and instruments are appropriate to answer the research questions specified in the thesis. They include i) gathering real data from several years of equipment operation and finding a way of managing such data, ii) searching for real/theoretical problems to solve as well as dealing with their solutions, iii) proposing the Heterogeneous Dependability Model, with the hope that it can facilitate the dependability assessment process, and iv) analyzing dependability attributes under transient faults, with the hope of overcoming lacks of many standards being mostly limited to permanent faults.

5. **Evaluation of the results and contributions of the dissertation**: Conclusions made in the thesis are supported by appropriate results. The results have been critically interpreted and relevant knowledge in the field has been included to a sufficient extent in the interpretation. The main contribution of the thesis comprises several aspects, some of which are listed below. Firstly, the thesis introduces the Heterogeneous Dependability Model (HDM) capable of using a mixture of various model types, such as Fault tree or Markov chain models, to express dependability aspects as precisely as possible. Secondly, the thesis shows a way in which the model can be used to assess dependability attributes assuming, e.g., transient faults and temporal redundancy. Finally, though the thesis builds on real data from industry, focuses to real applications and a limited set of dependability characteristics, its conclusions can be generalized and applied in further areas of interest.

Ing. Josef Strnadlo, Ph.D., RT VUT v Brně Tel: +420 5411411 Email: strnadlo@ffv.vutbr.cz Web: http://www.ffv.vutbr.cz/~strnadlo

Page 1 (of 2)
6. Remarks, objections, notes, and questions for the defense:

(a) Remarks, objections, notes

i. The meanings of "Common" (the title of ch. 5) and "partial failure" (p. 19, par. "Gamma") are unclear.

ii. The attribute "causes no permanent hardware damage" (p. 23) seems redundant to define a transient fault (e.g., consult that with Fig. 2.4 on p. 24).

iii. The meaning of "predictive" is not properly justified. For example, why not simply replace "predictive reliability analysis" (p. 51) by "reliability analysis"?

(b) Questions for the defense

i. How does the computational complexity, and/or execution overheads, of processes over an HDM (such as the model creation process and dependability assessment process) depend, e.g., on HDM attributes?

ii. The thesis refers repeatedly to your database (i.e., the service database of operated devices), but does not provide more information about it. Could you present some information, e.g., about the number of records, types of devices, organization of data etc. in the database?

iii. Do you think it makes sense to model the staying of a transient fault in a system? If so, how would you embed such a functionality into your HDM approach?

iv. In the thesis, your HDM approach is not compared to existing (competitive) approaches, e.g., to those based on hybrid models. Could you make such a comparison?

v. Your thesis state (e.g., in "Abstract and contributions" on p. iii, in sect. 2.2.3 "Availability" on p. 15, in sect. 2.2.5 "Safety" on p. 17 or in sect. 6.1 "Summary") that it deals with reliability, availability and safety. However, after reading the thesis, it is not clear how did you deal with it (e.g., modeling and analyzing) availability and safety. Could you clarify that?

7. The overall evaluation of the dissertation: My evaluation is both heavily and positively affected especially by the high readability of the thesis, its contribution for both industry/academia and finally, by its topicality and by generality of its contribution. The author of the thesis has proven the ability

i) to understand the subject matter and associated literature, ii) to introduce a specific novelty and originality in his approach, iii) to evaluate his approach and to show that his approach is capable of solving problems that are beyond the scope of existing solutions, iv) to justify his conclusions and support them through data and v) to publish his approach in many conference proceedings and, finally, in a journal. In summary, my rating of the thesis ranges from very good to excellent.

8. Statement whether you DO or DO NOT recommend the dissertation for the defense:

The author of the dissertation proved the ability to conduct research and achieve scientific results. In accordance with par. 47, letter (4) of the Law Nr. 111/1998 (The Higher Education Act) I do recommend the thesis for the presentation and defense with the aim of receiving the Ph.D. degree.

Yours sincerely,

In Brno,
on April 9, 2018

[Signature]

Reviewer
Ing. Josef Strnadl, Ph.D.
FIT VUT v Brně

---

Ing. Josef Strnadl, Ph.D., FIT VUT v Brně   Tel: +420 541141211   Email: strnadl@fit.vutbr.cz   Web: http://www.fit.vutbr.cz/~strnadl