REVIEW OF DOCTORAL THESIS

Author: **Edita Djambazova**
Theme: **Study of the dependability characteristics of a fault-tolerant distributed real-time system with adjustable reliability**

Professional field: 5.3 Communication and computer equipment
Doctoral program: "Computer Systems, Complexes and Networks"
Consultant: Associate Professor Dr Rumen Andreev

Reviewer: Associate Professor Dr Peter Popov
Affiliation: Department of „Computer Science“,
City, University of London, United Kingdom

Reason: Order No. 191 / 20.07.2023 of the Director of IICT-BAS.

1. GENERAL DESCRIPTION OF THE THESIS

1.1. Structure and volume

The thesis consists of 134 pages of text, 6 pages of bibliography and 2 annexes with a total volume of 20 pages and includes: an introduction, 4 chapters, a conclusion with a summary of the results obtained and a discussion of future research, a declaration of originality and a bibliography.

The structure and the volume of the thesis present very clearly the ideas and achievements of the author. The text logically goes from a detailed coverage of the background on dependability and real-time systems, as two related and well-established scientific disciplines, through a justification of the research objectives, the results from the research, which include a new approach to creating a fault-tolerant distributed real-time control system with adjustable reliability and a methodology for quantitative reliability assessment of distributed real-time control systems, built with components with different levels of structural redundancy.

The structure of the thesis meets the requirements of the Development of Academic Staff Act in the Republic of Bulgaria (DASA) and the Act for its Institutional implementation (AII) as well as with the requirements for such documents in the UK and several European countries (e.g. Spain, Norway, Italy) with which I am familiar.

The introduction presents:

- The motivation for the research. Multichannel fault-tolerant control systems are built using redundancy (duplication/triple modular redundancy, etc.) resulting in additional delays required to synchronise the operation of the channels of the fault tolerant system. Real-time requirements, on the other hand, impose constraints on processing time and generating control stimuli to the respective actuators. Solving these two requirements at the same time – fault tolerance that does not violate time constraints – is a serious design challenge and is a major motivation for the research conducted.
- Scientific formulation of the study, which includes:
  - Subject of research
  - Objective of the research
  - A working hypothesis that is refined in several statements (research questions), for which confirmation is sought with the conducted studies.
  - Research methodology
  - Main tasks of research.

The *first* chapter provides an overview of the terminology used in the specialized literature dedicated to dependability of computer systems, real-time control of industrial systems. A significant part of the chapter is devoted to the various methods for increasing reliability by introducing redundancy – structural/functional and time – and creating fault-tolerant control systems.

The second chapter covers in detail the modelling of a fault tolerant distributed real-time control system. A detailed model of the distributed system is presented which consists of components with redundancy. The system reliability characteristics are defined and justified. The modelling assumptions are spelled out, too.

The third chapter is central in the thesis and presents the results obtained by using Monte Carlo simulation of the operation of a distributed fault-tolerant system for real-time control using specialized simulation software developed by the candidate. The usefulness of the proposed method for adjustable reliability is illustrated convincingly (more details on results are provided below).

The fourth chapter summarises the results of the conducted research.

1.2. Timeliness and importance of the topic

The timeliness and importance of the topic is beyond any doubts. Distributed real-time processing systems are used very widely in various industrial applications. Systems for safety-critical applications in nuclear industry, critical infrastructures (e.g., power systems, telecommunications, etc.), intelligent systems (robotics, autonomous cars, etc.) are examples where high reliability and real-time control is required. Not all functions in such control systems, however, are equally critical. In these circumstances, it becomes possible to seek high reliability via fault tolerance only for those "critical functions" which affect system reliability substantially. For systems of significant complexity (e.g., with many functions/components), it may *not be obvious* which functions are critical, especially in cases where redundancy can only be assigned to some components of the system. In such cases, developers are faced with a serious design problem of how to allocate available resources (i.e., available modules) to components in a way that leads to the highest system reliability. This problem cannot be solved without the use of quantitative assessment of the available alternatives (i.e., "design space exploration").

The proposed methodology for quantitative reliability assessment and the developed software for Monte Carlo simulation are essential contributions to the solution of the problem of optimal redundancy allocation among system components.

The thesis contains 49 figures and 4 tables that present the results of the conducted research.

1.3. Method of research

The thesis shows convincingly that Mrs. Djambazova has a lasting interest in dependable real-time control systems. She demonstrates competence in formulating a complex research problem, and ability to solve it by using stochastic models for reliability assessment of complex control systems.

1.4. Literature Review

102 literature sources were referenced in the thesis[1]. They cover well the topics of dependability, fault tolerance and real-time control systems. The cited sources, related to stochastic modelling, are also sufficient.

Most of the sources are in English, which shows an excellent awareness of the state-of-the-art in the respective technical areas.

[1] [40] and [41] appear identical.

About half of the references were published in the new century, a significant part – in the last 5 years.

All sources are described according to the official requirements and are cited in the thesis correctly and according to the recommended rules.

2. RESULTS AND CONTRIBUTIONS

The thesis is theoretically oriented. The original results are presented in Chapter 2 and Chapter 3.

The abstract of the Ph.D. thesis presents the work and the results very well.

The most significant results of the work are presented in Chapter 3. For example, Figure 3-37 (on page 90 of the thesis) and the following graphs, showing the results of research on a 20-module system, illustrate convincingly the usefulness of the proposed methodology for quantitative assessment of different configurations for given total number of modules, allowing an adequate comparison of the alternative configurations. Graphs of system reliability show that there is no "stochastic ordering" between the reliability of different configurations, which in turn implies that which of the possible configurations offers the best reliability depends not only on the configuration itself and how the redundancy is allocated to components of the system, but also on the time interval for which system reliability is evaluated and the possible configurations are compared.

Mrs. Djambazova states that the thesis has led to 3 scientific results, 4 scientific-applied results and 1 applied result (simulation program), statements that I accept.

I would like to highlight as *particularly significant* the demonstration that there is no stochastic ordering between the reliability functions of the different configurations created for a given number of modules. This result excludes the possibility for designers to identify a universally "optimal configuration" that would guarantee the best system reliability for a given total number of modules and components, *regardless of the time interval for which the reliability* is evaluated. In practice, this result shows that designing a distributed control system with a given number of modules should include an analysis similar to that proposed in the thesis,

3. EVALUATION OF PUBLICATIONS AND ABSTRACT OF PHD THESIS

Mrs. Djambazova's research has led to 5 publications and inclusion of the results in 2 scientific reports (on projects with external funding).

It is noteworthy that the publications were made over a significant period of time, which demonstrates that the author has long-lasting research interests on the topic of dependability[2].

40% of the publications are written by two authors, one of which is a joint work of the candidate with Dr Djambazov and one – with the supervisor / consultant Assoc. Prof. Dr Andreev.

The abstract of the Ph.D. Thesis summarizes accurately and clearly (within 49 pages) the main ideas of the author. The research achievements and directions for future work, are presented accurately, too.

4. NOTES, QUESTIONS AND RECOMMENDATIONS

Given that the study is focused on adjustable *hardware reliability*, it would be interesting to extend the proposed methodology and take into account the impact of *software* failures. This possibility is included in the thesis as one of the directions for future research.

[2] In confirmation of this statement, I would also like to point out that the list of references includes papers by Mrs. Djambazova, not listed as relevant to the thesis, which she published over the years in co-authorship or on her own.

4.1. Necessary adjustments

I believe that the following corrections to the text of the thesis are ***necessary***[3]:

1. (p.66) "Допуска се, че .... времената до отказ са нормално разпределени".

   C: I believe that this assumption is not needed, and the text should be corrected accordingly.

   > A stochastic model is fully defined by the model structure and the model parameters (failure and recovery rates). The probability distribution of the time to system failure (i.e., to reaching the absorbing state of system failure in the model) can be calculated by "solving" the model, e.g., using Monte Carlo simulation or appropriate numerical methods. Asymptotically this probability distribution should be *exponential* (see Littlewood's work from 1979[4] for the class of semi-Markov models).

2. (p. 71) "Тъй като размерът ѝ е голям (над 40 според изискванията на статистическите пресмятания; в нашия случай размерът на генералната съвкупност е 10^5), според централната гранична теорема [37], [100], [101] може да се допусне нормално разпределение на генералната съвкупност [99]".

   C: This statement needs clarification. It is not clear what random variable the envisaged population represents. Is this a population of times to system failures collected during simulation or of something else? The clarification is necessary so that one can see what the Central Limit Theorem is applied to.

   > The Central Limit Theorem (CLT) applies to the distribution of the *expected value* of a random variable for which a sample of observations used to estimate the expected value of the random variable in question. The CLT applies to random variables of *arbitrary* probability distribution.

3. (p. 71) "Надеждността се изчислява в зависимост от времената до отказ и можем да допуснем ..."

   C: This statement gives the impression that system reliability depends on MTBF and MTTR, but it is not clear whether these are the parameters of the components, the modules or the system.

   > System reliability, of course, depends on the MTBF and MTTR of the components, but could be calculated directly, for example using efficient numerical methods applied to the transition matrix of a specified continuous-time Markov chain. I suspect that the text above is an attempt to make it clear that the model parameters of the Markov chain are related to the MTBF and MTTR of the modules/components used in the system.

4. (p. 80+) X-axis scale is omitted for the figures in section 3.2.2.

   C: Omitted labels on the X axis should be added. I suspect that the interval of values which will appear on X-axis will be [0, 10^5] hours.

4.2. Questions on the Thesis

During the viva I would like to hear answers to the following ***questions***:

1. (p. 19) The thesis includes the following two statements:

[3] Excerpts are used from the thesis in Bulgarian so that the reviews in English and in Bulgarian are consistent.

[4] B. Littlewood, *Software reliability model for modular program structure.* IEEE Trans Reliability, 1979. **28**(3): p. 241-246.

a. “Коректна услуга (correct service) се предоставя, когато услугата прилага системната функция”. ...

b. “Отказ в услугата настъпва или поради отклонението ѝ от функционалните спецификации, или защото спецификациите не описват адекватно системната функция”.

Q. Can you explain what a ***correct service*** *is? Why is there a reference to a* ***system function*** *in the definition? Wouldn't it be more appropriate to use a reference to functional requirements instead? It seems to me that there is a contradiction between the two statements highlighted above. Would you, please, elaborate?*

My doubts are related to the following two aspects:

- deviation of the system behaviour from functional specification (functional requirements) is indeed a system failure. Such deviations should be detected during system *verification* (e.g., by testing) or by monitoring the system operation.

- malfunction due to incorrect functional specification should not be considered a system failure, but a fault of the specification, a problem that would have to be detected and fixed by *validation* of the specification.

2. (p. 21) Fault — forecasting is discussed. The thesis argues that the focus of the work is fault-tolerance.

Q. I would like to hear the candidate’s opinion on the relationship between fault-tolerance and fault-forecasting? In particular, is fault-forecasting necessary when one is designing fault-tolerant systems?

The relationship between fault-tolerance and fault-forecasting is implied in Fig. 1-3 (p.29) where forecasting (or more generally assessment) is shown as an essential part of fault tolerance. Would the candidate agree that the focus of the thesis, therefore, should also include "fault forecasting"?

3. (p.23) “Възлите са ***независими*** елементи, които комуникират помежду си по обща съобщителна среда”.

Q: Would the candidate clarify in what sense the nodes are independent? Is stochastic independence (i.e., nodes’ failures occur independently) envisaged here or something else?

(p.57) “Отказ на системата настъпва, когато ***повече от половината*** компоненти откажат с неоткрит отказ или при повече от половината отказали компоненти броят на тези с неоткрит отказ е по-голям от броя на компонентите с открит отказ”.

Q: What is this assumption based upon? In reliability theory (e.g., when one uses Reliability Block Diagrams, RBD), the concept of "structure function" is used. Structure function is a Boolean function defining the system state ("working/failure") as a function of the states ("working/failure") of the components used in the system. Would not the candidate agree that “structure function” would be appropriate for the work in the thesis, too?

Structure function obviously affects the results of reliability assessment. The "structure function" of systems without redundancy is a Boolean function AND, i.e., the system works correctly only when all components are working. Using components with redundancy, as in the thesis, leads to a structure function which includes Boolean OR(s).

4. (p. 61) "На изходите се поддържа безопасно управляващо въздействие (fail safe) ... Предимството на стоповото състояние е във възможността да се диагностицира по-лесно и бързо причината за отказ чрез информацията от средствата за самопроверка, което намалява времето за престой ".

   Q1: Would the candidate give examples of "fail safe" state?

   A fail-safe state is typically defined at SYSTEM level, e.g., an autonomous vehicle stops. In the thesis a fail-stop state is defined and used at component level. This suggests that during operation, some components may stop sending control signals to the devices (actuators) they control, while the rest of the components may continue to send control signals. It would be useful to give an example of a system in which such an approach with component-level safe states would apply.

   Q2: Would the candidate give an example illustrating how self-checking would be useful in fail-safe condition?

4.3. Recommended corrections

When reviewing the thesis, I took notes about possible improvements of the text, which are summarised below as ***recommendations*** to Mrs. Djambazova. I do not expect a response to these during the viva and leave it to her to decide whether to address any of them in a new revision of the thesis.

1. (p. 46) "Настройваемост е свойството на гарантоспособната разпределена система за реално време да разпределя структурния излишък ***според изискванията за надеждност на приложението***".

   R. It is clear that different components can be assigned different level of redundancy. It remains unclear, however, how the needs of the application for increased reliability will be accounted for. Would be good to see a clarification of this aspect in the thesis.

2. (p. 65) "Единичните компоненти имат най-малък коефициента на покритие – C1. Компонентите с двоен модулен излишък имат коефициент на покритие C2 > C1, а триплираните компоненти имат коефициент на покритие C3 > C2 > C1".

   R: It would be useful to clarify if the inequalities given above are mere assumptions. It would be even better if a justification for the plausibility of these assumptions were added.

3. (p.66) "...Определяне на времената до отказ (one of the outcomes from the studies)".

   R: It would be good to point out explicitly that the probability distribution (e.g., cumulative distribution function) of the time to system failure is used.

   I would also be curious to see if the Littlewood's asymptotic result (the time to failure is exponentially distributed) applies to the conducted studies.

4. (p. 75) "Данните са за следните интензивности на неизправностите и ремонтите: постоянни неизправности на процесор $\lambda_p=10^{-2}$ 1/h, случайни неизправности на процесор $\lambda_t=0.1$ 1/h, възстановяване на процесор след постоянна неизправност $\mu_p=0.1$ 1/h, ремонт на компонент $\mu_c=0.1$ 1/h...."

   R: The values of the rates (intensity) of failure are unrealistically high. The thesis makes it clear that these values have been adopted for "convenience" – to shorten the simulation time. It would be good to see in the thesis a discussion of possible side-effects, e.g., that some of the *model properties such as its "stiffness" may be affected by the "convenient" choice of model parameter values.*

5. I would recommend that the list of references be divided into the traditional categories of monographs, journal/conference articles, reports, etc.

5. CONCLUSION

The thesis "Study of the dependability characteristics of a fault-tolerant distributed real-time system with adjustable reliability", developed by Edita Djambazova under the scientific supervision of Assoc. Prof. Dr Rumen Andreev **meets the requirements for awarding the educational and scientific degree "Doctor".**

I therefore express a positive opinion on the work and strongly recommend that the honourable members of the scientific jury vote in favour of awarding the candidate the sought degree.

На основание ЗЗЛД

5 September 2023
London

Reviewer:
Associate P