

PhD Thesis Review

PhD student: **Peter Raab, M.Eng.**

Study field: **Computer Science and Engineering, Department of Computer Science and Engineering, Faculty of Applied Sciences, University West Bohemia in Pilsen**

Title: **Model-based Reliability Evaluation of Data Processing in HW-Fault-Tolerant Processor Systems**

Submitted thesis contains 5 chapters, followed by 7 author's publications which make the scientific basis of the thesis. Main contributions are summarized in chapter 3 and discussed in chapter 4 in more details. Chapter 5 concludes the thesis and depicted possible continuation and further improvements.

1. Topicality of the thesis' theme with respect to the today state of the art in the presented field

Prediction of the reliability properties in the early stages of development of software system is crucial point in recent research. The correlations between hardware faults and their impact to the concrete software computations is one of the most important challenges of this thesis.

2. Originality and contributions of thesis

The goals of this thesis are clearly specified. There are four contributions (aims):

- Development of an error model for arithmetic operations;
- The comparison of the residual error probability of different codes;
- Reliability evaluation of a tasks data flow;
- Validation of correctness of derived models.

Originality is based on software based reliability evaluations of hardware based faults, analytical approach and very precisely modeled instructions (MOV, ADD and XOR) by Markov chains. It seems to me that here is a lot of work for the future: more complicated instructions (minimally with respect to those which are most frequently used in programs) should be modeled. The used ones seem to be very simple and trivial - but it was necessary to explore them at first and the idea how to do it is original one.

I appreciate not yet published results from 4.2.3.3 section, where the probability of a deadline violation is formally introduced. It is very important for real-time systems designs (almost demands for embedded systems today).

3. Used methods, solving procedures and aim compliance

The methods and evaluations of proposed error models are based on detailed Markov models which are the good base for precise reliability parameters computations. Arithmetic codes and linear codes (as the most usable ones) were studied, possible transformations between them were presented. The validation of proposed method was performed by the simulation of ripple-carry-adder in simplified architecture of R³TOS. The proposed aims were fulfilled.

4. Publications of results and science erudition

The list of publications of author's results is included in a list (pp. 76-77), 7 from them create the organic part of the thesis. The number and quality of publications is sufficient, but all publications have more than 2 (up to 5) co-authors, therefore the mutual ratio of authorship should be stated during the defence.

5. Formal level of the theses

The structure of thesis as concern the chapters' content is adequate. I appreciate that the connection of the theoretical preface and published papers embedded is well balanced and seems to be a good example how to write theses where the most crucial part were published in journals and presented at good conferences.

There are very little formal mistakes (e.g. in word-division in Czech and English Abstracts). Formally the sentence at page 5 "Redundancy means additional functionality being implemented in parallel ..." is immoderate preposition, redundancy can be realized serially too, e.g. by repeated computations.

6. Questions for the defence:

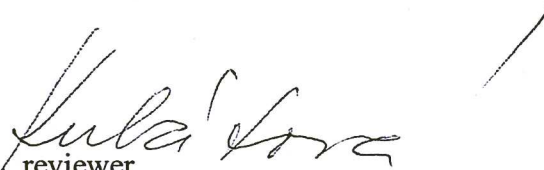
- What is the correlation between computed results (e.g. failure rate, repair rate, reliability flow) and the real values? Have you any idea how to compare it? Do you plan to use simulation or emulation methods?
- Are there any examples which can compare area overhead of the proposed methods?
- What is the real hardware redundancy for AN codes, linear codes, etc. including the control parts?
- Do you think that the proposed method should be usable also for cycles, jumps, etc. and how?
- How the propose method can be used for parallel processing (today trends are multi-core, many-core or heterogeneous architectures on a chip) with respect to the communication within a chip?

Finally, despite of some remarks and questions (and after their satisfactory explanations) I have to declare that PhD thesis **Model-based Reliability Evaluation of Data Processing in HW-Fault-Tolerant Processor Systems** by Peter Raab yields many new ideas and results in a very actual field of system reliability evaluations.

Therefore I can declare that he fulfils all requirements for PhD theses and agrees with the established conditions for graduation by the title PhD. I recommend this thesis for the defence.

Prague, 25. 11. 2013

doc. Ing. Hana Kubátová, CSc., reviewer



Fakulta informačních technologií
ČVUT v Praze

Review of the Doctoral Thesis

“Model-based Reliability Evaluation of Data Processing in HW-Fault-Tolerant Processor Systems”

by M. Eng. Dipl.-Ing. (FH) Peter Raab

Univ.-Prof. Dr.-Ing. Frank Schiller
Scientific Safety & Security
Ostendstr. 196
D-90482 Nuremberg, Germany
Phone: +49 911 54056-244
Fax: +49 911 54056-29
f.schiller@beckhoff.de

21 November 2013

Because of the increase of complexity in technical systems of all kinds and their application in various – even critical fields – their reliability becomes more and more important. Their efficiency in the overall life cycle (development, manufacturing, operation, costs of damages etc.) has always to be considered; and their behavior is nowadays mainly determined by software. Therefore, it is very important to research for software based or at least software supported approaches to reliability.

Starting Point and Goal of the Thesis

Measures to reliability range from approaches to simply try to avoid faults (perfect systems approach) up to their toleration (fault-tolerance approach). Tolerating faults in the field of data processing involves any kind of error detection

- by either voting, i.e. the value delivered by the majority of several functionally equivalent channels is considered as the correct one (e.g. 2-out-of-3), or
- by explicit detection mechanisms
 - in order to enable a decision in case of an even number of functionally equivalent channels (e.g. 1-out-of-2),
 - to correct the errors in the detected incorrect values, if possible, or
 - just to ignore the detected incorrect values and wait for correct ones, if the application would allow this.

In his thesis, Mr Raab investigates redundant structures of several functionally equivalent channels where each channel is additionally equipped with error detection measures. These error detection measures are based on arithmetic codes.

Mr Raab's approach does not necessarily refer to safety applications although he analyses and extends algorithms for error detection in a sophisticated way that are also applied in the safety area.

Structure and Content of the Thesis

This thesis is a cumulated one. Therefore, the main, comprehensive part is relatively short, and there are seven international publications put into the Appendix. These publications consist of five conference and two journal papers.

Title

I strongly recommend using the term Hardware-Fault-Tolerant Processor instead of the abbreviation "HW" there.

Abstract

The reference to dependability of safety-critical applications is correct but misleading a little. According to the title, the contribution of the thesis is mainly a contribution to reliable systems. Of course, safety-critical applications have to be reliable but there the term reliability includes the normal operating as well as the safe but possibly non-productive state. Therefore, other kinds of solutions to safety are possible that definitely do not belong to the focus of the thesis.

In general, definitions of important terms would be very helpful (reliability, availability, dependability, safety, fault, error, failure, malfunction, disturbance, mistake ...) since they are used differently in various areas and daily life; and the reader of the thesis is often confronted with a bunch of such terms, too.

Chapter 1 – Introduction

Again, the reference to safety might be misleading. The thesis is motivated here very clearly: a software approach has to be developed in order to increase the reliability of the underlying regular, non-specific hardware. Corresponding error models will be defined. As basis serves the coded processing approach (= arithmetic coding). In the following, random faults (that result in soft errors) will be dealt with only.

Chapter 2 – State of the Art

In the first section "Software-Implemented Hardware Fault Tolerance", software solutions are introduced that are capable to detect internal random errors and to make use of additional hardware and software resources of the hardware. For the sake of understandability, I would have appreciated an explicit distinction between the two ways of exploiting redundancy:

- to detect errors by comparison (or more general, consistency checks),
- to be capable to continue the operation in case of an error in one channel.

In this way, it would have been easier to explain solutions by means of codes (as a possibility of data redundancy) for error detection and correction for the originally stated task of increasing reliability (cf. Subsection 2.1.3). The same holds for Section 2.2. Besides this comment, the approaches of the literature are correctly explained there. Mr Raab introduces fault injection as an important mean to proof the efficiency of reliability approaches (hardware- and software-based).

Chapter 3 – Goals of the Thesis

Mr Raab defines four objectives:

1. Development of an error model
2. Comparison of different codes w.r.t. residual error probability
3. Reliability evaluation w.r.t. data flow
4. Validation of correctness of the error models

These four objectives describe the contributions of the thesis.

Chapter 4 – Error Models of Reliability Evaluation of Data Processing Units

This chapter constitutes the main part of the thesis. It refers to the publications in the Appendix. Fig. 4.1 shows how they are logically connected.

Section 4.1 – Arithmetic processors

Here, the discussion about error models is motivated; and the validity of the model of the Binary Symmetric Channel in the field of arithmetic processors is convincingly questioned. This section refers to the publication in A.2.

Section 4.2 Error models

The validation of codes for error detection needs to involve calculations of residual error probabilities. These calculations require error models. A discrete Markov model is proposed.

Subsection 4.2.1 Arithmetic Operation

A Markov model is introduced and discussed. This subsection refers to the publication in A.5.

Subsection 4.2.2 Fault Compensation

As a side effect, some errors compensate each other in a chain of independent components. In my opinion, the main contribution of this paper is to show the limits of the models instead of describing real useful effects - since the independence does not hold or is at least difficult to be proved. This subsection refers to the publication in A.6 and partly A.7.

Subsection 4.2.3 Data Flow Analysis

Several probability distributions and corresponding models are discussed in order to try to describe the time behavior a more realistic way. This subsection refers to the publication in A.3.

Section 4.3 Alternative Codes for Coded Data Processing

Mr Raab tries to make use of the advantages of linear codes applied in communication. He motivates a later transformation. Unfortunately, he does not take into account that the values of residual error probabilities of arithmetic codes always require an assumption about the probability distribution of net data. This section refers to the publication in A.7.

Section 4.4 Code Transformation

The transformation motivated above is described here more in detail. This transformation is correct but does not have a positive effect on error detectability. This section refers to the publication in A.4.

Section 4.5 Validation

Subsection 4.5.1 Concurrent Task Processing by an Operating System

A possible way to apply the introduced arithmetic codes is described. There, a task framework is introduced that fits to existing software architectures in the automotive industry. This subsection refers to the publication in A.1.

Subsection 4.5.2 Simulation Approach

A random fault distribution is taken in a simulation in order to validate the error models and corresponding detection methods. This subsection refers to the publication in A.5.

Chapter 5 – Conclusion

The objectives are now discussed related to the results of the thesis. Mr Raab states to have sufficiently discussed all issues. In contrast, he formulates five topics of further work that relativize this statement:

- Program flow
By explicitly referring to branch instructions, he makes obvious implicitly that the assumptions of independence he made are not realistic.
- Further alternative codes
Of course, additional codes are to be analyzed. But he does not mention any valuable additional criterion. His statement “This probably means the increase of fault tolerance by further hardware redundancy.” is not understandable. Additional hardware components that might be necessary (like DSP) are not necessarily redundant ones.
- Case study
Additional studies are definitely required (and they might refute some results of the thesis).
- Comparison between linear and arithmetic codes
He honestly recognized a lack of substance in his thesis. Some proofs are missing.
- Effective reliability caused by fault compensation
He would like to involve repair, but he still does not question the practicability of the compensation at all.

Cumulated Articles

A.1 Safe Software Processing by Concurrent Execution in a Real-time Operating System (International Conference on Applied Electronics, 2011)

The operations are executed within a task framework. Each operation is executed in form of two heterogeneously redundant tasks (“Leading” and “Trailing” Instance). The data and the operations are coded by different arithmetic codes. Therefore, the so called comparison in Section III, C, stands probably for a kind of consistency check of the coded data. Many practical issues such as synchronization have been solved. As

Beckhoff Automation GmbH
Eiserstr. 5
33415 Verl
Germany

Postfach 11 42
33398 Verl

Phone: +49 (0) 5246/963 -0
Fax: Reception: -149
Sales: -198
Service: -479
E-Mail: info@beckhoff.com
www.beckhoff.com

General manager:
Dipl. Phys. Hans Beckhoff
Arnold Beckhoff
Register court: Gütersloh HRB 1803
Ust.-Id.-Nr.: DE 126787444
Finanzamt Wiedenbrück
St.-Nr. 347/5819/0016

Kreissparkasse Verl
BLZ 478 535 20
Kto.Nr. 4 000 766
SWIFT WELADED
BL/47853520
IBAN DE114785352
00004000766

Deutsche Bank Gütersloh
BLZ 480 700 43
Kto.Nr. 371/7014
SWIFT DEUTDE33B480

IBAN DE854807004
00371701400

the authors mention the approach should be interpreted as a proof of concept. The potential use of multicore processors is convincingly discussed. There, the reliability could be increased and the safety could be preserved.

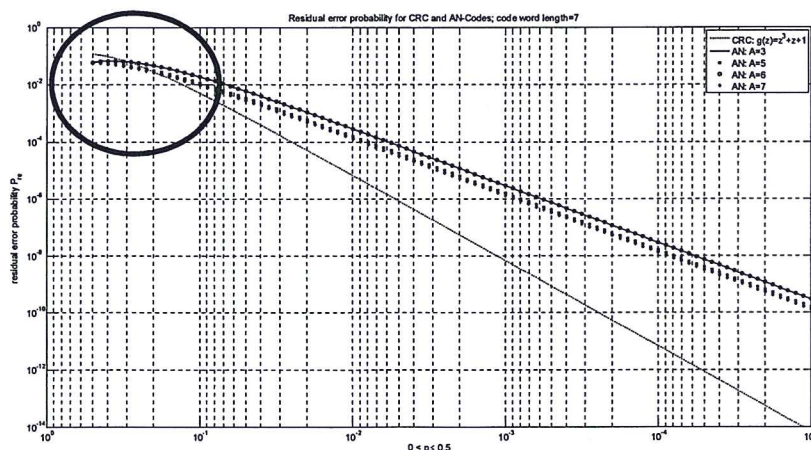
A.2 Cyclic Codes and Error Detection during Data Processing in Embedded Software Systems (4th Embedded Software Engineering Congress, 2011)

Possible transformations between cyclic linear codes and arithmetic codes are defined. It is asserted that the use of cyclic linear codes can lead to a lower residual error probability and can enable error correction. An important distinction between two cases is made: codes for data memory and communication versus codes for arithmetic operations. In my opinion, the considered transformation is interesting but not at all applicable, since different checksums and different checks are to be applied referring to different error models. Therefore, a meaningful transformation of code words (data and checksum) of one code to the other does not exist.

In the example of Fig. 4, the length of code words is not mentioned. It can only be calculated by means of the given code rate. The residual error probability of the CRC holds only for code word lengths ≤ 7 . For longer code words, the Hamming Distance of the applied CRC is 2. The comparison between CRC and arithmetic codes cannot be generalized since there are arithmetic codes with Hamming Distances far beyond 2. The statement "Note that using a generator polynomial which is not primitive, the generated cyclic code has a minimum hamming distance of 2 only." is not true.

The code rate allows calculating the number of information bits. For $A=5$, $A=6$, $A=7$, 4 information bits are applied. For $A=3$, the given code rate 0.57 cannot be correct. There, 2 additional (redundant) bits are sufficient. I assume the number of information bits is also 4, and the code rate should therefore be 0.67.

The residual error probability of arithmetic codes applying the Binary Symmetric Channel as error model depends on the probability distribution of the net data since the arithmetic codes is a non-linear one concerning bitwise operations. Obviously, Mr Raab assumed – but never formulated explicitly – a uniform distribution of the net data in Fig. 4. The correct calculation is depicted above. There are some minor differences for bit error probabilities lower than 0.1.



Beckhoff Automation GmbH
Eiserstr. 5
33415 Verl
Germany

Postfach 11 42
33398 Verl

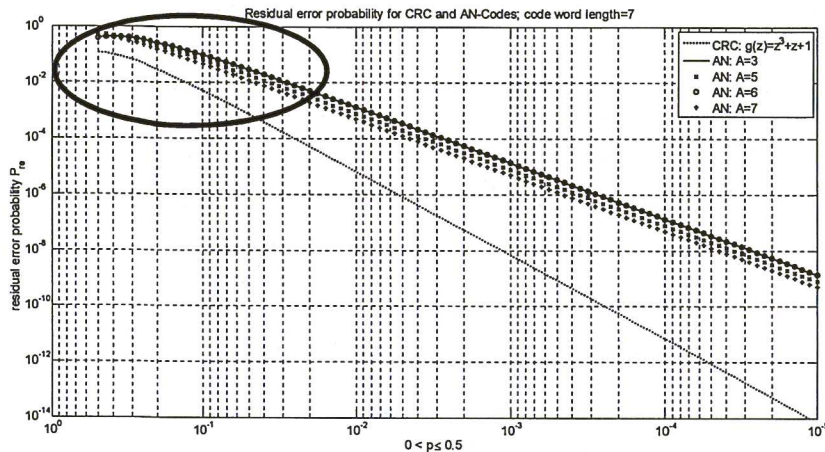
Phone: +49 (0) 5246/963 -0
Fax: Reception: -149
Sales: -198
Service: -479
E-Mail: info@beckhoff.com
www.beckhoff.com

General manager:
Dipl. Phys. Hans Beckhoff
Arnold Beckhoff
Register court: Gütersloh HRB 1803
Ust.-Id.-Nr.: DE 126787444
Finanzamt Wiedenbrück
St.-Nr. 347/5819/0016

Kreissparkasse Verl
BLZ 478 535 20
Kto.Nr. 4 000 766
SWIFT WELADED
BL47853520
IBAN DE114785352
00004000766

Deutsche Bank Gütersloh
BLZ 480 700 43
Kto.Nr. 371/7014
SWIFT DEUTDE3B480
IBAN DE854807004
00371701400

Another assumption would be the worst case assumption: For each error bit pattern, exactly one of those net data occurs (probability of 1) that would cause an undetectable error.



This figure is not identical to Fig. 4 in the paper neither.

A.3 Reliability of Task Execution during Safe Software Processing (15th Euromicro Conference on Digital System Design, 2012)

The terms reliability, safety and fault-tolerance are not properly used. A lack of the required diligence is missing. For instance, a maximum of $3 \cdot 10^9$ dangerous failures per hour is demanded ($3 \cdot 10^{-9}$ would be correct). Regardless of this, the n-staged-Markov model of a task is introduced. Unfortunately, the symbol "n" in the term "n- μ dt" is never explained. I do not see a relation to the number of steps (cf. e.g. the names of the states) that are abbreviate by "n", too.

According to general rules, many states of the Markov model could be merged without any loss of information. I do not understand why this has not been done.

A.4 Isomorphism between Linear Codes and Arithmetic Codes (Computing and Informatics, 2013)

In the paper, a transformation is proposed from linear codes applied in communication to arithmetic codes applied in data processing. It is stated that this transformation would combine the advantages of both types of codes for error detection and correction.

The residual error probability of linear block codes and of arithmetic codes cannot be compared as it is done in reference [11] (paper A.2) since the detectability of errors according to the Binary Symmetric Channel by means of arithmetic codes depends on the probability distribution of net data.

Separable codes can only be evaluated with modulo operation of the overall coded date. It is never mentioned here but the remarks in Section 2.3 leave the impression that Mr Raab wants to compare the information and the remainder somehow. Otherwise the discussion about the carry bit of the remainders would be obsolete immediately (just take the modulo remainder of the sum of the two remainders).

Beckhoff Automation GmbH
Eiserstr. 5
33415 Verl
Germany

Postfach 11 42
33398 Verl

Phone: +49 (0) 5246/963 -0
Fax: Reception: -149
Sales: -198
Service: -479
E-Mail: info@beckhoff.com
www.beckhoff.com

General manager:
Dipl. Phys. Hans Beckhoff
Arnold Beckhoff
Register court: Gütersloh HRB 1803
Ust.-Id.-Nr.: DE 126787444
Finanzamt Wiedenbrück
St.-Nr. 347/5819/0016

Kreissparkasse Verl
BLZ 478 535 20
Kto.Nr. 4 000 766
SWIFT WELADED
BL47853520
IBAN DE114785352
00004000766

Deutsche Bank Gütersloh
BLZ 480 700 43
Kto.Nr. 3717014
SWIFT DEUTDE33B480

IBAN DE854807004
00371701400

In the conclusion, it is more or less figured out that the original statement of improvement is not true. The transformation requires specific linear and arithmetic codes that are not at all the best ones. Even if the result would have been more encouraging: the assumed error models and the detection algorithms have to match. The proposed transformation does not make sense without discussing the basic error models.

A.5 Error Model and the Reliability of Arithmetic Operations (IEEE EUROCON - International Conference on Computer as a Tool, 2013)

The goal of the paper is the combination of previously introduced Markov models in order to detect errors of data that are decoded by means of an arithmetic code. The single Markov models are connected via the corresponding carry bit. Therefore, the probability distributions of the state variables of the single Markov models are not independent at all, and the determination of probabilities of paths according to eqn. (22) is not correct.

Therefore, instead of the calculations demonstrated in the paper, another comprehensive Markov model has to be established. Its state variables result out of the cross product of the state variables of the single models.

A.6 Data Flow Analysis of Software Executed by Unreliable Hardware (16th Euromicro Conference on Digital System Design, 2013)

The paper is similar to the paper A.5 but more emphasis is put on the data flow. Additionally, the effect of error compensation is discussed. Here, this effect occurs since the same error probability is assumed for each cell, and two errors compensate each other in the binary space. Obviously, the higher the error probability the higher is the probability of compensation. It seems to be interesting to analyze this effect and to determine optimum points theoretically, but I doubt any practical relevance.

A.7 Reliability of Data Processing and Fault Compensation in Unreliable Arithmetic Processors (Microprocessors and Microsystems, 2013)

This paper summarizes discussions and results of the previous ones.

Results of the Thesis

The results of the thesis are

- a valuable literature research,
- the formulation of some problems of coding for error detection,
- the evaluation of various approaches,
- to have supplied a valuable basis for further discussions, and
- a clear formulation of further work.

Beckhoff Automation GmbH

Eiserstr. 5
33415 Verl
Germany

Postfach 11 42
33398 Verl

Phone: +49 (0) 5246/963 -0
Fax: Reception: -149
Sales: -198
Service: -479

E-Mail: info@beckhoff.com
www.beckhoff.com

General manager:
Dipl. Phys. Hans Beckhoff
Arnold Beckhoff
Register court: Gütersloh HRB 1803
Ust.-Id.-Nr.: DE 126787444
Finanzamt Wiedenbrück
St.-Nr. 347/5819/0016

Kreissparkasse Verl
BLZ 478 535 20
Kto.Nr. 4 000 766
SWIFT WELADED
BL47853520
IBAN DE114785352
00004000766

Deutsche Bank Gütersloh
BLZ 480 700 43
Kto.Nr. 371/7014
SWIFT DEUTDE33B480

IBAN DE854807004
00371701400

Summarized Evaluation of the Thesis

The thesis by Mr Raab constitutes an original contribution to the area of coding for error detection.

The analyses have been developed and demonstrated systematically. Form and language of the thesis are appropriate. The appropriate literature has been considered.

Mr Raab shows an impressive record of seven contributions in international journals and conference proceedings. I am convinced that the result of the thesis would have been much better if he would have processed a complete thesis based on his papers instead of having prepared a cumulated one where he is forced to stick at former ideas despite new insights.

I recommend the thesis for defense.



(Prof. Dr. Frank Schiller)

Beckhoff Automation GmbH
Eiserstr. 5
33415 Verl
Germany

Postfach 11 42
33398 Verl

Phone: +49 (0) 5246/963 -0
Fax: Reception: -149
Sales: -198
Service: -479
E-Mail: info@beckhoff.com
www.beckhoff.com

General manager:
Dipl. Phys. Hans Beckhoff
Arnold Beckhoff
Register court: Gütersloh HRB 1803
Ust.-Id.-Nr.: DE 126787444
Finanzamt Wiedenbrück
St.-Nr. 347/5819/0016

Kreissparkasse Verl
BLZ 478 535 20
Kto.Nr. 4 000 766
SWIFT WELADED
BLJ47853520
IBAN DE114785352
00004000766

Deutsche Bank Gütersloh
BLZ 480 700 43
Kto.Nr. 3717014
SWIFT DEUTDE3B480

IBAN DE854807004
00371701400