BECKHOFF

Review of
Doctoral Thesis by M. Eng. Stefan Krämer:
Development and Simulation of Fault-tolerant Multicore Real-time Scheduling Covering Transient Faults

Univ.-Prof. Dr.-Ing. Frank Schiller
Beckhoff Automation GmbH & Co. KG
Scientific Safety & Security
Ostendstr. 196
D-90482 Nuremberg, Germany

F.Schiller@beckhoff.com
Phone: +49 911 54056-244

22 March 2016

Because of the increasing 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 that utilizes the hardware capabilities at its best.

On the hardware side, the reliability is supported by redundant structures. There, faults can be tolerated since parts of the redundant system, or channel, respectively, are still capable to deliver the correct values. Multicore processors which had been originally developed to distribute the load among the cores (load balancing) can be applied to enable fault-tolerance solutions.

On the software side, its tasks have to be executed such that faults can be detected and/or managed properly. Of course, the hardware properties are to be exploited. For instance, redundant tasks are distributed to different cores and are implemented in a diverse way additionally (heterogeneous redundancy).

In order to achieve fault-tolerance, the software tasks have to be scheduled. The different goals of such schedulers in general are:

- avoidance of faults, and
- minimization of their effects.

In his thesis, Mr Krämer puts the main emphasis on timing faults. Whenever necessary he discusses data integrity as well and refers to corresponding papers he co-authored.

Structure and Content of the Thesis

This thesis is a cumulated one. Nevertheless, the main, comprehensive part is still a self-standing thesis referring to seven international publications that have been put into the Appendix. These publications consist of six conference papers and one journal paper.

Chapter 1 – Introduction

Mr Krämer give a very good overview about what is needed to understand the following chapters. He met the challenge to give an introduction to faults / fault handling / fault tolerance, embedded systems, as well as multicore systems.

The subsection "1.2.3 Fault Tolerance" refers to "dangerous system failure" only. But fault tolerance is not necessarily related to danger.

There, some references are not available ("see Chapter 0").

In subsection 1.2.4, the explanation of Fail-silent should include that the silent behavior of the component is safe w.r.t. the overall system.

Chapter 2 – State of the Art

First, Mr Krämer describes current approaches to multicore scheduling. They are precisely explained such that he can refer to them later. Additionally, this section gives a really valuable and efficient overview others will appreciate.

In Subsection 1.2.2.3 it might be very helpful to emphasize that the deadline is task specific. This fact influences the overall strategy tremendously.

The second section "Safety related, Fault-tolerant Scheduling" deals with fault-tolerant scheduling only. Without doubt, fault-tolerance might contribute to safety, but there are other safety approaches where the safety is guaranteed by fault detection and corresponding safe reaction without any fault tolerance! Logically, the safety issue is not treated at all in the text of the section. I propose to delete the safety reference in the chapter title.

In the third section, the scheduling in multicore systems is treated. Important related work is introduced. Some related coding techniques are treated. Unfortunately, some terms are not used properly, e.g. the result of coding is a *code word* but not a *coded word*.

Chapter 3 – Objectives of the Thesis

Mr Krämer defines four objectives:

1. Specification of architecture
2. Specification of error models
3. Development of scheduling algorithm
4. Validation

These four objectives describe the contributions of the thesis.

Chapter 4 – Fault-Tolerant Multicore Real-Time Scheduling

This chapter constitutes the main part of the thesis. It refers to the publications in the Appendix. Fig. 13 shows how they are logically connected.

Section 4.1 – System Architecture

Refers to: *P.5 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 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.

Section 4.2 – Error Models and Fault Compensation

Refers to: *P.4 Reliability of Data Processing and Fault Compensation in Unreliable Arithmetic Processors (Microprocessors and Microsystems, 2015)*

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.

Additional reference to: *P.3 Data Flow Analysis of Software Executed by Unreliable Hardware (16th Euromicro Conference on Digital System Design, 2013)*

The paper puts emphasis 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.

Section 4.3 – Fault-Tolerant Multicore Scheduling

Subsection 4.3.1 – PFair Scheduling

Refers to: *P.1 Proportionate Fair based Multicore Scheduling for Fault Tolerant Multicore Real-Time Systems (Int. Conference on Electrical and Information Technologies, 2015)*

Here the Pfair algorithm is enhanced for its application for fault-tolerance. The main interesting point is the coupling with error detection (Fig. 3). The evaluation is done by means of simulation – even in combination with non-safety-related tasks (Fig. 16 in the thesis).

The important category ASIL (Automotive Safety Integrity Level) is not defined correctly at all, even the measuring unit (h^{-1}) is missing.

Subsection 4.3.2 – Safe Execution, Markov Analysis

Refers to: *P.2 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 "$n \cdot \mu\, dt$" 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.

Section 4.4 – Validation of Scheduling and Error Models

Subsection 4.4.1 – Markov Model and Discrete Event Simulation

Refers to: *P.6 Comparison of Enhanced Markov Models and Discrete Event Simulation – for evaluation of probabilistic Faults in safety-critical real-time task sets (17th Euromicro Conference on Digital System Design, 2014)*

The most important result is that both approaches deliver similar results.

The Markov model is represented by a set of differential equations that are solved numerically, i.e. by means of a specific simulation. The discrete event model is analyzed by typical discrete event simulation. The sentence "Dependant or probability based program flow branches can be modelled as well as operating system functionality for synchronization of task instances." is not clear.

Subsection 4.4.2 – Reliability Analysis by Stochastic Simulation

Refers to: *P.7 Reliability Analysis of Real-time Scheduling by Means of Stochastic Simulation (17th Conference on Applied Electronics, 2012)*

Faults are injected. Fault-tolerance is interpreted as repair here. The approach is promising although time-constraints are not met.

Chapter 5 – Conclusion

The objectives are now discussed related to the results of the thesis. Mr Krämer explains that he has sufficiently discussed all issues.

Unfortunately, only here it becomes visible that his main contribution is not to increase safety but to enable safety approaches by integrating them to powerful hardware and to ensure necessary fault-tolerance.

Additionally, he formulates some topics of further work:

- Analyzing of scheduling overhead
- Analysis of effects of the hardware architecture
- Case study
  Additional studies are definitely required (and they might refute some results of the thesis).
- Integration and implementation

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.

Summarized Evaluation of the Thesis

The thesis by Mr Krämer constitutes an original contribution to the area of task scheduling on multicore systems for fault-tolerance.

Some references to chapters, sections etc. within the thesis are not available. The language contains elements of British and American English. Some typing errors might cause understandability.

BECKHOFF

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

Mr Krämer shows an impressive record of seven contributions in international journals and conference proceedings.

I recommend the thesis for defense.

Frank Schiller

(Prof. Dr. Frank Schiller)

Beckhoff Automation
GmbH & Co. KG
Huelshorstweg 20
33415 Verl, Germany

PO Box 11 42
33398 Verl, Germany

Phone: +49 5246 963-0
Sales: +49 5246 963-1000
Service: +49 5246 963-460
Support: +49 5246 963-157

Fax Reception: -149
Fax Sales: -198

www.beckhoff.com
info@beckhoff.com
sales@beckhoff.com
service@beckhoff.com
support@beckhoff.com
international-sales@beckhoff.com
engineering@beckhoff.com

General Manager:
Dipl.-Phys. Hans Beckhoff

Register court:
Gütersloh HRA 7075

VAT ID number: DE 815529334

Kreissparkasse Wiedenbrück
BIC: WELADED1WDB
IBAN: DE24 4785 3520 0000 0600 04 (EUR)
IBAN: DE02 4785 3520 0000 0600 12 (USD)
Deutsche Bank (EUR, USD)
BIC: DEUTDE3B489
IBAN: DE95 4807 0043 0373 6014 00

PhD Thesis Review

PhD student: **Dipl.-Ing. (FH) Stefan Krämer, M.Eng.**

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

Title: **Development and Simulation of Fault-Tolerant Multicore Real-Time Scheduling Covering Transient Faults (Návrh a simulace FT plánovacího algoritmu pro vícejádrový processor a RT aplikace)**

Submitted theses contain 5 chapters, follows by 7 author's publications (P1 - P7) which make the basis of the thesis. Main objectives and contributions are summarized in Chapter 3. Each paper P1 - P7 is introduced by the brief summary and discussion. Chapter 5 concludes the thesis and depicts possible improvements and future work.

1. Recency and topicality of the theses' theme with respect to the today state of the art in the presented field

The area of this Theses is very actual, especially in today massively exploitations of embedded systems in mission critical areas, as e.g. automotive domain or other mission-critical systems. These areas are characterized by more and more complicated functions which are evolved by the Moore's law and ever increasing integration density. The using of multicore or manycore processors or other types of System-on-a chip is a today challenge for designers. The prediction of the reliability properties in the early stages of development of not only software system is crucial point in the recent research, especially due to failure-rate increasing. The Theses try to make a holistic view on these systems which connect many areas of (not only) digital systems research: real-time applications, several types of scheduling mechanisms based on types of tasks, evaluations of all types of dependability issues (reliability, availability, security, safety, survivability), area overhead, performance and different types of faults based on the final implementation areas.

2. Originality and contributions of theses

This main goal can be subdivided to the following objectives:

1. Specification of suitable software and operating system architecture to integrate fault-tolerance mechanisms in a real-time operating system.
2. Specification of error models for reliability evaluation of task execution.
3. Development of a fault-tolerant robust multicore scheduling algorithm.
4. Validation based on a discrete-event simulation methodology for evaluating the developed scheduling.

The main contribution of this work is a multicore real-time scheduling algorithm (LB-*Pfair*) that can guarantee an optimal schedule during fault free operation and maximize the adherence of timing constraints during the occurrence of transient faults. The other three objectives were necessary to perform evaluations of the presented methods and they make inherent (and very time-spending) part of Theses.

3. Publications of results and science erudition

The list of publications is excellent as concern both the quantity and quality. All crucial parts were published in journals and conference proceedings. I appreciate especially very self-explaining presentations of mutual content and time relations between the core publications P1 - P7 (see Figure 13) which make a Theses core.

4. Formal level of the theses

The Theses as concern the structure and organization of chapters are adequate. There are several formal mistakes (e.g. references to Chapter 0 - pages 8, 32, 48, or missing letters).

5. Questions for the defence:

- Please describe more precisely relations between figures 12, 15 and 18, especially with respect to the statement on page 48 about using DMR and TMR concepts (here is the bad reference to Chapter 0). What are the differences or advantages with using duplex or triplex implementation? Is this implementation hardware, software or both ones?
- Is it possible to shift some parts to hardware and when it is better as concern dependability issues?
- The Theses are restricted only to non-systematic, random, soft types of faults, why? Is it possible to use proposed solutions e.g. for stuck-at faults in hardware?
- The usability of different scheduling algorithms is mostly based on task types (frequency, period, laxity, probabilistic properties of sporadic tasks). Are there any quantitative limits of proposed solutions (e.g. at what application areas is possible to use it and for what task properties)?

Finally, despite of some remarks (and after their satisfactory explanations) I have to declare that PhD theses **Development and Simulation of Fault-Tolerant Multicore Real-Time Scheduling Covering Transient Faults** by **Stefan Krämer** propose new methods and their evaluations. They are original ones and provide new holistic insight on the recent digital design methods in the proposed area.
Therefore I can declare that **Stefan Krämer** fulfils all requirements for PhD theses and defence and he agrees with the established conditions for graduation by the title PhD.

I recommend this thesis for the defence.

Prague, 28. 4. 2016

doc. Ing. Hana Kubátová, CSc., reviewer
Fakulta informačních technologií, ČVUT v Praze