

DEPENDABILITY-AWARE EMBEDDED SYSTEM-LEVEL DESIGN

Michael Glaß and Jürgen Teich (supervisor)

Department of Computer Science 12, University of Erlangen-Nuremberg
Am Weichselgarten 3, D-91058 Erlangen, Germany
{glass,teich}@cs.fau.de

ABSTRACT

More and more embedded systems operate in safety-critical areas and have to cope with destructive agents present at their mounting spaces. As a result, dependability has become an objective of major importance. In this work, an automatic cost-aware embedded system-level design methodology is presented that contributes a) effective dependability analysis techniques, b) the usage of dependability-increasing methods, and c) the integration of the investigated techniques in a state-of-the-art design space exploration approach. Using a model-based design paradigm, the work at hand is applicable to several embedded domains like, e.g., SoC, MPSoC, networked embedded system, and ECU network design.

1. INTRODUCTION

Embedded systems typically consist of many interconnected processing units, e.g., homogeneous or heterogeneous *MPSoCs*, automotive and avionics *ECU* networks, etc. These systems work in safety-critical areas where high demands for *dependability*, i.e., *reliability* and *safety*, have to be fulfilled. Additionally, there is a trend towards an integration of embedded systems near sensors and actuators to decrease wiring cost and make use of currently unused mounting spaces. As a consequence, these systems have to cope with more and more destructive agents. Another challenge is the increasing complexity of embedded systems that have to carry out several applications in parallel. Embedded system-level design aims to optimize the system implementation with respect to several objectives like monetary costs or performance, while stringent constraints like maximum loads on processing and communication resources, or the maximum usage of space are respected.

2. CONTRIBUTIONS

The work at hand presents a design methodology at system-level with the goal of a cost-aware dependability increase for embedded systems. The methodology rests upon a model-based design paradigm: The system *specification* is given in a graph-based manner, i.e., the *application*, the available *architecture*, and a mapping relation between these two are represented as graphs with nodes modeling tasks and resources, edges modeling data dependencies and communication possibilities, respectively. This work contributes effective dependability analysis techniques, the automatic utilization of dependability-increasing techniques, and the integration of the developed methods in a state-of-the-art design space exploration approach.

Dependability Analysis. Previous approaches introducing analytical automatic dependability analyses for embedded system design assume a *series-parallel* system structure. This cannot be assumed in case of resource sharing and more complex system structures as induced by many dependability-increasing methods. To solve this problem, this work presents effective symbolic analysis techniques: Based on developed construction rules, Boolean functions are used to represent the *structure function* φ . The structure function is the most general model of a system that allows to determine whether a system is working

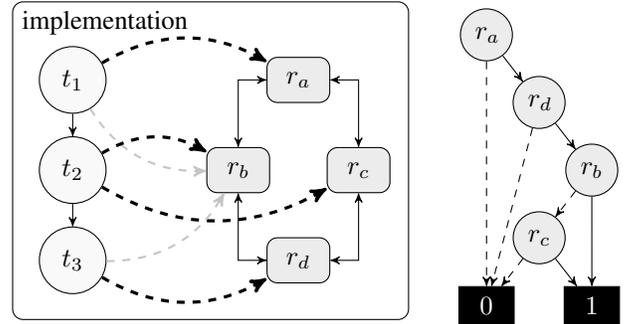


Fig. 1. An implementation with a multiple binding of task t_2 and the BDD encoding the structure function of the implementation in case a defect of resources is considered only.

properly or failed, respectively, in a given state. The developed approach efficiently encodes φ as Binary Decision Diagrams (BDDs) and makes use of their capability of a compact representation of Boolean functions. Due to the special graph-based structure of the BDDs, a methodology based on a special decomposition scheme is proposed to efficiently derive desired dependability-related measures. The unique characteristic of this approach allows the usage of arbitrary reliability functions and, thus, enables to model complex system behaviors like, e.g., *aging* and *wear*. The complete analysis flow is presented in detail in [6, 5]. The proposed analysis technique is not only applicable for different types of *redundancy*, but has also been extended to model the usage of *majority voters* [18]. An extension of the analysis approach covers the effect of *graceful degradation* scenarios on the dependability, cf. [1]. Graceful degradation describes the shutdown of low-priority applications in favor of essential applications in case of defects. Another enhancement of this approach allows to determine upper bounds for online algorithms that exhibit self-x properties from the organic computing area [4]. The developed analysis techniques have been publicly released as the JRELIABILITY library [2].

Dependability-Increasing Techniques. A novel concept developed in this work is called *multiple binding* [5], as illustrated in Fig 1. While former approaches bind each task of the application exactly once, this approach features the possibility to activate several mapping edges. Although simple at first glance, multiple binding enables to exploit several dependability-increasing techniques in the synthesis process. On the other hand, it requires sophisticated analysis techniques and design space exploration approaches to cover the considerably larger search space.

Multiple binding allows the usage of arbitrary redundancy strategies like hot and cold spares or functional redundancy, cf. [6]. Due to resource sharing, idle capacities are used to place other task instance on a resource in a cost-aware way. By using hierarchical models, introducing redundancy on different levels of abstraction is enabled. Note that multiple binding avoids costly multiplications of complete resources or subsystems including their tasks. Moreover, the deterministic system behavior enabled by the static binding of redundant task instances that can

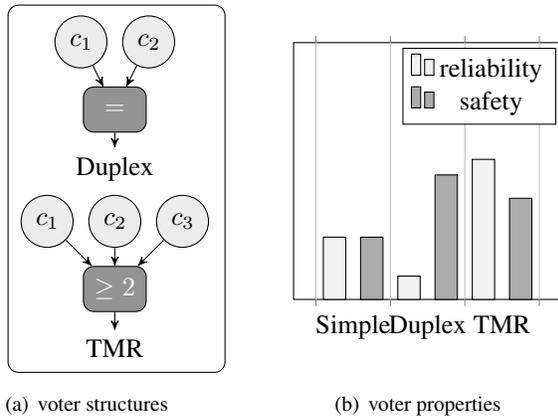


Fig. 2. Voting strategies and their characteristics, showing the need to optimize both, reliability and safety, to solve the problem of conflicting properties.

be activated at runtime is in compliance with the high safety-demands in the automotive area. Currently, other state-of-the-art techniques like dynamic task migration [20] do not meet these demands. This work also investigates the placement of arbitrary majority voting structures like, e.g., 2-out-of-2 voters called *duplex* or 2-out-of-3 voters, commonly known as *Triple Modular Redundancies* (TMRs). The developed voter placement covers both, a voting of data in software as well as the implicit binding of the voting procedure to qualified resources. Due to the special characteristics of different voting structures as illustrated in Fig. 2, the usage of either reliability or safety as the only objective is not sufficient: While the duplex voter would be avoided due to its decreased reliability compared to the single resource, the TMR would be neglected because of a decreased safety compared to the duplex voter, respectively. The usage of both objectives as proposed in [18] resolves this problem effectively.

Design Space Exploration. The developed techniques are integrated in a state-of-the-art design space exploration approach [12, 15, 17] that relies on a hybrid use of a symbolic problem representation to gather feasible implementations while a meta-heuristic optimization is used to cover the search space. This requires an automatic integration of dependability-increasing methods as 0-1 Integer Linear Programs (ILPs). General construction rules to formalize the multiple binding and the placement of arbitrary voting structures as 0-1 ILPs are developed and have been presented in [3, 18]. The integration of the dependability-increasing techniques directly in the design space exploration in compliance with the developed analysis techniques makes the proposed approach transparent for the designer. The effectiveness of the developed techniques is studied on testcases from the MPSoC [18], networked embedded system [19], and ECU network [3] design area.

3. BIBLIOGRAPHY AND FURTHER INFORMATION

Michael Glaß received the diploma degree in Computer Science from the University of Erlangen-Nuremberg, Germany, in 2006. He is currently a Ph.D. degree candidate in the Department of Computer Science at the University of Erlangen-Nuremberg, Germany and supported by the German Science Foundation SFB 694. Michael Glaß serves as a reviewer for renowned international conferences and journals. His research interest includes Reliability Engineering of Embedded Systems and Multi-Objective Meta-Heuristic Optimization techniques. The estimated gradu-

ation date is the end of this year. The work at hand has neither been presented at DAC PhD-Forum, DATE PhD-Forum or ASP-DAC PhD-Forum. The following papers have been authored or co-authored but are not referenced in the previous PhD-abstract: [8, 7, 9, 10, 11, 13, 14, 16]

4. REFERENCES

- [1] M. Glaß, M. Lukasiewicz, C. Haubelt, and J. Teich. Incorporating Graceful Degradation into Embedded System Design. In *To appear in Proc. of DATE '09*, 2009.
- [2] M. Glaß, M. Lukasiewicz, and F. Reimann. Jreliability - the java-based reliability library. <http://www.jreliability.org/>.
- [3] M. Glaß, M. Lukasiewicz, F. Reimann, C. Haubelt, and J. Teich. Symbolic Reliability Analysis and Optimization of ECU Networks. In *Proc. of DATE '08*, pages 158–163, 2008.
- [4] M. Glaß, M. Lukasiewicz, F. Reimann, C. Haubelt, and J. Teich. Symbolic Reliability Analysis of Self-healing Networked Embedded Systems. In *Proc. of SAFECOMP '08*, pages 139–152, 2008.
- [5] M. Glaß, M. Lukasiewicz, T. Streichert, C. Haubelt, and J. Teich. Reliability-Aware System Synthesis. In *Proc. of DATE '07*, pages 409–414, 2007.
- [6] M. Glaß, M. Lukasiewicz, T. Streichert, C. Haubelt, and J. Teich. Synthese zuverlässiger und flexibler Systeme. In *Proc. of ZuD '07*, pages 141–148, 2007.
- [7] M. Glaß, M. Lukasiewicz, J. Teich, U. Bordoloi, and S. Chakraborty. Designing Heterogeneous ECU Networks via Compact Architecture Encoding and Hybrid Timing Analysis. In *To appear in Proc. of DAC '09*, 2009.
- [8] M. Glaß, M. Lukasiewicz, R. Wanka, C. Haubelt, and J. Teich. Multi-Objective Routing and Topology Optimization in Networked Embedded Systems. In *Proc. of IC-SAMOS '08*, pages 74–81, 2008.
- [9] M. Lukasiewicz, M. Glaß, C. Haubelt, and J. Teich. SAT-Decoding in Evolutionary Algorithms for Discrete Constrained Optimization Problems. In *Proc. of CEC '07*, pages 935–942, 2007.
- [10] M. Lukasiewicz, M. Glaß, C. Haubelt, and J. Teich. Solving Multiobjective Pseudo-Boolean Problems. In *Proc. of SAT '07*, pages 56–69, 2007.
- [11] M. Lukasiewicz, M. Glaß, C. Haubelt, and J. Teich. Symbolic Archive Representation for a Fast Nondominance Test. In *Proc. of EMO '07*, pages 111–125, 2007.
- [12] M. Lukasiewicz, M. Glaß, C. Haubelt, and J. Teich. Efficient symbolic multi-objective design space exploration. In *Proc. of the ASP-DAC '08*, pages 691–696, 2008.
- [13] M. Lukasiewicz, M. Glaß, C. Haubelt, and J. Teich. A feasibility-preserving local search operator for constrained discrete optimization problems. In *Proc. of the CEC '08*, pages 1968–1975, 2008.
- [14] M. Lukasiewicz, M. Glaß, C. Haubelt, J. Teich, R. Regler, and B. Lang. Concurrent topology and routing optimization in automotive network integration. In *Proc. of DAC '08*, pages 626–629, 2008.
- [15] M. Lukasiewicz, M. Glaß, and F. Reimann. Opt4j - the optimization framework for java. <http://www.opt4j.org/>.
- [16] M. Lukasiewicz, M. Glaß, and J. Teich. A Feasibility-preserving Crossover and Mutation Operator for Constrained Combinatorial Problems. In *Proc. of PPSN '08*, pages 919–928, 2008.
- [17] M. Lukasiewicz, M. Streubühr, M. Glaß, C. Haubelt, and J. Teich. Combined System Synthesis and Communication Architecture Exploration for MPSoCs. In *To appear in Proc. of DATE '09*, 2009.
- [18] F. Reimann, M. Glaß, M. Lukasiewicz, C. Haubelt, J. Keinert, and J. Teich. Symbolic Voter Placement for Dependability-Aware System Synthesis. In *Proce. of CODES+ISSS '08*, pages 237–242, 2008.
- [19] T. Streichert, M. Glaß, C. Haubelt, and J. Teich. Design space exploration of reliable networked embedded systems. *Journal on Systems Architecture*, 53(10):751–763, 2007.
- [20] T. Streichert, M. Glaß, R. Wanka, C. Haubelt, and J. Teich. Topology-Aware Replica Placement in Fault-Tolerant Embedded Networks. In *Proc. of ARCS '08*, pages 23–37, 2008.