FAKULTÄT FÜR INFORMATIK

TECHNISCHE UNIVERSITÄT MÜNCHEN

TODO: Thesis type (Bachelor's Thesis in Informatics, Master's Thesis in Robotics...)

TODO: Thesis title

TODO: Author

FAKULTÄT FÜR INFORMATIK

TECHNISCHE UNIVERSITÄT MÜNCHEN

TODO: Thesis type (Bachelor's Thesis in Informatics, Master's Thesis in Robotics. . .)

TODO: Thesis title

TODO: Titel der Abschlussarbeit

Author:	TODO: Author
Supervisor:	TODO: Supervisor
Advisor:	TODO: Advisor
Submission Date:	TODO: Submission date

I assure the single handed composition of this todo: thesis type (bachelor's thesis in informatics, master's thesis in robotics. . .) only supported by declared resources.

Munich, TODO: Submission date TODO: Author

Acknowledgments

Abstract

Contents

1 Introduction

1.1 Background

Safety-Critical systems may hold several definitions but the intuitive notion behind them is the consequences of failures. Failure of such systems may lead to loss of life, potential damage of property or damage to the environment [**Knight:2002:SCS:581339.581406**]. As far as safety-critical embedded systems are concerned, ensuring functional safety in terms of freedom from unacceptable risk of physical injury or damage to the health of people, is of prime importance.

An essential design step during the engineering of Safety-Critical and Reliable embedded systems is the mapping of software components on the underlying hardware architecture, respecting various resource constraints and safety level requirements. During this phase, called the Design Space Exploration(DSE), designers have to decide between many design alternatives, representing a multi-criteria decision problem. Various national and international research projects are exploring new possibilities to automate this phase in the development process of embedded systems.

Developing Safety-Critical embedded systems requires developers to use certain tools and development techniques as suggested by appropriate standards. One such standard is ISO 26262, that ensures functional safety of electrical and electronic systems in road vehicles. Recent innovations in automotive domain such as Driver Assistance Systems, Break-By-Wire Systems and Steer-By-Wire Systems, have led to an increase in technological complexity of electrical and electronic systems for road vehicles. Therefore, ensuring the safe and reliable operation of such systems is becoming demanding everyday.

AUTOFOCUS3, developed at Fortiss GmbH, is one such research CASE tool that provides the functionality of generating deployments and schedules for mixed-critical shared-memory embedded systems [**6601578**]. Extending the deployment and schedule generation functionality of AUTOFOCUS3 with the safety metrics identified in ISO 26262 and various resource constraints such as memory, power consumption etc., will help us generate more safe and reliable deployments used in safety-critical embedded systems.

However, a pragmatic system with a large design space, may lead to multiple deployments that satisfy various deployment constraints. It is, therefore, desirable to have some optimization criteria that further reduces the design space and leads to optimal deployments.

One part of the thesis extends AUTOFOCUS3's deployment and schedule generation process with safety metrics and resource constraints, while the other part uses different MOO algorithms that optimizes multiple criteria (number of nodes, memory per node, power consumption, etc.) to yield an optimal (pareto-optimal) deployment.

1.2 Problem Statement

The AUTOFOCUS3 group, at Fortiss GmbH, is analyzing the possibility of extending the DSE phase of embedded system engineering with different safety metrics and resource constraints identified in ISO 26262, and to come up with a MOO approach that leads to pareto-optimal deployments. The real-world relevance of the results will be evaluated through implementation in the SAFE-E research project (www.safe-project.eu), which aims at bringing solutions to demonstrate compliance of ISO 26262 functional safety standard for developing safe automotive applications based on AUTOSAR architecture.

The hardware architectures used in safety critical embedded systems needs high reliability that may be affected due to random hardware failures occurring unpredictably during the lifetime of the electrical system. Such failures are difficult to explain and are often attributed to ageing effects. Hence one of the task is to integrate Hardware Reliablilty Metrics as a new criteria into existing DSE approach of AUTOFOCUS3.

The deployments can be made more realistic by taking into account various resource constraints associated with the technical architecture such as memory per node, power consumption, cost of hardware architecture, etc. Hence, the next task is to identify and integrate various resource constraints as new criteria into the DSE approach of AUTOFOCUS3.

Different safety requirements of hardware elements enforces disparate requirement stringencies and consequently different development costs. The final task of this thesis is to evaluate and compare several DSE optimization methods that optimizes multiple objectives and yield pareto-optimal deployments.

1.3 Description of the work

Here I am going to talk about the different phases in which the work was divided.

1. Finding appropriate safety metrics and resource constraints
2. Integrating them in AF3 with Z3 uses as the SAT solver
3. Integrating and evaluating new DSE optimization methods using a case study

1.4 Limitations

1. Notation of power - do not differentiate between static and dynamic.
2. Scaling with large industrial use cases is still an issue.

1.5 Organization of thesis

This thesis is structured as follows ...

2 Theoretical Background

2.1 ISO 26262

"State of the art" standard followed in automotive domain.

Different ways to assess hardware architecture for reliability in context of random hardware failures.

Explain terms like safety goal, hardware architectural metrics, PMHF, FRC, etc.

2.2 SAFE - ITEA

Talk about the safe project in brief

2.3 AUTOFOCUS3

Different layers of abstraction

1. Logical Architecture
2. Platform Architecture

And much more ..

2.3.1 Deployment and scheduling in AF3

Explanation about the deployment and scheduling process prior to inclusion of safety and resource constraints.

2.3.2 Technical Architecture Generation

Show the current work. How can it be improved with adding more criterias?

2.4 Multi-objective optimization

2.5 Pareto-efficiency

2.6 SMT Solver

Brief introduction of z3 solver.

3 Purpose Of The Work

Talk about the thesis contribution

1. Extending the DSE phase of embedded system engineering with safety metrics and resource constraints identified in ISO 26262 to yield safer and reliable deployments

2. Exploring different DSE Optimization approaches (MaxSAT for MOO, Mcses, Branch and bound, etc.) and comparing them with each other to yield an optimal deployment (pareto-optimal).

3. Integrating step 1 and step 2 into AF3 deployment and schedule generation functionality, as well as technical architecture generation functionality.

4. Evaluating the results using an industrial-like case-study in accordance with the SAFE-E project.

5. Published the results in SAFE Deliverable 4.4.a, chapter 10.

4 Phase I : DSE Of Safety Metrics And Resource Constraints

4.1 Safety metrics and deployment constraints

Need to give an example scenario depicting the importance of each type of constraint. Give the formal notations of each.

4.1.1 PMHF Constraints

4.1.2 Resource Constraints

4.1.3 Cost Constraints

4.1.4 Memory Constraint

4.1.5 Power Constraint

4.1.6 Node usage Constraint

4.2 Integration into AF3

Use an exemplary logical architecture and technical architecture and depict the effect of each constraint on deployment generation process of AF3.

Use screenshots.

5 Phase II: Pareto-Optimal Technical Architecture Generation

5.1 A new MOO Algorithms

5.2 Comparison of algorithms

5.3 Integration into AF3

6 Case Study And Results

6.1 Phase I Results

6.2 Phase II Results

7 Conclusion

8 Future Improvements

List of Figures

List of Tables