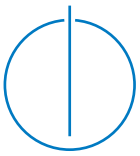
FAKULTÄT FÜR INFORMATIK

TECHNISCHE UNIVERSITÄT MÜNCHEN

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

TODO: Thesis title

TODO: Author



FAKULTÄT FÜR INFORMATIK

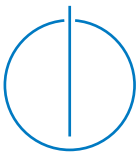
TECHNISCHE UNIVERSITÄT MÜNCHEN

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. 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.

1.2 Problem Statement

1.3 Description of the work

1.4 Limitations

2 Theoretical Background

2.1 ISO 26262

2.2 SAFE - ITEA

2.3 AUTOFOCUS3

2.4 Deployment and scheduling in AF3

2.5 Z3 Solver

2.6 UNSAT Cores

3 Purpose Of The Work

4 DSE Of Safety Metrics And Resource Constraints

4.1 Safety Constraints

4.2 Resource Constraints

4.3 Cost Constraints

5 SAFE Compliant Technical Architecture Generation

6 Case Study And Results

7 Conclusion

8 Future Improvements

List of Figures

List of Tables