Karlsruhe Institute of Technology

# A Theory of Refinement of Cyber-Physical-Systems into Implementations

Bachelor's Thesis of

Daniel H. Draper

at the Department of Informatics
Institute for Theorethical Informatics

| | |
|---|---|
| Reviewer: | Prof. Dr. Bernhard Beckert |
| Second reviewer: | |
| Advisor: | Dr. rer. nat. Mattias Ulbrich |

15. April 2015 – 15. August 2015

Karlsruher Institut für Technologie
Fakultät für Informatik
Postfach 6980
76128 Karlsruhe

I declare that I have developed and written the enclosed thesis completely by myself, and have not used sources or means without declaration in the text.

**PLACE, DATE**

Please replace with actual values

. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .

(Daniel H. Draper)

# Abstract

English abstract.

# Zusammenfassung

Deutsche Zusammenfassung

# Contents

# List of Figures

# List of Tables

# 1. Introduction

The following Bachelorthesis will try to formalize the following process: Replacing the abstract notion of the control program in a verified (by KeYmaera) Cyber-Physical-System (*CPS*) with an actual verified (by KeY) implementation through a form of Formal Refinement and being able to verify that the entire CPS still satisfys the required safety constraints, using both KeYmaera and KeY.

CPS are generally modelled as either Hybrid Automata or - Programs.(See ref. [**platzerb** ]). Mostly, this means, that an abstract version of the discrete control program is modelled, as a non-deterministic assignment of a control value (See app. A.1). To replace this non-deterministic assignment with an actual implementation a certain ”glue” or ”coupling” has to be found to translate discrete and real continous values into each other.

In logic this can be expressed as:

$$\begin{aligned} \textbf{If } (\models [controlValue := *, ?\psi(controlValue)\ldots]\alpha\ verified \\ \wedge \textit{“glue”(discreteVariables, continuousVariables)} \\ \textbf{Then } [controlValue := JavaProgram\ldots]\alpha\ also\ verified \end{aligned} \tag{1.1}$$

To explain this process we will take a look at the following:

**I:** Example-based Refinement on CPS Watertank (Example taken from KeYmaera).

**II:** Introduction of Formalized process to gain an actual implementation from a hybrid model.

**III:** Application of formalized process on example: CPS Gear-Backlash (See ref. [**bla** ]).

## 1.1. Introducing Cyber-Physical-Systems

In this thesis we take a close look at **CPS**. These are systems in which a physical aspect or value is controlled by a computer (program). For example, an aircraft control system in which the computer exerts a form of speed control on the airplane would be a CPS.

In our case we take a closer look at the closely related notion of *Hybrid Systems*, in which discrete values (in the control program) and continuous values (in the physical world) coexist. The difficulty in analyzing these kinds of systems stems from the “hybridness” of the systems: There is always some form of translation necessary to go from the program (discrete values) to the physical (continous reals) world.

two basic modelling approaches exist for hybrid systems: Hybrid Automata that are based on Non-Determnistic Finite Automata.

# 2. Example-based Refinement on CPS Watertank

### 2.0.1. Finding the concrete Control Value Assisgnment

In order to apply Eq. 1.1 to this concrete example, the first challenge we faced was finding an actual spot in which a concrete control value is actually assigned. Taking a look at the Hybrid Automata describing the Watertank (See Fig. ??),

### 2.0.2. Refining the original Hybrid Automata

### 2.0.3. Finding the correct Program Safety Condition

### 2.0.4. The (simple) Java Control Program

### 2.0.5. Finding the glue between Java and the Hybrid Model of the system

### 2.0.6. Verification based on KeYmaera

# 3. Evaluation

...

## 3.1. First Section

...

## 3.2. Second Section

...

## 3.3. Third Section

...

# 4. Conclusion

…

# A. Appendix

## A.1. Images

Figure A.1.: Watertank Hybrid Program and - Automata with Non-Deterministic Control Program Abstraction marked.