Budapest University of Technology and Economics
Faculty of Electrical Engineering and Informatics
Department of Measurement and Information Systems

Formal Verification of Activity Diagrams Using the Gamma Framework

Scientific Students' Association Report

Author:

Ármin Zavada

Advisor:

dr. Vince Molnár

Contents

Kivonat

Jelen dokumentum egy diplomaterv sablon, amely formai keretet ad a BME Villamosmérnöki és Informatikai Karán végző hallgatók által elkészítendő szakdolgozatnak és diplomatervnek. A sablon használata opcionális. Ez a sablon LaTeX alapú, a *TeXLive* TeX-implementációval és a PDF-LaTeX fordítóval működőképes.

Abstract

This document is a LaTeX-based skeleton for BSc/MSc theses of students at the Electrical Engineering and Informatics Faculty, Budapest University of Technology and Economics. The usage of this skeleton is optional. It has been tested with the *TeXLive* TeX implementation, and it requires the PDF-LaTeX compiler.

Chapter 1

Introduction

Model-Based Systems Engineering is a widely used technique for designing, testing and executing otherwise too complicated systems in a well defined, *high-level* language (e.g. SysML). Such systems usually come from critical domains (e.g. transportation, flight) which have a very low tolerance for errors. As such, early detection of otherwise deadly mistakes is mandatory.

Formal model verification is a technique (among many) for detecting such errors. They use formal proving algorithms to check whether a given system property (usually an undesired state) is *reachable* and how to reach that state. However, these proving methods require low-level, *state based mathematical models*, which are far from the high-level languages we are used to. In order to verify such models, we need to *bridge* the gap between the two worlds.

Gamma is one of such frameworks. Right now Gamma only supports composite systems of only statecharts, however, real world models use activity diagrams heavily. For this reason, I propose to add an activity language to Gamma, and with it enable the systematic verification of a larger subset of SysML models.

TODO valahol még le kéne írni, hogy milyen létező megoldások vannak (Beni, egyéb?)

TODO dolgozat felépítése

Chapter 2

Background

2.1 Model Verification

Kell ez egyáltalán? A cél az lett volna, hogy leírja a fontosságát, de ezt a bevezetőben megteszem..

2.2 Modeling Formalisms

Mondok Milán Bsc 2.2-höz hasonlóan: modellezési formalizmusok, activity formális leírása, petri net, tranzíciós rendszerek, stb

2.3 Gamma

Gamma általánosságban, jelenleg mire képes, miket támogat

2.4 SysML

SysML activity-jainak magas szintű leírása

2.5 Related Work

Itt is jó, de kicsit a bevezetőnél is beszélek róla. Talán ott jobb lenne.

Chapter 3

Activity Language

3.1 Design Decisions and Inspirations

3.2 Metamodel

3.3 Domain-specific Language

3.4 Examples

Chapter 4

Activity Model Verification

4.1 Activities as State-based Models

4.2 Transforming Individual Elements

4.3 Equivalence with Petri Nets

Chapter 5

Implementation

TODO: rövid leírása az implementációnak; kb milyen méretű a változtatás. nem szeretném hosszúra, annyira nem érdekes, viszont jó lenne valahogy mutatni, hogy nem volt azért triviális.

Chapter 6

Evaluation

Chapter 7

Conclusion and Future Work

Bibliography