Modelling, verification and experimentation for software-based systems (MOVEX)

Dominique Méry
LORIA & Telecom Nancy
Université de Lorraine
https://members.loria.fr/Mery
dominique.mery@loria.fr

March 18, 2025

Abstract

This repository contains course notes, exercises, models and projects from two courses given as part of master's level training on modelling an verifying software-based systems. It provides access to resources in the form of pdf files, TLA files, ACSL files or Rodin files. Moreover, it aims to prepare students of the fourth year of University to apply modelling techniques for software-based systems. It is divided into two main parts:

- Part 1 MALG is shared by students in software engineering and in CPS engineering; the course is oganised in 6 weeks (6 lectures x 2h00) (6 tutorials x 2 h 00). Topics are transition systems, invariance, safety, fixed-point theory, induction principles, Floyd/Hoare proof systems,
- Part 2 is divided into two distinct streams:
  - MOVEX-SE is the course is oganised in 6 weeks (6 lectures x 2h00) (6 tutorials x 2 h 00)
  - MOVEX-CPS the course is oganised in 6 weeks (6 lectures x 2h00) (6 tutorials x 2 h 00)

The table of contents shows the summary of two main courses (at Université de Lorraine/University of Lorraine) based on our experiment using the modelling languages as TLA, Event-B and ACSL

- The first course **MALG** is part of the curriculum of the second year students of Telecom Nancy who are focusing on software engineering.
- The second course **MOVEX** is part of the curriculum of the second year students of Telecom Nancy who are focusing on embedded systems, as well as students of seconf year of ENSEM.

Contents

1 Documentation and Tools

The TLA+ ToolBox platform is available at the following link.

The Rodin platform is available at the following link.

The Prob platform is available at the following link.

The Frama-c platform is available at the following link.

The Synchrone Reactive Toolbox for LUSTRE is available at the following link.

The Kind 2 platform is available at the following link.

2 Course MALG1/MOVEX1 at Telecom Nancy

2.1 Slides for the course MALG1/MOVEX1

2.1.1 Lecture 0 Overview of the course

Overview of the course

2.1.2 Lecture 1 Modélisation, spécification et vérification (I)

- Modélisation, spécification et vérification (I)
- The MODULE access_control.tla.

2.1.3 Lecture 2 Modélisation, spécification et vérification (II)

Modélisation, spécification et vérification (II)

2.1.4 Lecture 3 Modélisation, spécification et vérification (III)

Modélisation, spécification et vérification (III)

2.1.5 Lecture 4 Vérification mécanisée de contrats (I)

Vérification mécanisée de contrats (I)

2.1.6 Lecture 5 Vérification mécanisée de contrats (II)

Vérification mécanisée de contrats (II)

2.2 Lectures Notes

Notes sur la logique Notes sur la logique.

Notes sur la vérification Notes sur la vérification.

Notes sur la preuve Notes sur la preuve.

2.3 Tutorials

Notes on a tutorial using proofs Tutorial Notes for Proofs and Verifications Conditions of Contract.

Serie A Tutorials serie A.

Tutorials serie A with solutions.

TLA solutions for serie A .

Notes on a tutorial for verification conditions for the `assert` clause Tutorial Notes for verification conditions for the `assert` clause ..

Serie B Tutorials serie B.

Tutorials serie B with solutions.

ACSL solutions for serie B with additional notes .

2.4 Assessment

The assessment of students is based on three works:

- Two written exams: E1 and E2
- A practical exam: TP

2.5 Examens passés

Les sujets des années passées sont contenus dans l'archive ANNALES.zip et des corrections sont données dans cette liste:

- Correction-malg-19mars2024

3 Course MOVEX2 at Telecom Nancy

3.1 Slides for the course MOVEX2

3.1.1 Lecture 0 Overview of the course

Overview of the course

3.1.2 Lecture 1 Vérification mécanisée de contrats (III)

Lecture 1 Vérification mécanisée de contrats (III)