Modelling Software-based Systems

Dominique Méry
LORIA & Telecom Nancy
Université de Lorraine
`dominique.mery@loria.fr`

October 9, 2024

This site contains resources relating to the use of the Event-B language and the Rodin platform to verify contracts for a small sequential programming language. We give the Rodin models and a description of these models in the form of a text LaTeX.

The Event-B method is based on a modelling language used to describe state-based models and safety properties of those state-based models. The originality of Event-B lies in its ability to enable incremental and proof-based modelling of *reactive systems*. The Event-B language contains both set notations and a first-order predicate calculus; it offers the possibility of defining models of reactive systems called machines and contexts and includes the refinement relationship that allows us to follow an incremental development methodology.

Contents

1   Documentation and Tools

The main document on the Event-B modelling language and methodology is the book of Jean-Raymond Abrial [1].

The Rodin platform is available at the following link.

The list of symbols is useful for typing symbols which will appear as mathematical notations.

The first chapter on the modelling language Event-B chapter 1 summarizes details on the foundations and on the applications.

The second chapter on using the modelling language Event-B for developing sequential algorithms chapter 2 with examples.

The third chapter on using the modelling language Event-B for verifying contracts for sequential algorithms chapter 3 with examples.

The chapter [3] (from [2].) authored by Dominique Cansell and Dominique Méry and entitled *The Event-B Modelling Method: Concepts and Case Studies* has benne published from lectures notes given in a Summer School and you can use it for getting details from Event-B see the following link.

Lectures Notes *The Modelling Language* at the following link.

Chapter *Event-B* at the following link.

2   Course MCFSI at Telecom Nancy

2.1   Slides for the course MCFSI

2.1.1   Lecture 1 The Modelling Language Event-B.

2.1.2   Lecture 2 Proof Obligations.

2.1.3   Lecture 3 Checking contract using Event-B.

2.1.4   Lecture 4 Correctness by Construction with the Modelling Language Event-B using the Refinement.

2.1.5   Lecture 5 Access Control

2.2   Tutorials

Tutorial 1 Using the Event-B modelling language on simple examples.

Tutorial 2 Using the Event-B modelling language for verifying contracts.

2.3 Project

The assessment of students is based on two works:

- An written exam

- A project which is stated in the following document Projet 3A IL

3 Event-B Models

The Event-B models related to the tutoriuals are given in the next list:

3.1 Event-B Archives for the lectures

Archive Rodin for explaining differences between Event-B invariant and Eveny-B theorem. Archive Rodin for the management of school.

3.2 Event-B Archives for the tutorial 1

Archive Rodin mcfsi1-ex1-tut1.zip.
Archive Rodin mcfsi1-ex2-tut1.zip.
Archive Rodin mcfsi1-simple.zip.
Archive Rodin mcfsi1-variant1.zip.
Archive Rodin mcfsi1-variant2.zip.
Archive Rodin mcfsi1-summation.zip.
Archive Rodin mcfsi1-ressource-pb1.zip.
Archive Rodin mcfsi1-ressource-pb2.zip.
Archive Rodin mcfsi1-invariantsafety.zip.
Archive Rodin mcfsi1-ex8.zip.
Archive Rodin mcfsi1-ex9.zip.

3.3   Event-B Archives for the tutorial 2

3.4   Event-B Archives for the tutorial 3

4   Course Modelling and verifying software-based systems for Master in Compurer Science of the University of Lorraine

4.1   Slides of the course

4.1.1   Lecture 1 The Modelling Language Event-B.

4.1.2   Lecture 2 Proof Obligations.

4.1.3   Lecture 3 Correctness by Construction with the Modelling Language Event-B using the Refinement.

4.1.4   Lecture 4 Access Control

4.2   Tutorials

Tutorial 1 Using the Event-B modelling language.

5   Event-B Models

The Event-B models related to the tutoriuals are given in the next list:

5.1   Event-B Archives for the lectures

Archive Rodin for explaining differences between Event-B invariant and Eveny-B theorem.
Archive Rodin for the management of school.

5.2   Event-B Archives for the tutorial 1

Archive Rodin ex1-tut1.zip.
Archive Rodin ex2-tut1.zip.
Archive Rodin ex4-tut1.zip.
Archive Rodin ex51-tut1.zip.
Archive Rodin ex52-tut1.zip.
Archive Rodin ex6-tut1.zip.
Archive Rodin ex7-tut1.zip.
Archive Rodin ex8-tut1.zip.
Archive Rodin ex9-tut1.zip.
Archive Rodin mcfsi1-variant1.zip.
Archive Rodin mcfsi1-variant2.zip.

References

[1] J.-R. Abrial. *Modeling in Event-B: System and Software Engineering*. 2010.

[2] Dines Bjørner and Martin C. Henson, editors. *Logics of Specification Languages*. EATCS Textbook in Computer Science. Springer, 2007.

[3] Dominique Cansell and Dominique Méry. *The event-B Modelling Method: Concepts and Case Studies*, pages 33–140. Springer, 2007. See [2].