

**Clayton School of Information Technology**  
**FIT3013 Assignment 1a and b**  
**Train Control to Major Tom**  
**Basic Specification**

Due Date: (a1-2,b1-3) 12noon, 23 Mar 2009

Due Date: (c1-3) 12noon, 30 Mar 2009

## 1 Assignment Objectives

This assignment is about building a simple specification of a railway system. You are to use the RODIN tool to build the specification. Objectives addressed by this assignment include

- 1 An understanding of the Fundamentals of the Event-B Method
- 5 The role of proof obligations and consistent specifications
- 10 Skills in using the Event-B notation to develop and prove software specifications
- 11 The ability to install an Event-B toolkit (such as Rodin) on a Unix/Linux/Mac/Windows platform
- 12 The ability to write basic Event-B specifications

## 2 Submission

Submit your solution as a single zip or tar file containing PDF file generated by LaTeX through the Moodle submission mechanism. Your submission **MUST** be labelled *<your student ID>.pdf*. LaTeX is encouraged for this purpose, and should include the LaTeX generated listings of your specification from Rodin.

Multiple submissions are allowed, but only the last one received by the due date will be marked.

Submit your solution as a single zip or tar file (please, no RARs!) containing your answers as a PDF generated by LaTeX (*answers.pdf*), the PDF specification code generated from the Rodin LaTeX files (*A1.Context.pdf* and *A1.Machine.pdf* - including comments, please!), and an exported file system (*A1.Project*) of your project from Rodin. The zip/tar file should be submitted through the Moodle submission mechanism. Your submission **MUST** be labelled *<your student ID>.tar/zip/tgz*. Multiple submissions are allowed, but only the last one received by the due date will be marked.

You **must** submit the answers to questions 4 and 5 by the first deadline (23 Mar 2009), but you can delay submitting your solution to question 6 until the second deadline (30 Mar 2009). Late penalties will be applied at the rate of 1 mark per working day late, counting from each deadline (the two parts are worth 10 marks each). You should use the same format for both submissions, and include your answers for questions 4 and 5 in your submission for question 6 (add machine *A1.SignallingMachine* to your project file *A1.Project* – in the spirit of true refinement :-)

## 3 Background

In lecture 1, one of the applications cited for the (Event-)B method has been the development of various safety-critical systems such as railway signalling. Using the approach of the island bridge system discussed as a case study in lectures, you are to develop a simple model of the Huntingdale-Rowville railway line. (Further information about this proposed line can be found in the Moodle and Web Pages.)

The system is to initially modelled as single track (called a **section**) between the two terminals (Huntingdale and Rowville), with sidings and platforms (a distinction need not be made between

the two at this stage) at each end to store spare trains. Multiple trains may be stabled in the platforms or sidings, but only one train may be travelling between the two terminals at any one time. (Hint: trains take a finite time to traverse the section.)

#### 4 Context Design, Basic System

- a.1 Design a context `A1.Context` for the system.
- a.2 Identify at least one theorem for your context, and prove it. You should attempt this proof by hand, and show the steps of the proof in your answer.

*(5 marks)*

#### 5 Machine Design, Basic System

- b.1 Design a machine `A1.BasicMachine` for the system.
- b.2 Give a brief explanation of the variables and events in your machine. (You can use the comments fields in the Rodin tool to do this.)
- b.3 Attempt to discharge the proof obligations. Comment on any undischarged POs, and explain the reasons why they are undischarged (or prove them by hand).

*(5 marks)*

#### 6 Machine Design, Signalling System

You are to add signals to the system. There is one signal at each end of the track, indicating either a red aspect (do not proceed) or green aspect (you may proceed). Design a **new** machine, which refines `A1.BasicMachine`, and has additional state to model these signals. You may need to extend the `A1.Context` context, but make sure that your changes to the context do not affect your `A1.BasicMachine`.

- c.1 Design a machine `A1.SignallingMachine` for the system.
- c.2 Give a brief explanation of the variables and events in your machine. (You can use the comments fields in the Rodin tool to do this.)
- c.3 Attempt to discharge the proof obligations. Comment on any undischarged POs, and explain the reasons why they are undischarged (or prove them by hand).

*(10 marks)*