Specification Critique

Group 03
se2020.grp03@cse.unsw.edu.au

05 August 2012

Contents

Chapter 1

Specification Critique

1.1 Introduction

Invariants & Theorems

Invariants should express all constraints on the machine that are important to the integrity of the system. They are not merely used as a method to declare variable types. The invariants should be used to specify the semantic relationships between variables. It is also said that invariants should be as strong as necessary but no stronger. Theorems provide a way for checks to confirm those properties that are *"obviously"* true.

Correctness & Consistency

Correctness & consistency is one of the important aspects in a model. Not only the model has to be correctly modelled, i.e. all proof obligations discharged, it has to be consistent with the requirements. The model also has to be complete, fulfilling all the requirements.

Concrete

The models should describe behaviour, not details of how that behaviour is obtained. Therefore, models should be abstract, rather than concrete.

Machine Sequence

The way the refinements are carried out in the model should be in a way that the previous machine has a link to the next. The refinements should carry over properties is related to the previous machine.

Clarity

The model should be readable by humans. A model that looks complicated and impressive might not be a good model. Don't confuse complexity with quality. Readability of naming convention is also very important.

1.2 Invariants & Theorems

1.3 Correctness & Consistency

1.4 Concrete

1.5 Machine Sequence

1.6 Clarity

Chapter 2

"New" Specification Summary

Chapter 3

Project Plan

Chapter 4

Appendix