INSTITUTO SUPERIOR TÉCNICO
UNIVERSIDADE DE LISBOA

Specification of Software 2015/16
1st Project Report

Daiane Oliveira ist423160
Tiago Diogo ist173559

November 8, 2015

1 PROJECT APPROACH

Given the operations and restrictions presented in the project statement the group decided to use a hierarchical approach, where each machine would be responsible for a specific group of operations and restrictions. This allows the use of a refinement process where each machine considers a single dimension and is then refined and expanded with the operations and restrictions of the next dimension. The used machines are explained in the following section, ordered by the refining sequence (each item refines the previous).

2 DEVELOPED MACHINES AND CONTEXT

Machine mac_users The abstract model. In this machine we addressed the management of the users. The static part (SETS and AXIOMS defining the use of the CONSTANTS for the finite sets) was developed in Context ctx1. The state was modelled with 3 variables representing the USERS and their properties. The machine is responsible for the 4 user management operations and respects the restrictions [1-9]

Machine mac_files The mac_users refinement. In this machine we addressed the file management section. The state was modelled with 7 variables representing the FILES, their properties as well as the local versions and archive capabilities. The machine is responsible for the 4 file management operations and respects the restrictions [10-19,38]

Machine mac_shares The mac_files refinement. In this machine we addressed the sharing functionality. The state was modelled with 2 variable representing the sharing MODE and the USERS with access. This machine is responsible for the 3 file sharing operations and respects the restrictions [20-37]

Machine mac_backups The mac_shares refinement and final machine (GitBob). In this machine we addressed the backup and restore capabilities. The state was modelled with 2 variables that kept record of the files being backed up and their log history. The machine is responsible for the 3 backup and restore operations and respects the restrictions[39-50]

3 INTERACTIVE PROVER

The following profs were not automatically proved and required the group intervention

Machine mac_files uploadFile/inv4/INV

Machine mac_shares addFile/inv2/INV

Machine mac_shares downgradeBasic/inv6/INV

Machine mac_shares uploadFile/inv5/INV

Machine mac_backups uploadFileWithBackup/inv2/INV

Machine mac_backups addFile/inv3/INV

Machine mac_backups uploadFileWithBackup/inv2/INV