T-79.5303 Safety Critical Systems

Home Assignment 2008

Teemu Tynjälä

April 10, 2008

Ilkka's questions

(Neil Storey, Chapter 15.2 An explosive chemical plant - the material for the question is found in the links on the course web page)

1. List potential hazards of the basic nitrator process

2. Explain the function of the safety system components

3. Write safety requirements for the control system and link them to your list of hazards (show the relation between a safety requirement and a hazard)

Teemu Tynjälä

Teemu's questions - 1

A machine **Access.mch** is provided on the course web page with this assignment.

Add an operation **exchange** to Access, which switches the printers associated with two users. Submit the B code for the new operation (it's a good idea to simulate the whole machine with this change, but only the new operation code is required to be submitted).

Teemu's questions - 2

Still dealing with the Access machine..

Add an operation **maintenance** to Access, which removes one printer from the relation *access* (the first parameter to the operation), and associates all of the corresponding users with an alternative printer (the second parameter to the operation). Submit the B code for the new operation.

Teemu's questions - 3

Still dealing with the Access machine..

Introduce into the invariant of *Access* the condition that no user should have access to more than 6 printers. Which operations are not consistent with your revised invariant? Strengthen the preconditions of any such operations.

In your answer, submit the new invariant clause, and the changed operations.

You may find the inconsistent operations simply by observations. If you want to use ProB to help, you can change the set sizes in the **Preferences -> Animation Preferences** menu. Pick the "Size of unspecified sets in SETS section" and experiment with different values. This helps you to find the invariant violations.

Teemu Tynjälä

Teemus's questions - 4

A car park has 640 parking spaces. Give an abstract machine which specifies a system to control cars entering the car park. It should keep track of the number of cars currently in the car park, and should provide three operations:

- **enter**, which records the entry of a new car. This should occur only when the car park is not full;
- **leave**, which records the exit of a car from the car park;
- $nn \leftarrow$ **query**, which outputs the number of cars currently in the car park.

Submit the complete B machine for this question. It's a good idea to model check your answer for 1000 steps to make sure it's OK.

Teemu Tynjälä

Teemu's questions - 5

What is the weakest precondition required for the following statement to establish a state in which $category \neq medium$?

CASE (i + 2)/3 **OF**
EITHER 0 **THEN** category := small
OR 1 **THEN** category := small
OR 2 **THEN** category := medium
OR 3 **THEN** category := medium
ELSE category := large
END

Teemu's questions - 6

What does the following statement achieve?

ANY a **WHERE** $a \in \mathbb{N}_1 \wedge a \leq 5$ **THEN** $total := total + a$ **END**

What is the weakest precondition required for it to guarantee the postcondition $(total > 8)$?

($\mathbb{N}_1$ set means the natural numbers starting with 1)

Teemu’s questions - 7

Read the article "Meteor: A successful Application of B in a Large Project". Answer the following questions:

1) Draw a schematic diagram of each of the 4 subsystems of the Paris metro line 14.

2) Compare formal development with conventional development (waterfall model). What are the advantages of formal development over conventional development? Contrast the two methods especially on the dimension which development steps may be automated and which must always be completed by humans.

3) How was Meteor organization structured to support system development via B?

Your answers to the 3 subquestions (total length) should be 1-2 pages.

Teemu Tynjälä

Due Dates + Submission format

- You have until midnight on May 9 to return the assignments.
- Make an electronic submission (*.doc, *.ps or *.pdf – B machines sent separately as text files) and mail your answers to Ilkka and myself to addresses teemu.tynjala@nokia.com and HERTTUA@uic.asso.fr)