AGREE Exercises

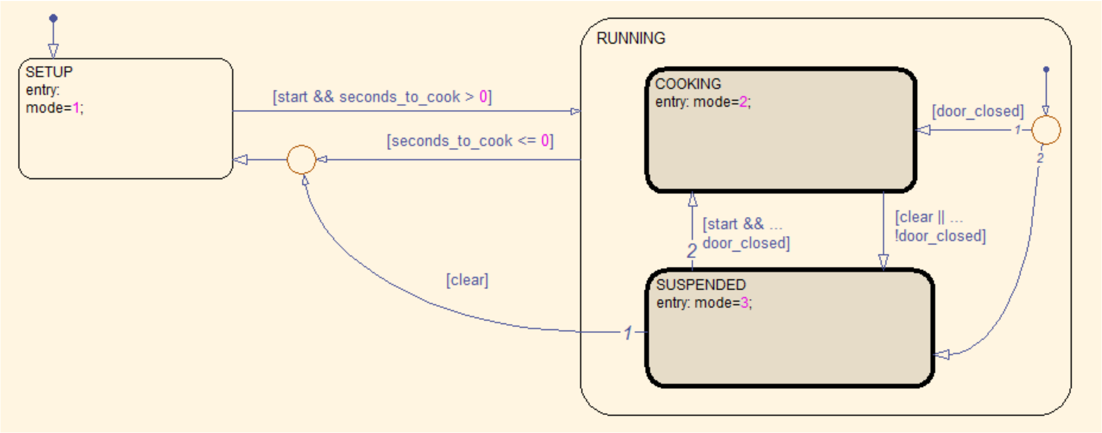
Mike Whalen
10/2013

First, use the AGREE User's Guide (in the smaccm/Documentation/AGREE directory) to install OSATE and AGREE. The exercises will reference models in three locations, documented below. Please follow the instructions in the AGREE User's guide to import the projects into the OSATE environment.

The first project is /smaccm/models/GPCA. This directory contains a medical device infusion pump example discussed in a HILT 2013 paper that is also contained in the directory. This model provides a good example of behavioral composition across multiple subsystems.

The second project is /smaccm/models/Toy_AGREE_Models/Toy_Example. This example is described in our "Your What is My How" IEEE Software article that is also included within the directory.

The third project is /smaccm/models/Microwave, which is the main focus of this exercise. This example defines the behavior for a very simple microwave controller in terms of two subsystems that control the operating mode of the microwave (Mode_Control) and the display panel (Display_Control), respectively. The Mode_Control uses a simple state machine to control its behavior:



The mode controller starts in the SETUP mode, and transitions to the RUNNING mode when the start button is pressed (if the seconds_to_cook parameter is > 0). In the RUNNING mode, the microwave can either be in COOKING or in SUSPENDED mode. If the microwave door is opened when in RUNNING mode or the clear button is pressed, then the microwave is in SUSPENDED mode, where the user can either press the start button to go back to COOKING, or press the clear button again to go back to SETUP.

Similarly, the Display_Control model processes keypad inputs and displays the time to cook (in terms of three digits that represent minutes, tens of seconds, and seconds, respectively). If the microwave is RUNNING, then the numeric keypad buttons are locked out; the user can't change the time when the microwave is running (try this on your microwave at home!). While the microwave is COOKING, the digits should decrease (along with the total seconds to cook); when it is in SUSPENDED, the display digits should be frozen. In SETUP mode, the user can program in the desired time to cook.

When the microwave is assembled from these two subsystems, we should be able to prove three safety properties about the overall microwave behavior:

```
        guarantee "The heating element is on only when door_closed_sensor is true"
        guarantee "When the heating element is on the time to cook shall decrease"
        guarantee "When time to cook is zero, the heating element shall be off"
```

I have provided the skeleton of the microwave example and a set of property skeletons (currently all set to 'true') that you must fill in to verify the system level safety properties.

a. [5 points] For the Integer_Toy.aadl and Real_Toy.aadl files, briefly describe why the property is true when the types of the inputs and outputs are Integers, but false when they are floating points.

b. [5 points] For the Real_Toy.aadl file, what is the maximum value that you can use as an assumption for the Input?

c. [25 points] fill in the definitions of the guarantees in the Microwave example and prove that the components are consistent and that the system properties are satisfied. Include the .aadl file that you create as a separate file.

d. [10 points] Which (if any) of the three system properties actually require guarantees on all components, and which require guarantees on only a subset of the components? Why?

e. [10 points] Is it possible to write a property of the form: "The microwave will eventually stop cooking?" Why or why not? If so, write it in AGREE. If not, is it possible to approximate the property?