CMU 17-651 Models of Software Systems

Project 2: Concurrency

Garlan & Kang **Due: November 14, 2018**

The purpose of this second project is to give you experience in modeling a realistic system as a state machine using concurrency. The example that we will use is the familiar Infusion Pump. A general description of an Infusion Pump and a variety of documents describing failures of real infusion pump systems can be found in the Infusion Pump Documents Module on the class website. The key ideas that we would like you to get out of this project are: (1) the use of concurrency to manage complexity, separate concerns, model reality; (2) checking of properties related to concurrency (safety and liveness); and (3) additional practice in creating appropriately abstract models.

You should carry out this project in your assigned team. Make sure that everyone in the group contributes to the overall effort. Each team should submit a single write-up of the project, due at the beginning of class on the project due date. We have posted a template for a group project write-up under the Latex section of the course web site.

To give you a head start, we are including a very simple model of an infusion pump, which you may want to use as a starting point for your modeling effort.

Task 1 (50 points): Modeling with Concurrency

Model a 2-line infusion pump in FSP, using concurrency to factor the model into parts that represent different concerns. Possibilities for separation include things like (a) power system (b) an individual line (c) alarms (d) user interface for setting of the pump (both initially and during operation).

As always, you will need to pick a level of abstraction appropriate for this model, and it is up to you to figure out what are the significant aspects of the system that should be included in your model.

Task 2 (32 points): Stating and Checking Properties

Once you have your pump specified, consider the following properties. For each say (a) whether the property is a safety or liveness property, (b) whether your model allows you to check this property, and if so, (c) whether it is true or not, and what features of FSP and LTSA allowed you to check the property. It would be particularly helpful if you include in your write-up the specific checks that you performed – which should also appear in your FSP file. (Note: not all of these properties have to be true of your pump, depending on how you interpret the requirements for an infusion pump.)

1. The pump cannot start pumping without the operator first confirming the settings on the pump.
2. Electrical power can fail at any time.
3. If the backup battery power fails, pumping will not occur on any line.
4. It is always possible to resume pumping after a failure.
5. An alarm will sound on any line failure (blockage, pinching, empty fluid, or whatever failures you model).
6. In the absence of errors the pump will continue to pump until the treatment is finished.

7. The system never deadlocks.
8. Property A of your choosing.
9. Property B of your choosing

Task 3 (18 points): Reflection

You have now seen several notations for specifying systems and their properties: Pre-post conditions, Alloy, and FSP (LTSA). In this part of the report we would like you to reflect on that experience. For each of these notations write a paragraph or two explaining:

1. What are the strengths of this notation and its tools? Under what situations would you recommend its use? Why?
2. What are the weaknesses of this notation and its tools. Under what situations would you not recommend its use? Why?
3. With respect to this notation, what is the single most-important future development that would be needed to make it more generally useful to practitioners?