Using Medical Devices to Teach Formal Modeling
Orieta Celiku and David Garlan
Carnegie Mellon University

Motivation
Offer suitable training in formal modeling to practicing engineers and domain specialists through educational materials that:
- Show how formal modeling can be used to improve the quality and reliability of software-intensive systems
- Provide guidelines on selecting appropriate modeling approaches for the problem at hand
- Give students hands-on experience in modeling and tool-assisted analysis

Modeling Notations
- **State Machines**
  - Provide simple abstractions of complex systems
  - Have intuitive graphical representations
  - Underlie many formalisms
- **Abstract Specification Languages**
  - Based on set theory and logic
  - Provide calculi for building specifications from parts and refining specifications
- **Concurrent Processes**
  - Suitable for modeling interaction
  - Enable analysis of important liveness and safety properties

Modeling Tasks: Infusion Pump as Unifying Example

Infusion Pump
- Regulates intravenous flow of liquids to patients
- Complex and safety-critical system
- Well-documented features and failures

Students model an infusion pump in a series of tasks focusing on three formal notations.

![Diagram of Infusion Pump](image)

**Task 1: Modeling with State Machines**
- Extend model to account for errors, such as occlusions in the line, power failure, etc.
- Decide on additional functionality to model, such as set-up, self-checks on start-up, and pump control by nurse or patient

**Base Specification**
- Single-line pump
- Captures rudimentary behavior, basic flow of processing

**Task 2: Modeling with Abstract Specification Languages**
- Extend model to handle multiple delivery lines
- Specify the pre- and post-conditions for safe operation
- Specify remedies in the presence of failures
- Use calculus to build larger specifications from smaller ones

**Task 3: Modeling with Concurrent Processes**
- Use concurrency to factor the model into parts representing different concerns
- Parts to model: power system, individual lines, alarms, interface for set-up and pump control

Model Analysis
Students are asked to analyze their models:
- Which aspects of the pump did you choose to model; which did you choose to leave out?
- State some general properties that your pump guarantees.
- Which recorded failures of real infusion pumps does your model address?
- What ambiguities in the English description of the infusion pump does your specification resolves?

Reflection
Students answer questions reflecting on their experience:
- What are the strengths and weaknesses of the notation and tools used?
- Under what situation would you recommend using each notation?
- With respect to each notation, what is the single most-important future development that could make it more generally useful to practitioners?