Verification of Programmable Logic Controllers for Critical Infrastructures

McKenzy Heavlin
CS 584
Spring 2025

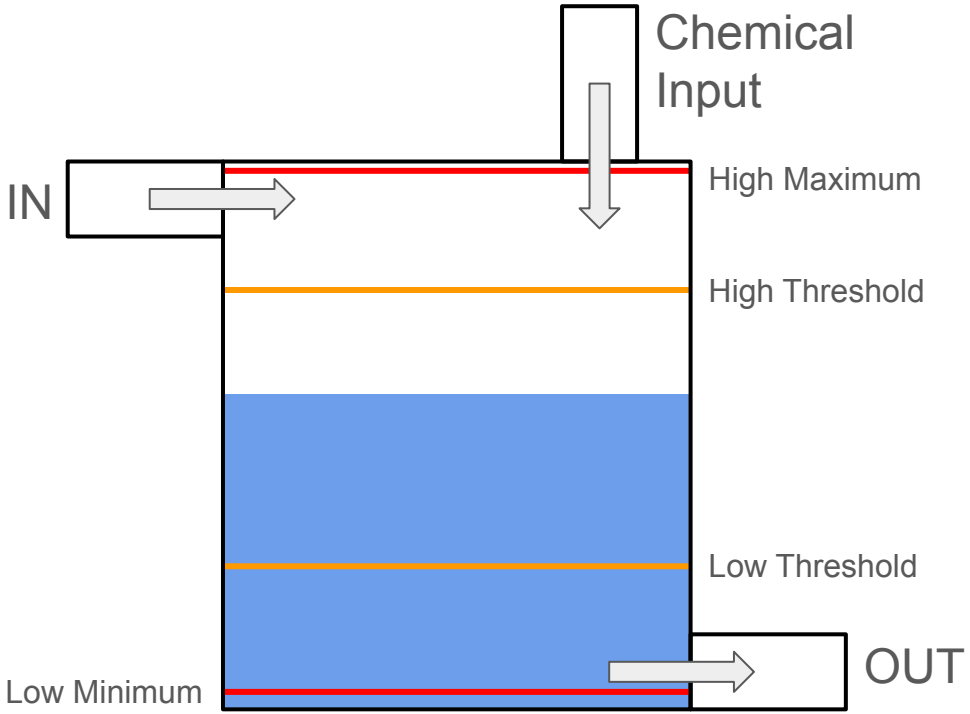
Background & Problem Statement

Programmable Logic Controllers (PLCs) are computers specifically designed to **manage and run industrial plant processes** reliably and repeatedly.

PLC programs must **operate safely** and **adhere to strict safety principles** assigned by system operators.

<u>Goal:</u> verify simple PLC controller code in a simplified system.

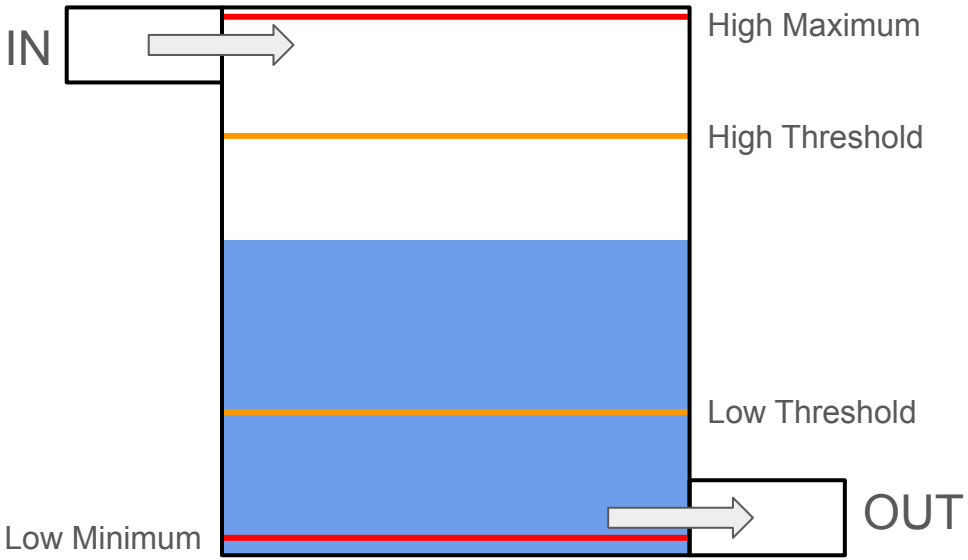
Problem Setting: Water Treatment Facility

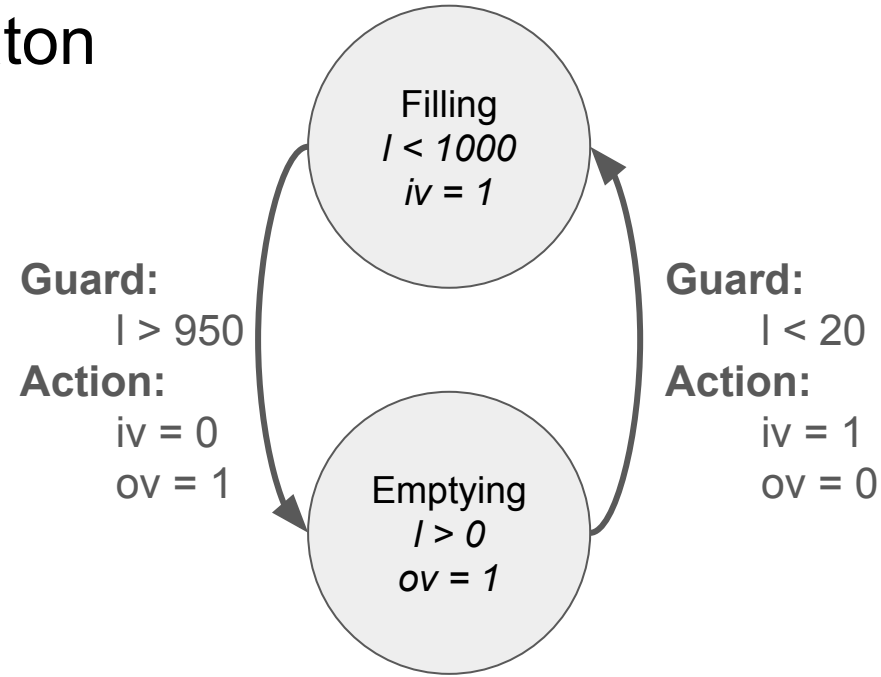


- Sensor's monitor the thresholds, maximums, and chemical input rate
- Valve actuators enable opening/closing of all input and output valves

- Focus on water thresholds, flow rates first; then add in chemical dosing if time allows

Converting to a Simple Automaton

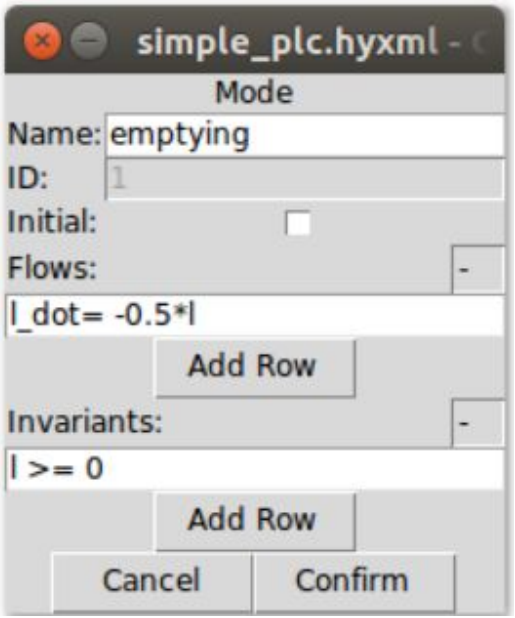


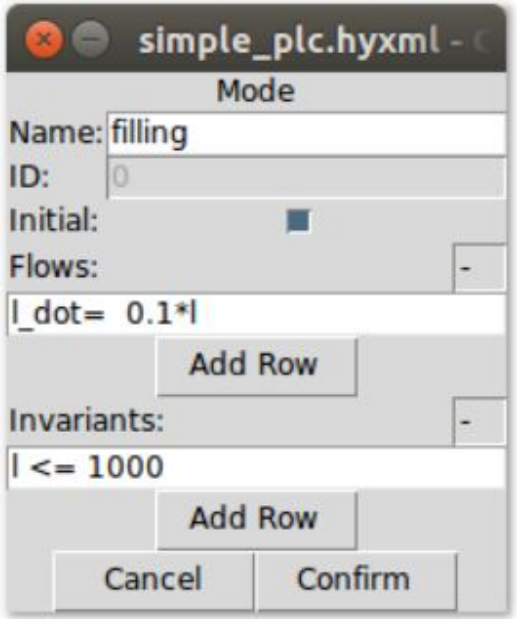


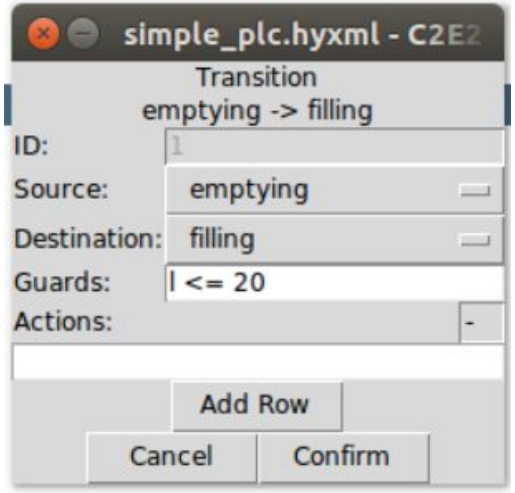
Explored adding an *'Idle'* state where the '*iv=0*' and '*ov=0*' but ran into C2E2 difficulties

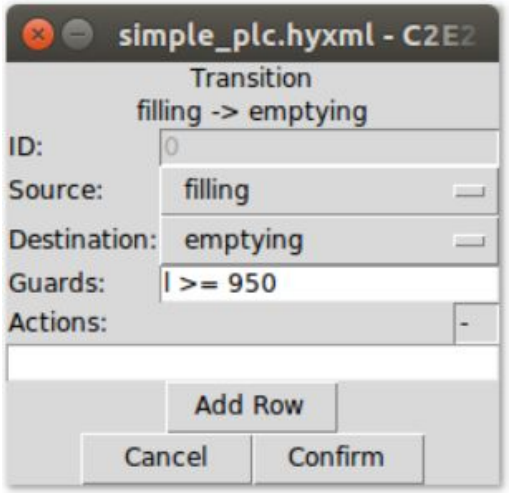
C2E2 Conversion – Sanity Check

- Most simple automaton with one variable, two modes









C2E2 Conversion – Sanity Check

Requirement

Name: low_level

◆ Safety

Time step: 0.1

Time horizon: 20.0

K value: 0.0

Simulator: ODEINT: fixed step

Refinement: Default Strategy

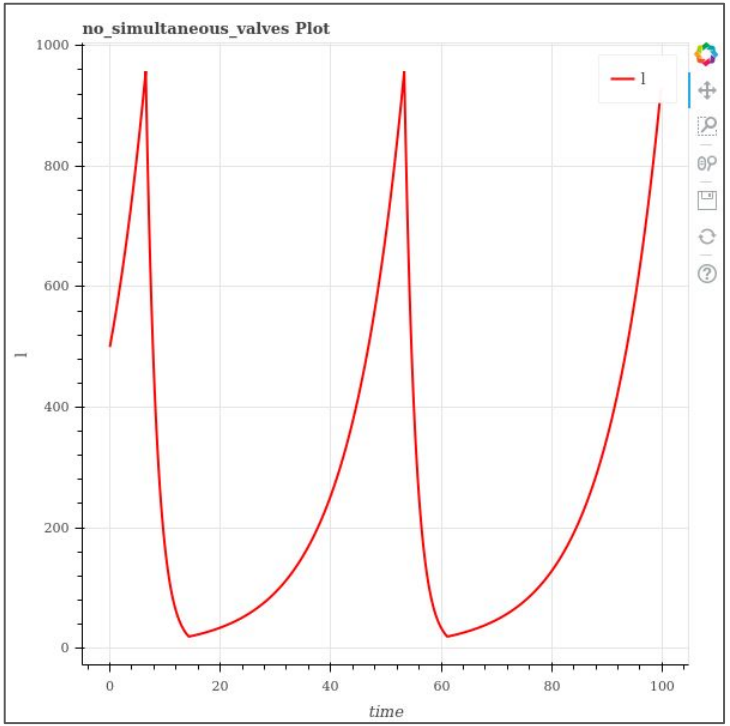
Linear Model: Generalized Star

Initial set:

```
filling: l == 50
```

Unsafe set:

```
l < 0
```

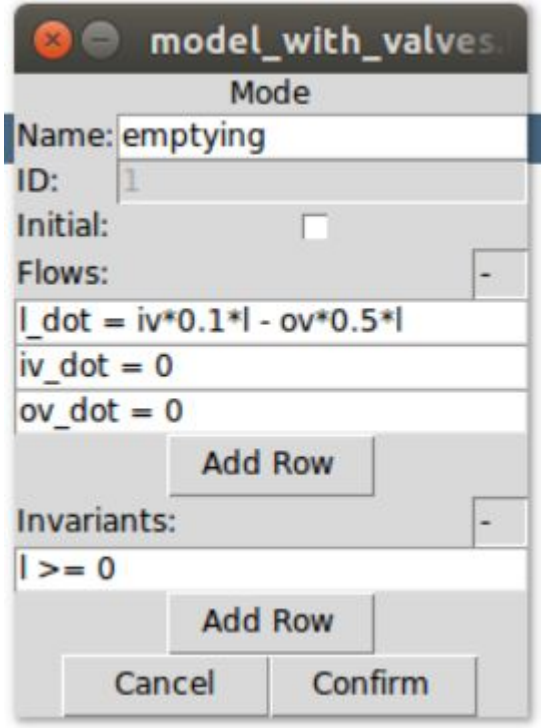


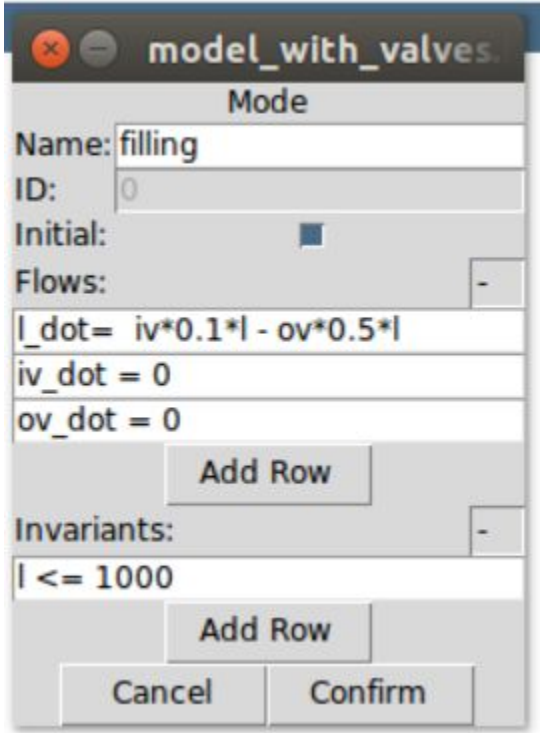
Requirement List

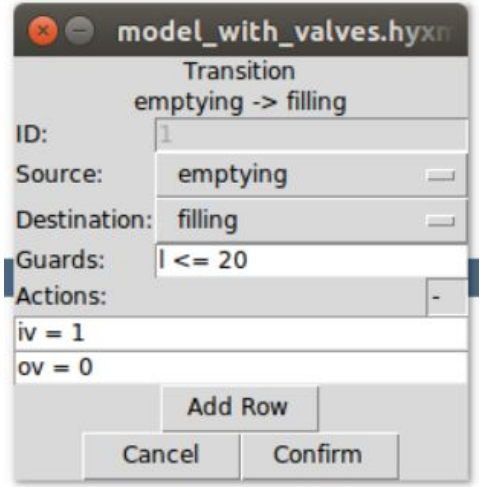
Requirement	Status	Result
high_level	Verified	Safe
low_level	Verified*	Expired

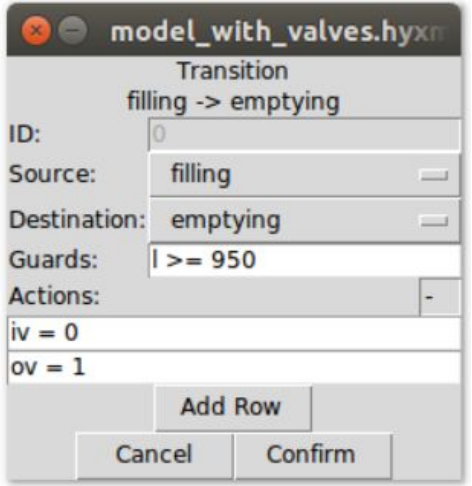
C2E2 Conversion – Adding in Valves

Updated Modes: 3 variables









C2E2 Conversion – Adding in Valves

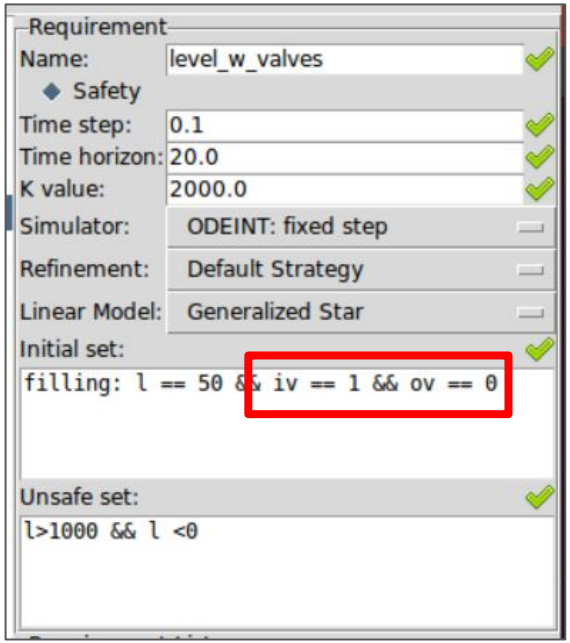
- Need initial states for the valves and a new unsafe set
- Checking that *'iv'* and *'ov'* aren't open at the same time

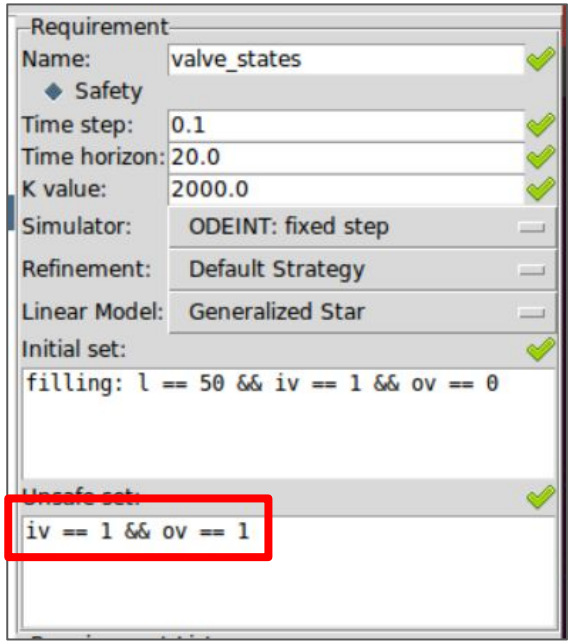
Requirement List

Requirement	Status	Result
level_w_valves	Simulated	Safe
valve_states	Simulated	Safe

Requirement List

Requirement	Status	Result
level_w_valves	Verified	Safe
valve_states	Verified	Safe





C2E2 Simulation

"Sequence of initial states are drawn randomly from the starting set. Once the simulation is computed, the result is checked to see if any guards are hit"

- C2E2 User Manual

C2E2 Conversion – Adding in Valves

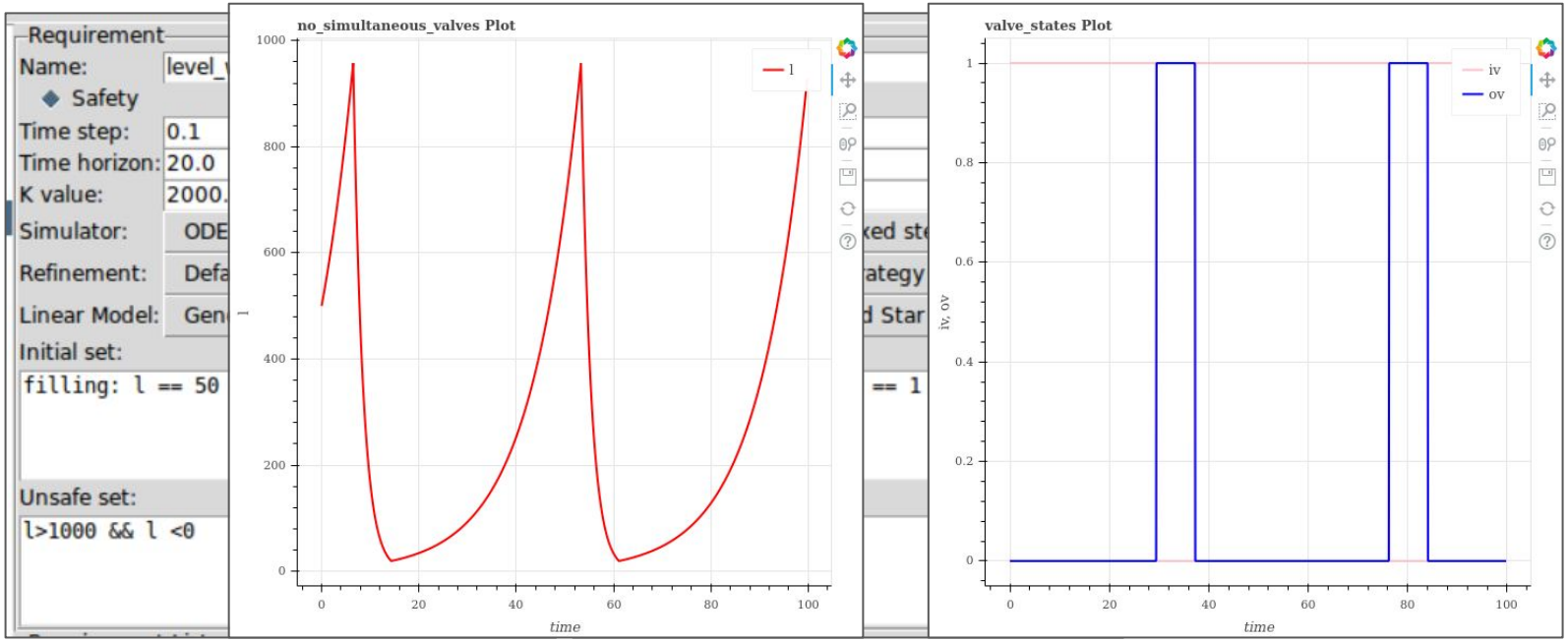
- Need initial states for the valves and a new unsafe set
- Checking that *‘iv’* and *‘ov’* aren’t open at the same time

Requirement List

Requirement	Status	Result
level_w_valves	Simulated	Safe
valve_states	Simulated	Safe

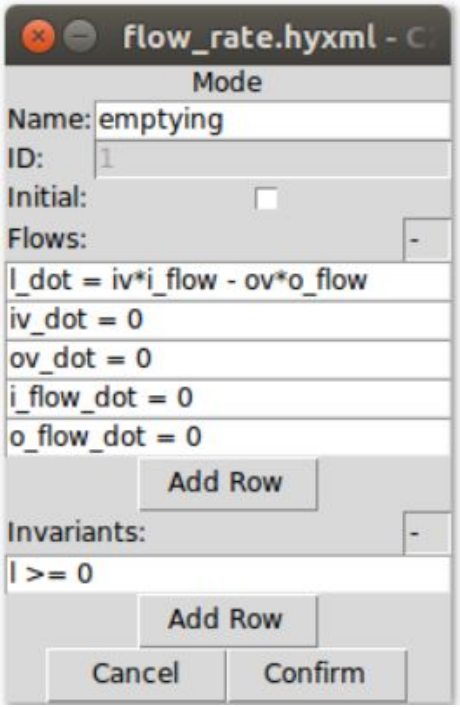
Requirement List

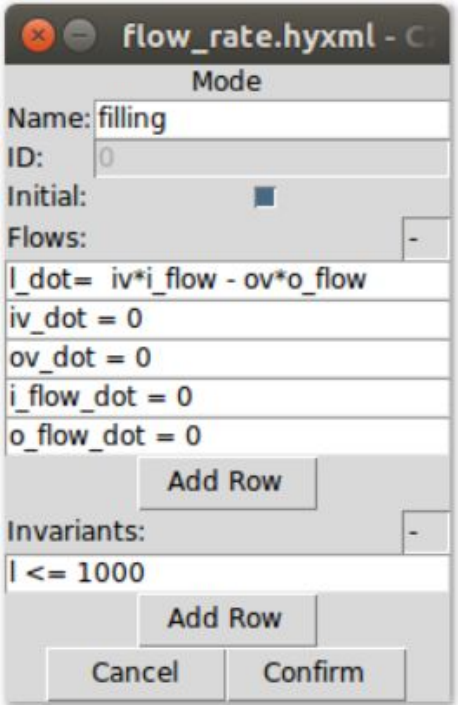
Requirement	Status	Result
level_w_valves	Verified	Safe
valve_states	Verified	Safe

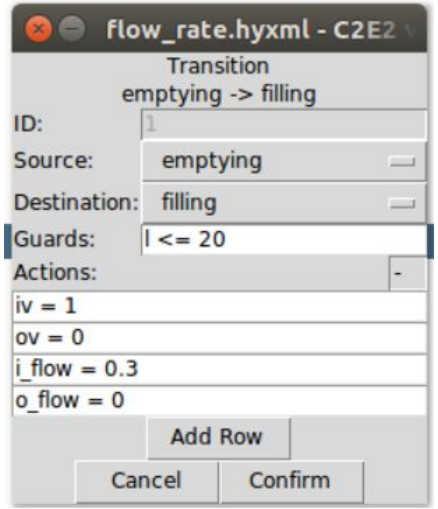


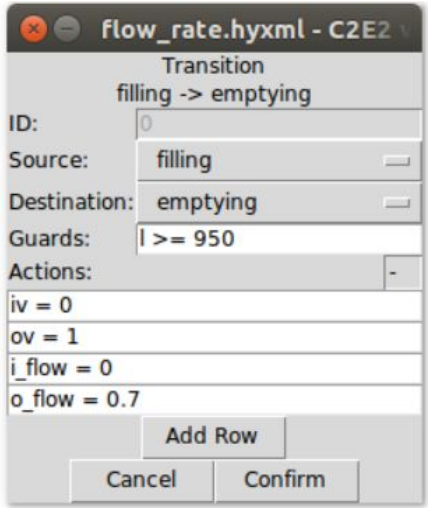
C2E2 Conversion – Adding in Flow Rates

- Update model to reflect variable flow rates (5 vars)



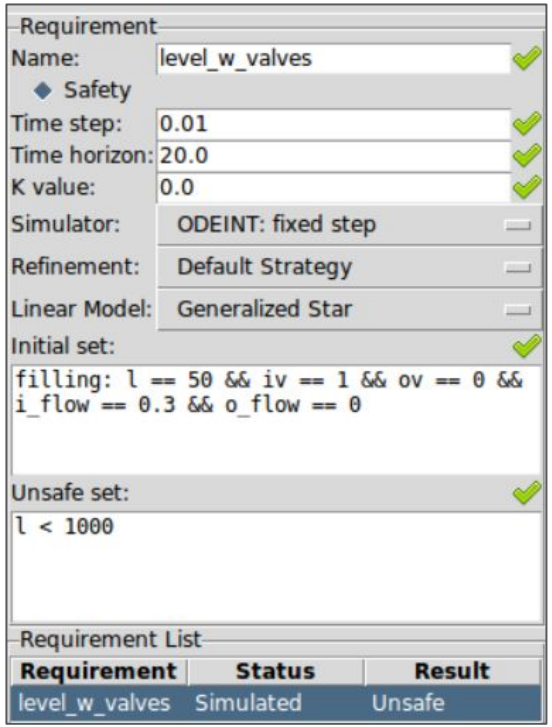


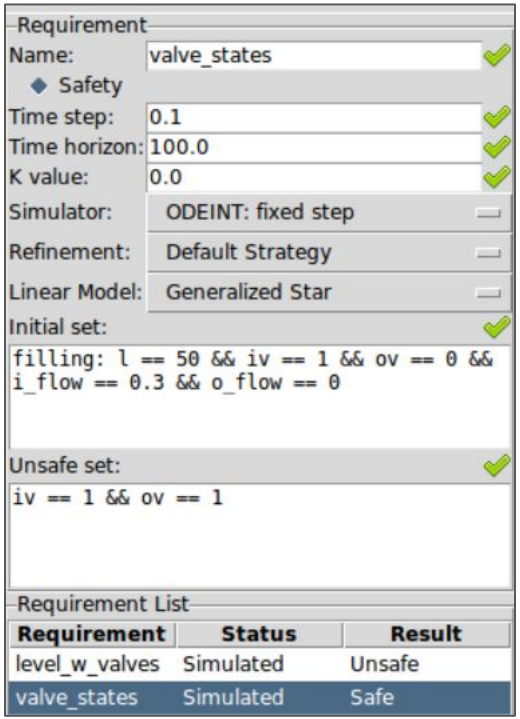


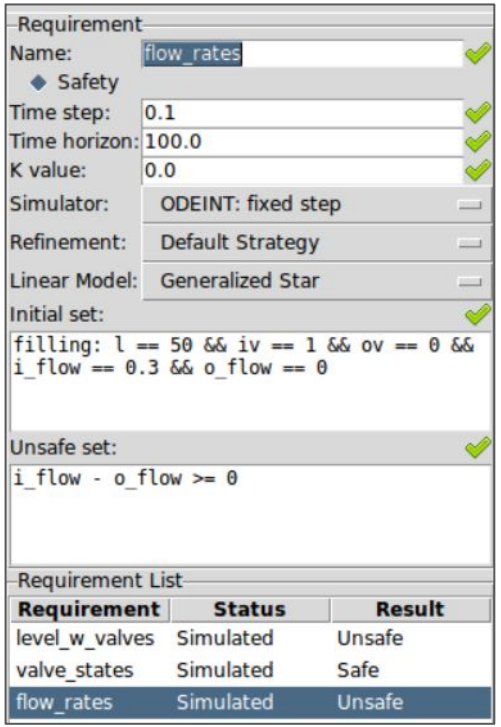


C2E2 Conversion – Adding in Flow Rates

- Update initial set and check a new condition

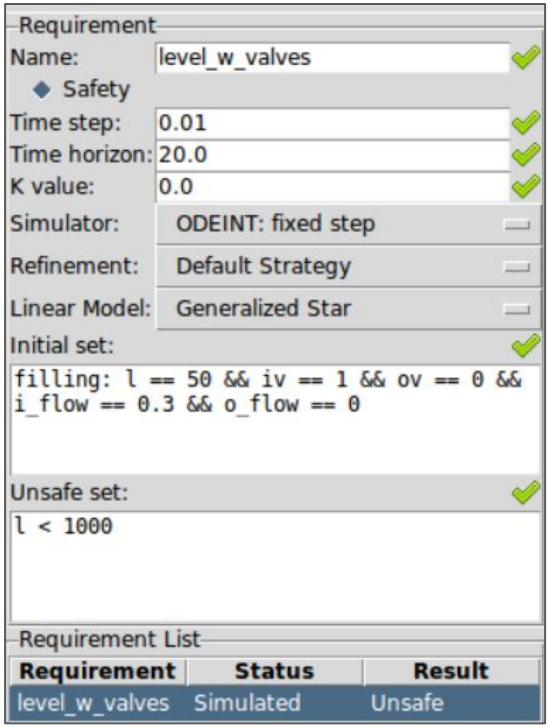






C2E2 Conversion – Adding in Flow Rates

- The issue:
  - Values quickly bypass the *l < 1000* condition
  - Appears to never make the transition from *filling -> emptying*
  - Implies there is some error in the transition between modes which I have yet to debug
    - User manual not too helpful
    - ChatGPT suggested it may be an issue with the time step granularity and how C2E2 progresses – not too convinced of this though



Challenges

- Interaction between transition guards/actions and mode invariants
- Software would buffer *for a while* if too many variables were added at once
- C2E2 documentation was not very helpful—lots of trial and error
- Poor warning/error messages made debugging a pain

Challenges

- Interaction between transition guards/actions and mode invariants
- Software would buffer *for a while* if too many variables were added at once
- C2E2 documentation was not very helpful—lots of trial and error
- Poor warning/error messages made debugging a pain

Next Steps

- Finish integrating the flow rate variables with a possible third *‘Idle’* state
- Add a *timer* variable to ensure that the valves don’t change state too frequently
- Attempt to add chemical dosing [if time allows]

Questions?