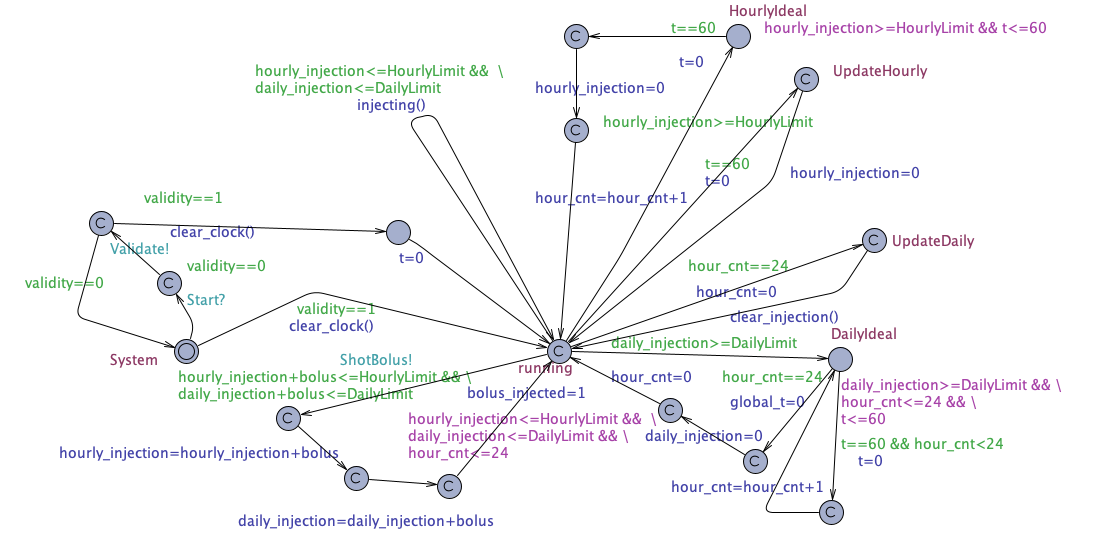
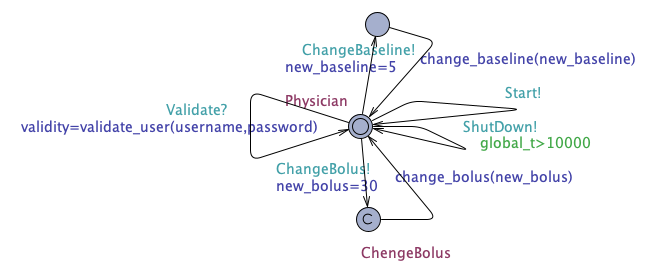
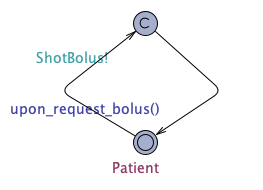
## T4: Model Checking

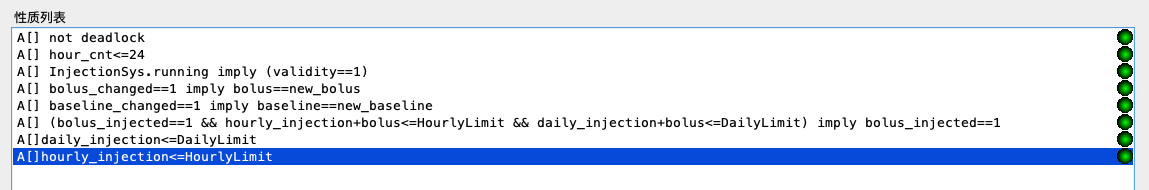


Injection System

Physician Patient

The queries below are validated:



Preliminary requirement was written in TCTL as:

A[] not deadlock

This guarantees that the painkiller injection system would not deadlock under any circumstance.

Requirement 1.1 was written in TCTL as:

A[] (bolus\_injected==1 && hourly\_injection+bolus<=HourlyLimit && daily\_injection+bolus<=DailyLimit) imply bolus\_injected==1

This guarantees that the patient should be able to ask for a bolus by pressing a button

Requirement 2.1 was written in TCTL as:

A[] bolus\_changed==1 imply bolus==new\_bolus

A[] baseline\_changed==1 imply baseline==new\_baseline

This guarantees that the physician should be able to change programmable parameters of the system on his UI. In this case, physician can decide a new baseline or bolus value and change the previous parameters.

Requirement 2.3 was written in TCTL as:

A[] InjectionSys.running imply (validity==1)

This guarantees that the physician should be able to validate one’s identity, proving that one has medical certification by inputting a username and password, the painkiller injection system would not start injection without valid user logging in.

Requirement 3.1 was written in TCTL as:

A[] (bolus\_injected==1 && hourly\_injection+bolus<=HourlyLimit && daily\_injection+bolus<=DailyLimit) imply bolus\_injected==1

This guarantees that the processor should be able to decide whether to give bolus to the patient when button is pressed. In uppaal model, painkiller system does not give bolus unless the injection amount does not surpass limits afterwards.

Requirement 3.2.1 was written in TCTL as:

A[] daily\_injection<=DailyLimit

This guarantees that the painkiller injection system would never injection too many medicine per day. The processor would be able to stop injection when injection amount exceeds daily upper limit.

Requirement 3.2.2 was written in TCTL as:

A[]hourly\_injection<=HourlyLimit

This guarantees that the painkiller injection system would never injection too many medicines per hour. The processor would be able to stop injection when injection amount exceeds hourly upper limit

Extra query was written in TCTL as:

A[] hour\_cnt<=24

This guarantees that the painkiller injection system would clear the clock every day.