Delay Completion phenotype (Zero-order)

**Definition: Action continues beyond latest finishing time**

Scenario: Infusion pump continues infusing beyond the amount of drugs specified. This can be dangerous since an overdose can lead to serious injury or death. This is a ‘Delay Completion’ as the latest time to finish the action of (safe) infusion has passed. Beyond this point, the patient is in a dangerous state.

Forcing function applied: Patching with conditionals.

Property: Dispensing more than three times is a safety violation.

|  |  |
| --- | --- |
| Without Patching | With Patching |
| The user is free to continue manually injecting the patient with drugs forever. At the INFUSE state, as is with any realistic environment, the user can make mistakes and potentially continue to administer drugs past intended capacity.  This violates the safety property that users cannot inject beyond max capacity.  ------------------------------------------------------------------  Safety check  Trace to property violation in DISPENSE:  turn\_on  setting\_rate  set\_rate\_low  confirm\_rate  confirm\_settings  set\_capacity  set\_capacity\_low  dispense\_main\_med\_flow  dispense\_main\_med\_flow  dispense\_main\_med\_flow  dispense\_main\_med\_flow | There are guards set up after the user specifies a rate and capacity. Patch is set up to force user to move out of infusion state after the specified ‘capacity’ is used up.  This satisfies the safety property.  ------------------------------------------------------------------  Safety check  Analysing...  Depth 13 -- States: 24 Transitions: 48 Memory used: 11810K  No deadlocks/errors |

Forcing function

CONFIRM\_PATH = P[Cap],

P[c:0..3] =

(

when(c == 0) **<- Only when the capacity is set to 0 can the user move on to completion**

completion\_state -> P[0]

|

when (c > 0)

dispense\_main\_med\_flow -> P[c - Rat]

).