Safety-Assured Development of the GPCA Infusion Pump Software

BaekGyu Kim, Anaheed Ayoub

Oleg Sokolsky, Insup Lee

Computer and Information Science Dept.

University of Pennsylvania

Paul Jones, Yi Zhang,

Raoul Jetley

OSEL, Center for Devices and Radiological Health

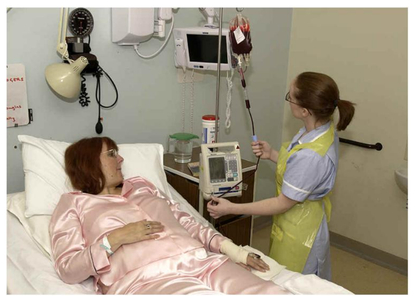
U.S. Food and Drug Administration

Motivation : Safety Issues of Infusion Pump Systems

Infusion Pump

Infusion pumps are medical devices that deliver fluids, including nutrients and medications such as antibiotics, chemotherapy drugs, and pain relievers, into a patient's body in controlled manner.

Example) PCA infusion pump, Insulin pump



Infusion Pump Safety Issues

*Infusion Pump Improvement Initiate, FDA, 2010

FDA has received numerous reports of adverse events associated with the use of infusion pumps, including serious injuries and deaths. From 2005 through 2009, 87 infusion pump recalls were conducted by firms to address identified safety problems.

The Goal : Safety of the PCA Infusion Pump Software

Contribution

1. A case study of Patient-Controlled Analgesic (PCA) infusion pump software that has an immediate practical importance.
2. Identifying challenges encountered applying Model-Based Development approach to the case study.
3. Evaluation of the current version of Generic PCA infusion pump safety requirements and model from the implementation perspective.

Abstracted Safety Model

↓

Implementation

The GPCA Infusion Pump Project

•The GPCA Safety Requirements (FDA)

The GPCA safety requirements were derived from an analysis of hazards encountered in the use of PCA infusion pumps on the market. They serve to establish a minimum degree of safety for these devices.

Example

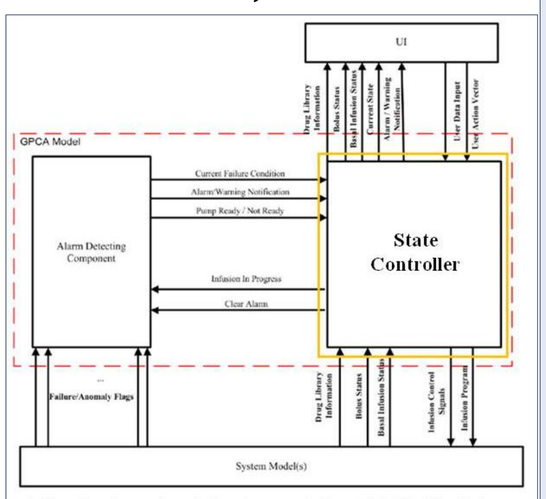
1. No normal bolus doses should be administered when the pump is alarming.
2. If the calculated volume of the reservoir is y ml, and an infusion is in progress, an Empty Reservoir alarm shall be issued.

•The GPCA Model (FDA)

The GPCA model is an abstract representation of common behaviors shared by typical PCA pump software. The model is built using *Mathworks Simulink* and *Stateflow*.

GPCA Model Components

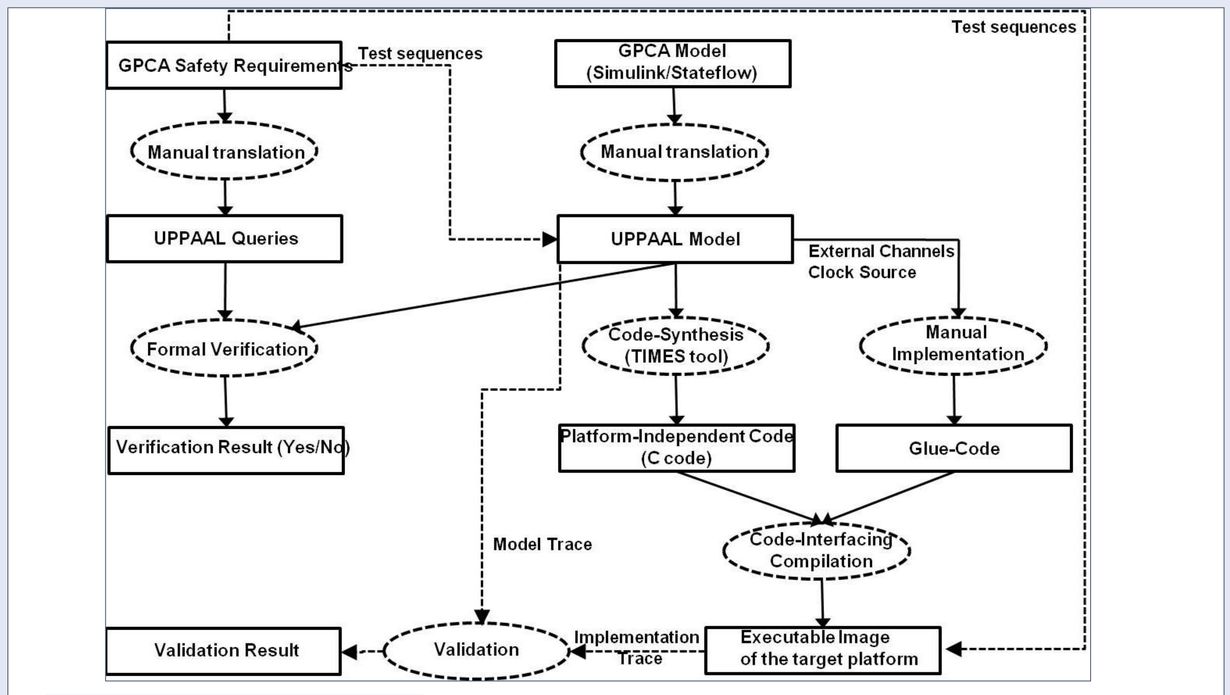
1. **State-Controller**
   - regulate the rest of the pump to fulfill its expected functionality, i.e., administering the right drug to the right patient at a right rate and dosage.
2. **Alarm-Detecting-Component**
   - Check hardware conditions and process alarm on any hardware failure , e.g., ambient temperature, from hardware sensors.



The System Architecture of the GPCA Model

Approach : Model-Based Development

Category	Safety Requirement (SR) / Safety Property(SP)
SR.1.4.3	No normal bolus doses should be administered when the pump is alarming (in an error state).
SP	A[](! (ISSM.BolusRequest && CDR.Alrm-UnknownDrug))
SR 3.4.3	The POST shall take no longer than t seconds.
SP	(POST.Post-In-Progress && x1 > MAX-POST-WAIT) -> POST.Alrm-POSTFailure
SR 1.5.6	If the calculated volume of the reservoir is y ml, and an infusion is in progress, an Empty Reservoir alarm shall be issued.
SP	(ISSM.Infusion-NormalOperation && Cond-6-3 == true) -> (ISSM.Alrm-EmptyReservior)
SR 2.2.4	If the pump is idle for t minutes while programming a dose setting, the pump shall issue an alert to indicate that the user needs to finish programming and start infusion.
SP	(ICR.ChangeDoseRate && x1 > MAX-WAIT-INPUT-T) -> (ICR.Alrm-LongWait-ChangeDoseRate)

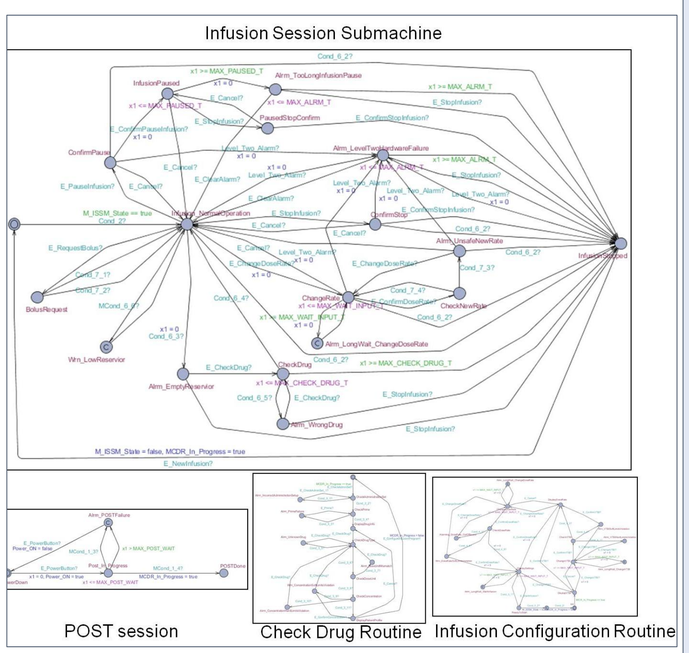


Formal Verification

- **Model Translation**
- **Requirements Translation**
- **Formal Verification**

Automated Implementation

1. **Platform Independent Code**
2. **Glue Code**
3. **Abstracted functionalities**



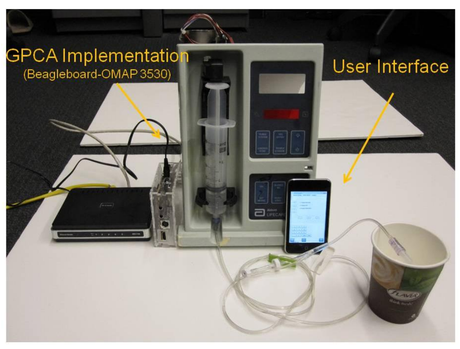
The Categorization of the Safety Requirements

The Categorization of the GPCA Safety Requirements (total 97 requirements)

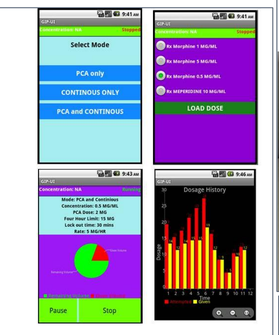
Category 1(20)	Safety requirements that can be formalized and verified in the UPPAAL model.
Example	No normal bolus doses should be administered when the pump is alarming (in an error state).
Category 2(23)	Safety requirements that can be formalized, but the GPCA Simulink/Stateflow model needs additional information to verify them.
Example	If the suspend occurs due to a fault condition, the pump shall be stopped immediately without completing the current pump stroke.
Category 3(31)	Safety requirements that cannot be formalized, but can be validated at the implementation level.
Example	The flow rate for the bolus dose shall be programmable.
Category 4(23)	Safety requirements that cannot be formalized because they address issues related to the ambient environment of the pump or they are vague in description.
Example	Flow discontinuity at low flows (f ml/hr or less) should be minimal.

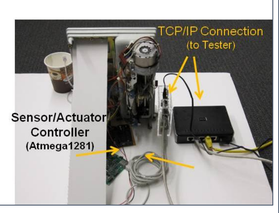
The Testbed for the GPCA Reference Implementation

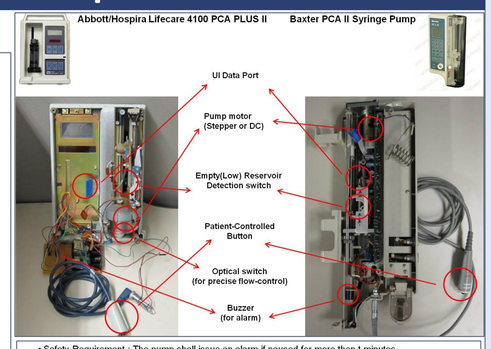
GPCA Infusion Pump Testbed

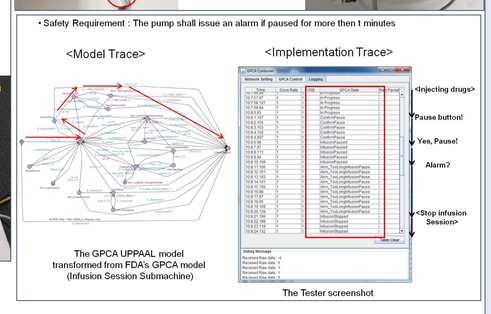


•We note that the Android UI design is motivated from CADD –Solis Ambulatory Infusion System. The functionalities are instantiated from the GPCA model.









Acknowledgement

We would like to thank David Arney for his contribution on the GPCA model and safety requirements. In addition, we also would like to thank Jnana Panuganti for her contribution on the User Interface design of the GPCA Infusion pump.