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,
Raouf Jetley

OSEL, Center for Devices and Radiological Health
U.S. Food and Drug Administration

Motivation : Safety Issues of Infusion Pump Systems

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 a controlled manner. Example: PCA infusion pump, insulin pump.

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\((\text{ISGM BolusFrequency \&\& CDF.Arm-UnknownDrug})\)
SR 1.5.6 If the calculated volume of the reservoir is y ml, and an infusion in progress, an Empty Reservoir alarm shall be issued.
SP F\((\text{ISGM InfusionNormalOperation \&\& Cond 6.5 \rightarrow true \&\& ISGM Arm-EmptyReservoir})\)
SR 2.2.4 If the pump is idle for 3 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 [\text{CIR.ChangeDoseRate \&\& i > MAX (60/IMPRT-FUT-1)} \rightarrow \text{CIR.Arm-Long取出ChangeDoseRate}]

Infusion Pump Improvement Initiate, FDA, 2010

The GPCA Infusion Pump Software

The GPCA Infusion Pump Project

The GPCA Infusion Pump Software

The GPCA Infusion Pump Software

The Categorization of the Safety Requirements

The Testbed for the GPCA Reference Implementation

Acknowledgement

This research is supported in part by NSF CNS-1035715 (CPS: Large: Assuring the Safety, Security and Reliability of Medical Device Cyber Physical Systems) and DGIST Research and Development Program at CPS Global Center.