Dr. Sithu D Sudarsan / Dr. Raoul Jetley, ABB Corporate Research, India, 2014-10-17

Formal Methods for Assurance of Safety Critical Systems: A Case Study

CSI NCFM 2014

Safety Critical Systems
Regulated industry

- Healthcare, Insurance, Finance, …
- Healthcare – safety critical systems
- Regulations – pre-market and post-market

Safety Critical Systems
Regulated industry

- Healthcare, Insurance, Finance, …
- Healthcare – safety critical systems
- Regulations – pre-market and post-market
- Pre-market
  - Provide evidence of safe design
- Post-market
  - Surveillance and follow-up

Safety Critical Systems
Case study – Generic Infusion Pump

- Infusion pump
  - Deliver medication, fluids, nutrients, … to a patient
  - Various types:
    - External/Implanted
    - Therapeutic/Analgesic
  - Is it safety critical?
    - Between 2005-2009: about 56000 adverse event reports including about 500 deaths*

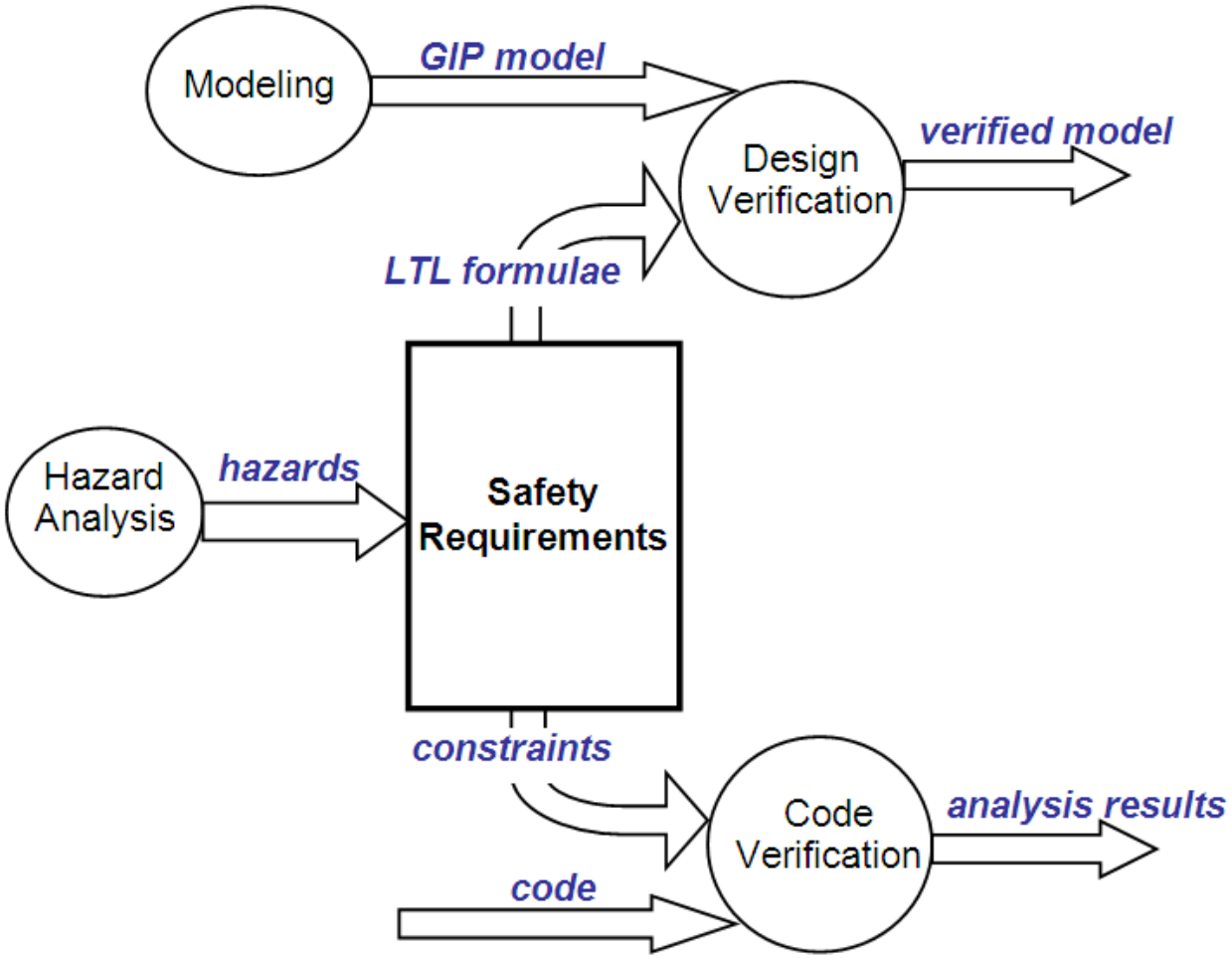
*MAUDE database accessible from: http://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfMAUDE/search.CFM

Generic Infusion Pump
Safety Assurance

- Identify potential hazards
- Identify safety requirements
- Examples:

Hazard	Cause	Mitigation	Pump
Underinfusion	Airlock, Occlusion, Empty reservoir	Maintain minimum pre-defined flow rate	All types
Low Battery	Failure to plug in (user?)	Monitor battery condition and generate alarm appropriately	External

Safety requirements verification
Design / Code



Safety Requirement
Requirements

- **The pump should maintain a minimum Keep Vein Open (KVO) rate of 0.1 ml/hr at all times during infusion. (1)**
- **If the calculated volume of the pump reservoir is 0 ml, and an infusion is in progress, the pump shall issue an 'Empty Reservoir' alarm. (2)**

Safety Requirement
Requirements and LTL

- The pump should maintain a minimum Keep Vein Open (KVO) rate of 0.1 ml/hr at all times during infusion. (1)
- If the calculated volume of the pump reservoir is 0 ml, and an infusion is in progress, the pump shall issue an 'Empty Reservoir' alarm. (2)

AG(pump.active → infusion rate > 0.1) (1)

AG(pump.active ∧ reservoir.empty → X(pump.alarm)) (2)

Safety Requirement
Requirements, LTL and Code Verification

- The pump should maintain a minimum Keep Vein Open (KVO) rate of 0.1 ml/hr at all times during infusion. (1)
- If the calculated volume of the pump reservoir is 0 ml, and an infusion is in progress, the pump shall issue an 'Empty Reservoir' alarm. (2)

$AG(pump.active \rightarrow infusion\ rate > 0.1)$ (1)

$AG(pump.active \wedge reservoir.empty \rightarrow X(pump.alarm))$ (2)

- assert ((pump.mode == INACTIVE) ||
(pump.mode == ACTIVE && infusion rate > 0.1))
- assert ((pump.mode == INACTIVE) ||
(reservoir.volume ! = 0) ||
(emptyReservoirAlarm == true))

Verification of approach

- GUI of a pump (20k C++)
- 16 alarms identified for verification
- Only 10 were triggered by GUI
- 4 were never triggered!
- 2 alarms did not have a corresponding variable!!

Conclusion

- Possible to verify specific safety requirements
  - Using formal methods
  - In an automated manner
    - Of course, after variables in the software are mapped to safety parameters

Reference:

http://www.fda.gov/MedicalDevices/ProductsandMedicalProcedures/GeneralHospitalDevicesandSupplies/InfusionPumps/ucm202511.htm

Power and productivity
for a better world™