Model Based Engineering and Its Integration with Safety Assurance Cases for Medical Device Software

Yi Zhang Ph.D., Paul Jones

Office of Science and Engineering Laboratories
Center for Devices and Radiological Health
Food and Drug Administration

March 25th, 2015

Disclaimer

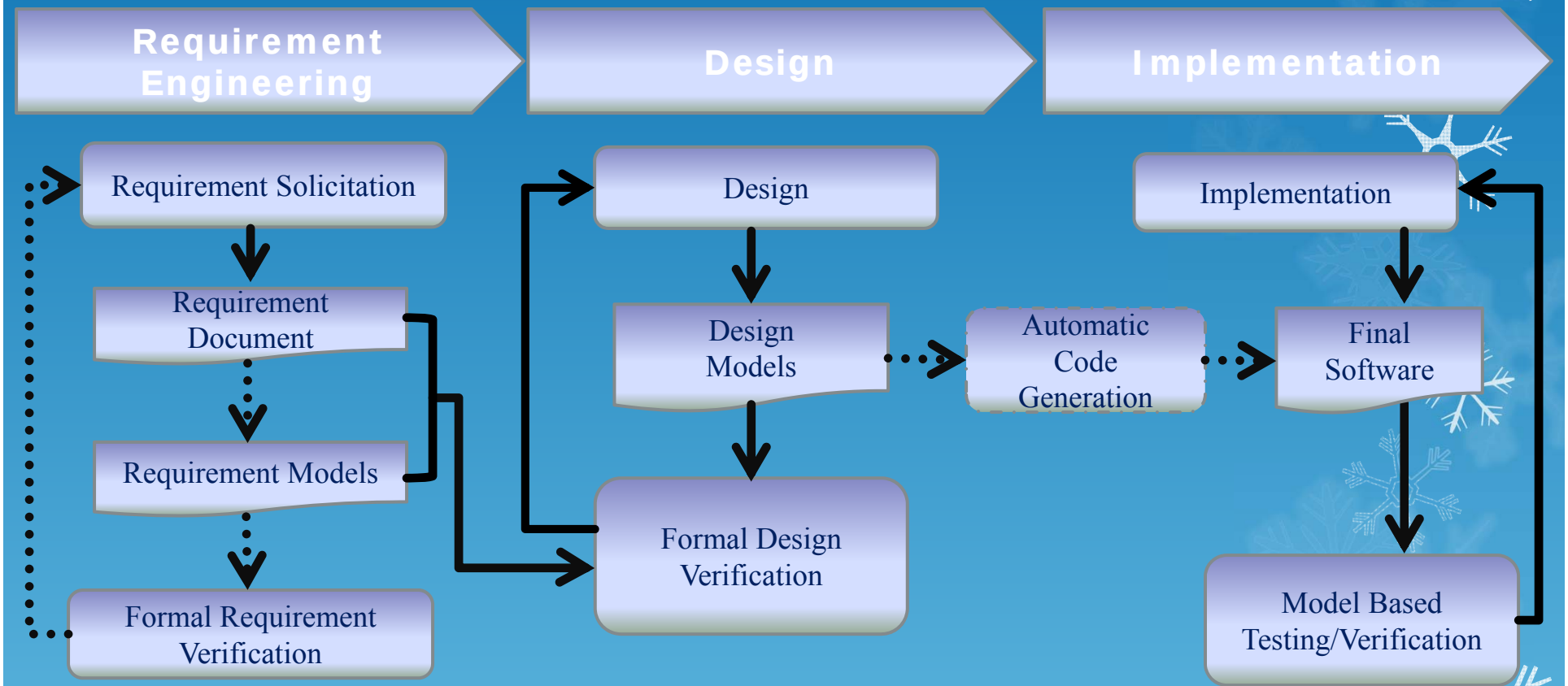
The opinions and information in this presentation are those of the authors, and do not represent the views and/or policies of the U.S. Food and Drug Administration.

Abstract

Model based engineering (MBE) has the potential to help medical device manufacturers detect subtle design flaws at early stages of the development lifecycle, and reduce design/implementation errors in the final device. The rigor of the MBE process and derived artifacts can serve to justify the confidence of stakeholders (e.g. internal, third party, and regulatory) in device safety. In particular, artifacts generated through the MBE process are objective, verifiable, and traceable, and hence can be used as evidence in safety assurance cases to facilitate and ease vested stakeholder assessments of device safety.

A variety of modeling and verification tools are available to implement the MBE process. These tools vary in their semantics, expressiveness, and verification rigor. Thus, developers have to realize the strength and weakness of these tools, and make reasonable choices. Furthermore, when applied to the design of medical devices, the MBE process has to be integrated with the organization's risk management activities (as specified in ISO-14971), to ensure that all foreseeable risks are adequately addressed and mitigated in the final device.

Model Based Engineering (MBE) of Medical Device Software



- Verification results could cause re-iteration of previous development activities
- Trustworthy development artifacts: clearly/unambiguous defined, and demonstrable/verifiable properties
- Explicit and complete traceability among development artifacts

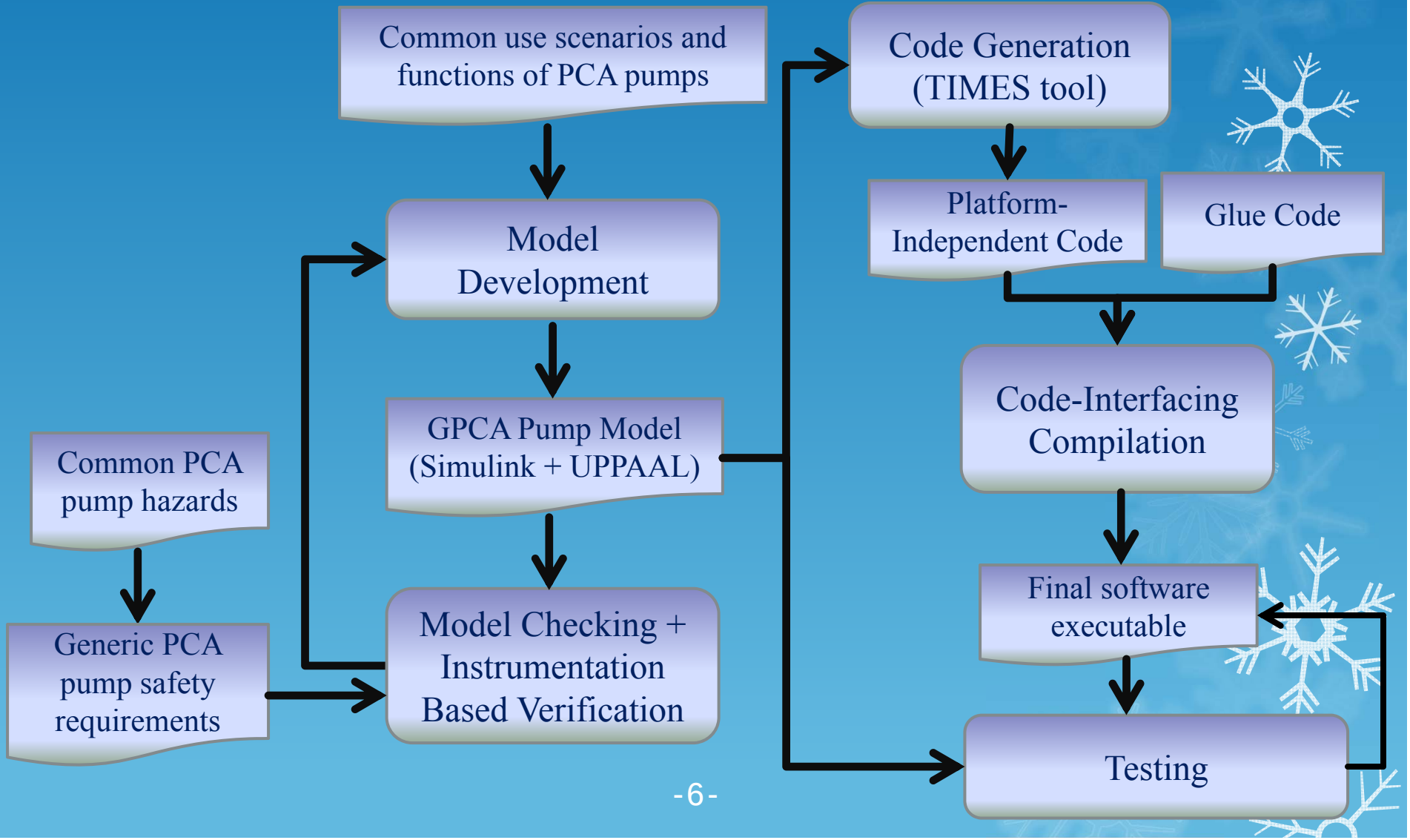
Safety-Driven Development of Medical Device Software

- Safety and effectiveness are two primary properties of interest.
- ISO 14971: Application of risk management to medical devices.
- All foreseeable risks of the device have to be identified and adequately mitigated.
  - Software mitigation measures have to be correctly implemented and tested;
  - Risks caused by software have to be adequately mitigated.
- Risk mitigation measures need to be traceable throughout the development artifacts to the final device.

Generic Infusion Pump Project

- Establish safety-driven MBE methods for generic infusion pump software safety model.
  - Developed a set of generic infusion pump safety reference models that can be used as a reference standard to verify safety properties in difference classes of infusion pumps.
- Joint effort between FDA and several universities
  - GIP web site (http://rtg.cis.upenn.edu/gip.php3): a repository of software development artifacts for infusion pump software
  - Open contribution for community (manufacturers & academics) to advance the science and practice of developing high-confidence medical device software.

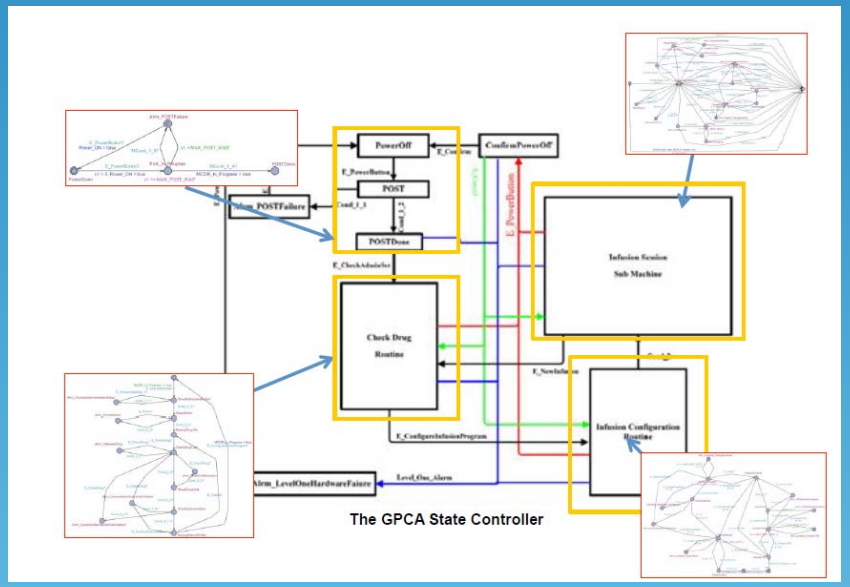
Safety-Driven MBE of Generic Patient Controlled Analgesic Pump (GPCA) Model



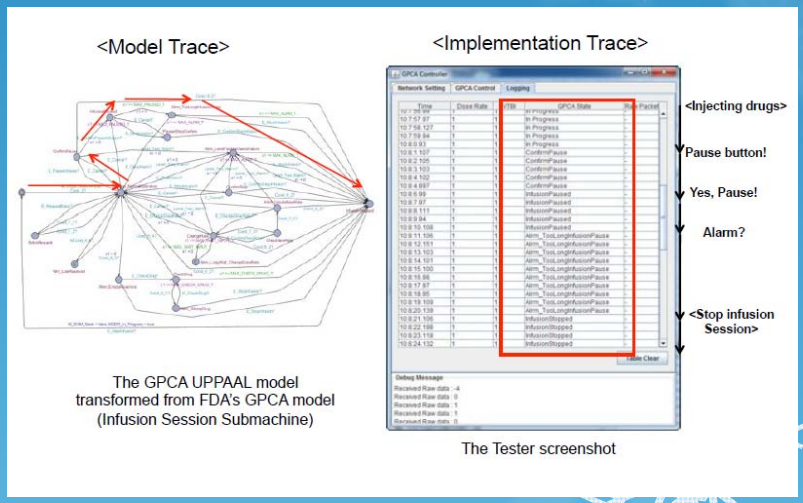
GPCA Pump Development Artifacts

HID	Hazard	Pump Type	Cause	Action	Mitigated by	Safety Requirement
1.1	Overinfusion	All	Programmed flow rate too high	Alarm(); Log()	Drug library	1.1, 1.4.4, 1.4.11
1.2	Overinfusion	All	Dose limit exceeded due to too many bolus requests	Alarm(); Log()	Flow sensor	1.4, 3.4.6
1.3	Overinfusion	All	(Programmed) Bolus volume/concentration too high	Alarm(); Log()	Drug library	1.4, 3.4.6
1.4	Overinfusion/	All	Incorrect drug concentration	Alarm(); Log()	Barcode scanner	1.1, 6.1.3, 6.1.4

Hazards + Generic Safety Requirements



GPCA Model + Verification Results (Simulink/Stateflow + UPPAAL)



Deployable code + Test cases and results

Lessons Learned

- Fidelity of design model is bounded by assumptions

  e.g. use scenarios, user inputs, environment, etc.

- There is gap between design models and final implementation of the device

  e.g. computational platform, operational systems

- Various verification techniques can be used to ensure the correctness and safety of design models
  - Expert review → Testing/Simulation/Instrumentation based verification → Formal verification (i.e., model checking)

    Increasing order of rigor vs. increasing order of cost
  - Not all safety/functional requirements can be formally verified

* Details can be found in *Safety-Assured Development of the GPCA Infusion Pump Software,* B. Kim and et al., in proceedings of *the 11th International Conference on Embedded Software (EMSOFT 2011)*, pages 155-164, October 2011.

MBE and Safety Assurance Cases

- Safety Assurance Case: structured argument about "device" safety
  - Claim: Device is safe (ISO 14971: free from unacceptable risk)
  - Argument: Rationale & appeal to evidence justifying the claim
  - Evidence: objective, verifiable, traceable
- Benefits of using MBE artifacts in Assurance Cases
  - Using MBE processes as arguments & artifacts as evidence can improve the quality and trustworthiness of the claim (i.e. device is safe)
    - Models support mathematical & computational rigor
    - Verification results of models are objective &/measurable
  - Explicit traceability among MBE artifacts helps justify design & development integrity

Safety Assurance Case with MBE Artifacts

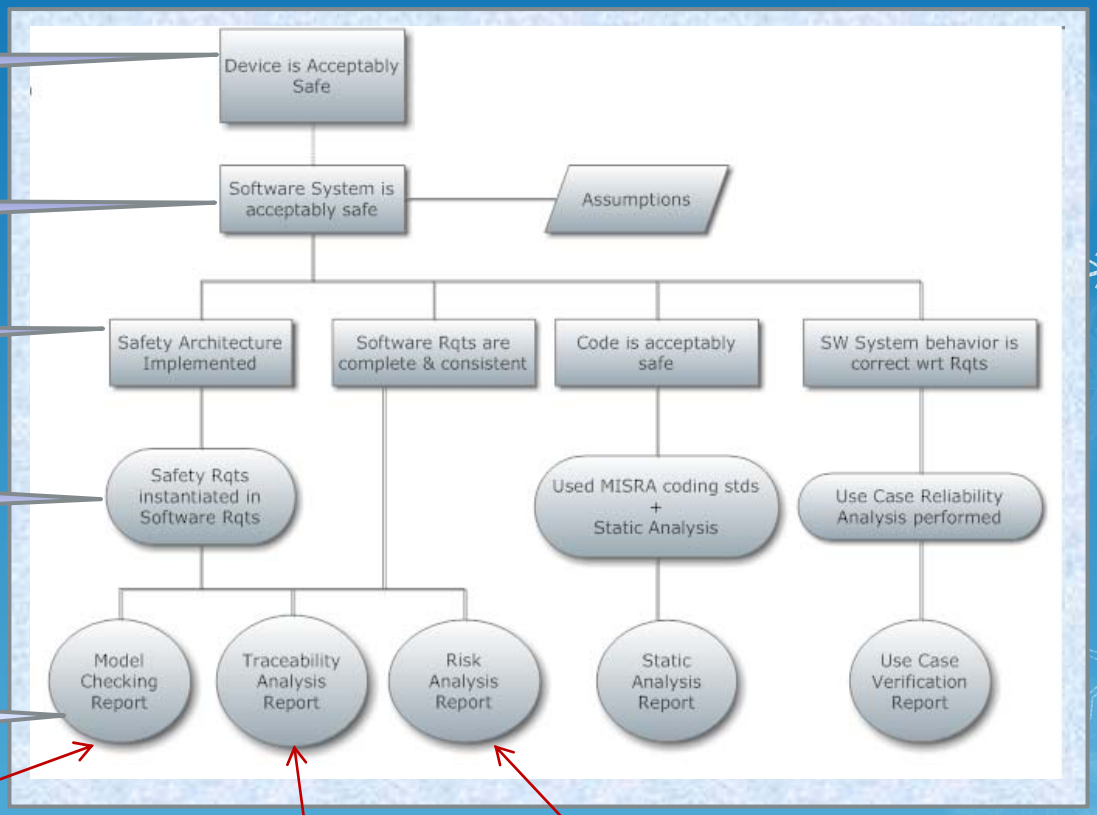
Claims

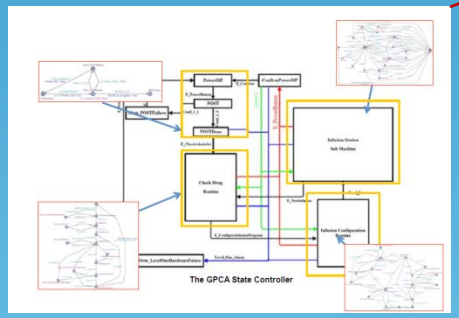
Claims

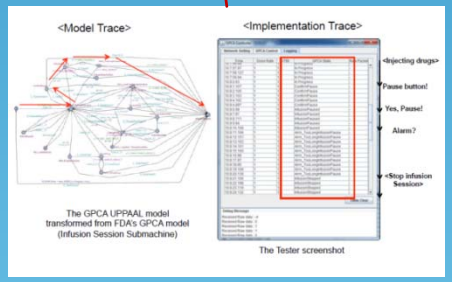
Claims

Arguments

Evidence







HID	Hazard	Pump Type	Cause	Action	Mitigated by	Safety Requirement
1.1	Overinfusion	All	Programmed flow rate too high	Alarm(); Log()	Drug library	1.1, 1.4.4, 1.4.11
1.2	Overinfusion	All	Dose limit exceeded due to too many bolus requests	Alarm(); Log()	Flow sensor	1.4, 3.4.6
1.3	Overinfusion	All	(Programmed) Bolus volume/concentration too high	Alarm(); Log()	Drug library	1.4, 3.4.6
1.4	Overinfusion	All	Incorrect drug concentration	Alarm(); Log()	Barcode scanner	1.1, 6.1.3, 6.1.4

Questions?