Assurance Cases for Medical Devices
PRECISE Center
Department of Computer and Information Science, University of Pennsylvania
Anaheed Ayoub, Oleg Sokolsky, Insup Lee

The assurance of safety-critical systems is of a great concern. Many such systems are approved by regulatory agencies. For example, medical devices sold in the United States are regulated by the U.S. Food and Drug Administration (FDA). Which means that manufacturers of such systems are expected not only to achieve acceptable assurance level but also to convince regulators that it has been achieved.

Assurance and Safety Cases

Recently, assurance cases have become popular and acceptable ways for communicating information about safety-critical systems among the stakeholders. An assurance case, addressing safety, is called a safety case. A safety case is a structured argument, supported by a body of evidence, that provides a compelling, comprehensible and valid case that a system is safe for a given application in a given environment.

Ongoing Work

Our ongoing work is constructing a safety case (safety argument & confidence arguments) for the Patient Controlled Analgesia (PCA) infusion pump system that we are developing.

Beyond the Case Study

+ Reusing the argument: define a safety case pattern for model-based development.
+ Evaluating the safety argument: where are the gaps?
+ Reviewing the safety argument: questioning about the overall sufficiency of the safety argument.

A Safety Case Pattern for Model-Based Development

1. Identify common characteristics of concepts that require confidence argument
2. Summarize relationship between the concepts in a map
3. Systematically construct confidence arguments
   1. Instantiate the map
   2. Generate the confidence argument

Identify safety gaps (assurance deficits)

The Common Characteristics Map

The map Instance for C1.1.1 context

Part of C1.1.1 Confidence Argument

The Pattern Instance for the PCA Safety Case

Context | Goal
---|---

Strategy

- Modeling the system
- Verifying the model
- Transformation the model into an implementation
- Validating the implementation

Evidence

Evidence

Sub-Goal | Sub-Goal
---|---

Goal

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence

Evidence