Assurance Cases for External Infusion Pumps Update

Richard Chapman
FDA
July 20, 2012
UMSEC Summer Software Symposium
The Problem

• In 2005-2006, FDA formed a working group to develop recommendations to reduce the number and severity of infusion pump recalls. The efforts of this group culminated with the Infusion Pump Improvement Initiative of April 2010.

• The improvement initiative included a guidance document, which increases the premarket review requirements for pumps as a measure to improve safety of these devices.
• www.fda.gov/infusionpumps
External Infusion Pump Guidance

• The new infusion pump guidance steers manufacturers to the top level safety claims based on a comprehensive analysis of the hazards associated with the use of infusion pumps.

• The guidance does this by recommending the use of ASSURANCE CASES to organize the content of 510(k) premarket submissions.
External Infusion Pump Guidance

• Draft guidance published in Federal Register April 2010.
  
  New draft Special Controls Guidance in May 2011…?

• New draft Special Controls Guidance in 2012
  – Incorporates lessons learned and industry comments
510(K) AND SCIENCE REPORT

RECOMMENDATIONS:

- **Original:** CDRH should adopt an assurance case framework for 510(k) submissions.
- **Modified:** We plan to implement an assurance case pilot program for infusion pumps, conduct an assessment of the pilot, and then seek public input before determining next steps to assure that we proceed in a way that addresses the concerns raised in public comments.
Safety Assurance Framework

• A process for distilling the REASONS for product integrity from the totality of activities and resources employed to realize it.

• … and for making an argument as to why the evidence, your test data and analyses, supports the claims.
What is a Safety Case?

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.

- This type of assurance case contains a structured argument (rationale) demonstrating that the evidence it contains is sufficient to show that the system is safe.
- The argument is commensurate with the potential risk and the system’s complexity.
Reasoning

• Legal system
  – Risk based
    • Reasonable suspicion – temporary loss of liberty
    • Probable cause – arrest
    • Beyond a reasonable doubt – Loss of life or liberty
    • Civil court – preponderance of evidence – loss of money

• Scientific Method
  – Hypothesis
  – Experiments, methods, to test the hypothesis
  – Statistical measures of the reliability of data
  – Discussion and conclusions
Where did this all come from?

- Stephen Toulmin a professor of philosophy and mathematics at Oxford in 1949 wanted to examine the mathematical formalisms of argument and certainty.
- Wrote several books which did not sell!
- But which, surprisingly, are used today as teaching aids to litigators, safety professionals, regulators, scientists, and intelligence communities.
How does this relate to FDA premarket processes

- A 510(k) is mostly a checklist
- FDA asserts that we know what we want
- Sponsor just follows the checklist
- Once upon a time a checklist was a way to assure coverage and completion and equitable application
- As systems become more complex this becomes less true
So what do premarket technical regulators really look for?

What the design trade-offs actually were:

• Are they safe?
• Who made them and stands by them?
• Why they were made this way?
• How they were verified as the right ones?
• Can they be reeled back if something goes wrong later?
• Are they at or near the currently accepted state of the art?
• Can manufacturing realize the product once approved with the same trade-offs?
• Will they persist in continued use?
• With increased functional complexity comes increased diversity of solutions. With increased diversity of solutions comes diverse implementations and our equitable review begins to become harder

• We soon don’t know what to ask for, so we rely on additional information requests to satisfy coverage, but this consumes time so we begin to take a risk management approach
A safety case is the best way to both document and review a submittal based on a risk management approach because the argument shows the proportionality of the mitigation.
Safety Engineering

The assurance case is a method for reasoning about systems appropriate for scientists and engineers.
Safety Engineering

• Safety Case
  – Claims
    • Top Level Claim – Infusion pump is reasonably safe and effective for its intended use.
      – Users
      – Environment
  – Evidence
  – Arguments
Hazard Analysis

• Hazard Analysis
  – ISO 14971 – Application of Risk Management to Medical Devices
Hazard Analysis

• Start with the hazards and hazardous situations
• The claim is that you have mitigated the hazard or the hazardous situation.
• Determine the properties of the system that will make it safe.
• Generate safety requirements
Evidence

- Lack of clear definition of evidence and how to evaluate it.
  - Guidance Documents, Standards
  - Checklist
    - Presence versus quality
  - Domain Experts
- Evidence is:
  - Test data
  - Results from experiments
  - Historical performance
  - Compliance with standards
  - Analysis
  - Scientific and engineering information from the literature
Suitability of Evidence

Assurance (of a Requirement for Evidence) The degree of confidence that the set of safety evidence satisfies the requirement for evidence.

- **Relevance** - The extent to which an item of evidence entails the requirement for evidence
- **Trustworthiness** - The perceived ability to rely on the character, ability, strength or truth of the evidence
- **Independence** - The extent to which complementary items of evidence follow diverse approaches in fulfilling the requirement for evidence
Suitability of Evidence

**Relevance** - The extent to which an item of evidence entails the requirement for evidence

- **Directness** - The extent to which an item of evidence directly fulfils the requirement for evidence
  - Direct – e.g., timing data
  - Indirect – e.g., competence of personnel

- **Coverage** - The proportion of the requirement for evidence which the evidence addresses
  - Thorough – e.g., a technique which provides evidence of the handling of all runtime exceptions
  - Less thorough – e.g., a technique which provides evidence of the handling of divide by zero
Suitability of Evidence

**Trustworthiness** - The perceived ability to rely on the character, ability, strength or truth of the evidence

- The trustworthiness of evidence is an expression of the *process evidence* related to generating the evidence. These factors include, but are not limited to:
  - “Buggy-ness” – how many “faults” there are in the evidence presented;
  - Level of review;
  - For tool-derived evidence: Tool Qualification and Assurance;
  - Experience and Competence of the personnel.
Suitability of Evidence

**Independence** - The extent to which complementary items of evidence follow diverse approaches in fulfilling the requirement for evidence

- Independent - Manual code inspection and static analysis are independent methods to eliminate software defects
- Not Independent - Human factors testing by software developers is the fox watching the hen-house
Argumentation

The action or operation of inferring a conclusion from propositions premised.

• **Premise** - A previous statement or proposition from which another is inferred or follows as a conclusion
Argumentation

• **Conclusion** - A judgment or statement arrived at by any reasoning process
  – Deductive - If premises are true, then the conclusion must also be true
  – Inductive - The conclusion follows from the premises not with necessity but only with probability
  – Abductive - Inference to the best explanation
  – Argument by Analogy

– Beware of logical fallacies
  • Argument by analogy
  • Drawing the wrong conclusion
  • Omission of key data
  • Etc.
Argumentation

• The strongest arguments are both valid and sound
  – **Valid** - If premises are true, conclusion is true
  – **Sound** - Argument which is valid and has true premises

• Weaker Argument
  – **Consistent** - If premises are true, conclusion may be true. True with some probability.
What is a Safety Argument

• This infusion pump is **safe because**
  – The safety requirements are **defined in my**
    • Safety requirements analysis, derived requirements …
    • Legislation, policy …

• The safety requirements are **met through our**
  – Safety analysis of design, use …
  – Hazard management through problem reporting
  – Observing failures are at a ‘safe’ level
  – Appropriate quantity, quality and rigor of evidence

• Safety management continues to be **adequate because we have**
  – SMS
  – staff competence
  – ongoing independent scrutiny …
4-Part Harmony

• a statement of what was provided
• why the information provided is not sufficient
• what additional information is needed
• why the requested additional information is needed to answer a regulatory or scientific question
Argue the point

- There should be an argument at each sub-goal of the safety case.
- Convince us at each sub-goal that we should not have to look any further down into your safety case.
- Summarize what is below, emergent properties, highlights
Format

• Narrative
• Tabular
• Graphical

• All are acceptable formats
• Tools
  – Adelard – ASCE
  – Will implement others that manufacturers choose to use
Graphical representation

Some Top level claim

Body of evidence [Results of analysis]

An argument about why this evidence is persuasive

Body of evidence [test results]

Another argument about why this other evidence is persuasive

Some other subsidiary claim

Body of evidence [test results]
Safety Case Reports

• The Safety Case
  – A complex body of interdependent and evolving documentation
  – Created and managed by the manufacturer
  – Not easily auditable or reviewable

• Safety Case Reports
  – A ‘snapshot’ of the rationale and content of a safety case at an appropriate milestone
  – Shows that any arbitrary set of requirements has been met
Safety Case Reports

- Safety Case Reports (continued)
  - Reviewable against the project expectation at the milestone
  - May need several report types for various stakeholders
  - May need several updates over time
Implications for manufacturers

• The Safety Case will evolve over the life of the system

• While the structure of the Safety Case will broadly remain constant,
  – the status of the evidence will change, e.g., planned test coverage will be replaced by evidence of test results
  – the relative weight of the arguments may change, e.g., compliance with a process standard might be replaced by proven in use

• Therefore plan for multiple reports
  – Obtain agreement on the argument structure first
  – Use identification of evidence as management tool
Examples

  - Infusion pump specific
• A New Approach to creating Clear Safety Arguments

*Richard Hawkins, Tim Kelly, John Knight and Patrick Graydon*

Current Work

• MCM syringes, needles, catheters
• Insulin pump
• Analysis of safety cases to see what worked and what didn’t
• Application to other medical device types
Thank You!

End
What I forgot

Reviewers
Static analysis
Problems
  Final finished product
  Arbitrary specifications
Software anomalies
OSEL software

- Interoperability
- Static Analysis (binaries)
- Super Computer
- Modeling
- Assurance Cases
- Generic Infusion Pump
- Model-Based Development
- FDA Search