Goal-Based Certification for Medical Devices

John Rushby

Computer Science Laboratory
SRI International
333 Ravenswood Avenue
Menlo Park, CA 94025 USA

rushby@csl.sri.com, phone +1 650 859-5456, fax +1 650 859-2844

Abstract. Certification for medical devices should be undertaken in a goal-based, rather than a prescriptive, manner. This approach will best support the rapid pace of innovation in medical devices. Some research topics in goal-based certification for medical devices are proposed.

1 Introduction

As software-controlled medical devices become more complex, ubiquitous, intrusive—and beneficial—they stress existing certification processes for pre-market approval and 510(k) exemptions based on pre-market equivalence. Current guidelines for software validation in medical devices [1,2] provide little discussion of networked and distributed systems, do not anticipate modern methods of software development such as model-based design and, apart from testing, do not cover systematic methods of analysis such as static analysis or model checking, nor hazard avoidance methods such as runtime verification. I suggest it is prudent to consider how such topics should be incorporated into regulatory guidance, and how the regulatory process can be adjusted to remain abreast of future developments in this rapidly changing field.

2 Goal-Based Certification

The traditional, *prescriptive*, approach for assuring the safety of complex systems is based on standards and regulations that enshrine accepted practice. This approach works well for classes of systems where there is extensive experience to support the efficacy of the practice, and where there is relatively little innovation, so that one system in the class is very much like another. Software for commercial aircraft is a typical example—though even here the recommendations have progressed from DO-178A [3] to the current DO-178B [4] and on to DO-178C, which is in development: the progression reflects technological change in methods for software development and assurance, and in the context of its use within aircraft (most notably fly-by-wire).

Medical devices are far more varied than aircraft, many more of them are developed, and the pace of technological change is much higher. While suitable regulatory guidance can establish a floor that eliminates the most egregious systems, it will be difficult for a standards-based approach to ensure safety at reasonable cost and without stifling innovation in such a rapidly developing area. Similar pressures in other fields that are faced with rapid technological change have led to increasing interest in *goal-based* approaches to safety assurance.

In a goal-based approach, the developer provides *claims* concerning safety-relevant attributes of the system (e.g., "this radiation therapy machine will never deliver a harmful dose," or "this system will deliver the specified service at least 999 times in 1,000 demands") together with an *argument* justifying those claims that rests on verifiable *evidence*. The claims, argument, and evidence are collectively referred to as a *safety case*. The suitability of the claims to a particular application may be determined by the customer, by regulation, or by the safety argument for a higher-level system. The efficacy of the argument and the evidence to sustain the claims will usually be evaluated by an independent organization, which may be a government regulator or a commercial or nonprofit entity specializing in this business.

In a goal-based approach, developers (in coordination with their evaluators and regulators) are free to work out the most effective safety case for their particular system, and are thereby able to respond appropriately to novel hazards introduced by new applications or new system integrations, while being able to take advantage of new methods for reducing hazards and improved methods for analyzing software. Developers do not have complete freedom in developing safety cases: each application domain generally provides regulations or guidelines covering the general shape of acceptable safety cases. An example is the UK Defence Standard 00-56 [5], which establishes a framework for goal-based regulation, together with supporting guidelines [6].

3 Research Agenda for Medical Device Certification

I propose a community-wide exploration of topics in goal-based methods for certification of medical devices, leading to recommended approaches and suggested guidelines that can attract wide support.

Safety cases and goal-based certification are emerging topics for academic study. Many of the issues are largely generic across application domains (e.g., hazard analysis and mitigation, risk assessment, computer security, classical software analysis and testing), so that advances in methods of analysis and design, and in architectural methods of risk reduction (e.g., availability of safety- and security-certified RTOSs) developed in one domain can be imported into the safety cases of another. The field of medical devices will be better positioned to benefit from these advances if it is an active participant in the general topic area. I therefore propose investigation of the methods and technologies for goal-based approaches to certification used in other fields, and research in their application to medical devices.

There are some issues that arise in many application areas but are particularly acute in medical devices. These include ad-hoc integration of many systems (e.g., the large numbers of devices used in hospitals) and of many kinds of systems (e.g., devices, decision support, and information management), creating excellent opportunities for unintended emergent effects, and the role of human factors (cf. [7] where poor human factors facilitate rather than reduce medication errors). Active participation by the medical device community in the topic of goal-based certification (e.g., by providing case studies) may encourage researchers from related fields to apply their expertise to these challenging problems—to the benefit of all. More proactively, I propose research in a *systems approach* to automation in medicine that will focus on issues such as compositional methods for assurance and certification. Compositional techniques in computer science focus on interactions among computational systems, whereas systems-level compositional methods must also consider interactions through the plants that the computational systems control and the environment in which they are embedded (for example, a failure in one device may trigger reactions in the body that were not anticipated by the designers of another device, causing it to exhibit some inappropriate behavior and thereby compound the problem).

There are, of course, some issues that are very special to medical devices, most obviously interaction with the human body. Different devices interact with the human body across different "dimensions," ranging from the pharmacological (e.g., insulin infusion pumps) through the electro-neurological (e.g., pacemakers and defibrillators) and the mechanical (e.g., assistive robots) to the cognitive (e.g., brain implants). In most cases, the software controlling the device operates with respect to some model of the human system concerned. These models are approximate and almost certainly inexact for any particular patient at any particular time. So an interesting topic of research is the extent to which "safe" behavior can be assured by imprecise models. The models concerned are likely to be hybrid systems, so the technical topic becomes one of assuredly safe approximations in hybrid systems (cf. the methods of Tiwari [8])—extended in light of the previous paragraph to assuredly safe compositions of such approximations.

I believe that the research areas suggested above, undertaken in support of a move to goal-based methods of assurance and certification for medical devices, will provide both exciting intellectual challenges and a framework for safe deployment of rapidly evolving and innovative medical devices.

References

[1] Office of Device Evaluation, Center for Devices and Radiological Health, Food and Drug Administration: Guidance for the Content of Premarket Submissions for Software Contained in Medical Devices. (1998) Available at `http://www.fda.gov/cdrh/ode/software.pdf`.

[2] Center for Biologics Evaluation and Research, Center for Devices and Radiological Health, Food and Drug Administration: General Principles of Software Validation; Final Guidance for Industry and FDA Staff. (2002) Available at `http://www.fda.gov/cdrh/comp/guidance/938.pdf`.

[3] Radio Technical Commission for Aeronautics Washington, DC: DO-178A: Software Considerations in Airborne Systems and Equipment Certification. (1985)

[4] Requirements and Technical Concepts for Aviation Washington, DC: DO-178B: Software Considerations in Airborne Systems and Equipment Certification. (1992) This document is known as EUROCAE ED-12B in Europe.

[5] UK Ministry of Defence: Interim Defence Standard 00-56, Issue 3: Safety Management Requirements for Defence Systems. Part 1: Requiremnents. (2004) Available at http://www.dstan.mod.uk/data/00/056/01000300.pdf.

[6] UK Ministry of Defence: Interim Defence Standard 00-56, Issue 3: Safety Management Requirements for Defence Systems. Part 2: Guidance on Establishing a Means of Complying with Part 1. (2004) Available at http://www.dstan.mod.uk/data/00/056/02000300.pdf.

[7] Koppel, R., Metlay, J.P., Cohen, A., Abaluck, B., Localio, A.R., Kimmel, S.E., Strom, B.L.: Role of computerized physician order entry systems in facilitating medication errors. Journal of the American Medical Association **293** (2005) 1197–1203

[8] Tiwari, A.: Abstractions for Hybrid Systems, Computer Science Laboratory, SRI International, Menlo Park, CA. (2004) Combines several conference papers: available at http://www.csl.sri.com/~tiwari/new.pdf.