Assurance Cases: A New Form of Requirements Traceability Matrix for Medical Devices

Fritz Eubanks, Ph.D. and Melissa Masters
Advanced Engineering for Life Sciences
Battelle Memorial Institute
505 King Ave.
Columbus, OH 43201

Abstract. Scientific and medical innovations have led to great improvements and advancements in the lives of people around the world. As technology has progressed so has the complexity of the medical devices that have been created. Not only has the technical complexity increased but additionally, the user interaction with the device has also become more complex and involved. Both of these intricacies have been identified as complicating factors in the safe and effective use of infusion pumps. To this end, the FDA identified an initiative in April of 2010 to address these concerns. One outcome that was identified is the requirement to perform an assurance case. This requirement presents several challenges to practicing medical systems engineers to ensure the assurance case report is complete and assures the device is arguably wholly safe and effective.

Introduction

Infusion pumps are medical devices that deliver nutrients and medications into patient's bodies. These devices are used throughout the world in the home, nursing facilities, hospitals etc. So there are a wide variety of users in very diverse environments that could be interfacing with these devices. Manufacturers must design a safe and effective device from both a hardware and software perspective, but it is expected by various regulatory bodies that they also need to understand how the device will be used, what the environment is like, what are the cognitive abilities of the operators etc. and then ensure the device is safe and effective for its intended use in its intended environment with its intended operators. Infusion pumps that are not operated correctly, or that fail could lead to the death or serious injury of a patient. So making certain that the device is both safe and effective is an enormous undertaking..

Over the past several years, there have been numerous incidents that have been reported to the FDA and in various news outlets. "From 2005 through 2009, FDA received approximately 56,000 reports of adverse events associated with the use of infusion pump, including numerous injuries and deaths. During this time period, 87 infusion pump recalls were designated as Class II, a category that applies when the use of the recalled device may cause temporary or medically reversible adverse health consequences, or when the use of the recalled device may cause temporary or medically reversible adverse health consequences, or when the probability

of serious adverse health consequences is remote. 14 recalls were Class I – situations in which there is a reasonable probability that use of the recalled device will cause serious adverse health consequences or death. These adverse event reports and device recalls have not been isolated to a specific manufacturer, type of infusion pump, or use environment; rather, they have occurred across the board." FDA [2010a]

The FDA began an initiative in April of 2010 to improve infusion pumps. The initiative will:

"1. Establish additional requirements for infusion pump manufacturers;
2. Proactively facilitate device improvements; and
3. Increase user awareness." FDA. [2010a]

One of the identified requirements was the conduct of an assurance case. An assurance case is a "formal method for demonstrating the validity of a claim by providing a convincing argument together with supporting evidence. It is a way to structure arguments to help ensure that top-level claims are credible and supported." FDA [2010b] This process and methodology has been implemented in legal arguments and also in other safety-critical systems such as nuclear reactors and avionics, but this is not a typical method implemented in medical device development processes to date. It should also be noted that the FDA is considering requiring assurance case analyses for all life-supporting devices in the future.

Background

Bishop [1998] presented the basic safety case methodology that had been developed through defense programs in the United Kingdom. It is based on Goal Structuring Notation (GSN), which parallels Toulmin's [1958] model of argumentation. He defined the main elements of the safety case as follows:

- *Claim* about a property of the system or some subsystem.
- *Evidence* which is used as the basis of the safety argument. This can be either *facts*, (e.g. based on established scientific principles and prior research), *assumptions*, or *subclaims*, derived from a lower-level sub-argument.
- *Argument* linking the evidence to the claim, which can be deterministic, probabilistic or qualitative.

It is important to note that evidence, in a regulatory environment, consists of objective facts provided by verification and/or validation testing. Under this definition, assumptions and sub-claims would not be considered evidence.

Kelly [1998] provided additional detail on the background and logic behind GSN, and addresses methods for the maintenance, reuse and evaluation of safety cases. His element terminology differs from Bishop by replacing claim, evidence and argument with goal, solution and strategy, respectively. He also adds elements as follows:

- Justification: used to provide rationale for a strategy
- Assumption: explanations or references generally associated with a goal or strategy

He points out that experience had identified the following key problems being faced regarding safety case maintenance:

- Difficulty in recognizing change
- Difficulty in identifying the indirect impact of change
- Insufficient information recorded to support the change process
- Lack of a systematic process

He went on to employ AI-based computational methods such as hierarchical propagation and pattern recognition. It should be noted that safety case pattern recognition required extending GSN relationship definitions to support structural abstraction of the safety case diagram in a computational environment.

Weinstock [2004] of the Carnegie Mellon (CMU) Software Engineering Institute (SEI) issued technical note CMU/SEI-2004-TN-016 that presented dependability cases, a type of assurance case, as a means for assessing software dependability, where dependability is defined as "the trustworthiness of a computer system such that reliance can justifiably be placed on the service it delivers. The authors also cite the following issues associated with dependability cases, and by inference, assurance cases:

- Completeness
- Bulkiness
- Expense

In 2009, the CMU SEI issued a technical note CMU/SEI-2009-TN-018 [Weinstock, 2009] that explored the use of assurance cases for justifying claims of medical device safety, illustrating the use of the assurance case on a particular type of medical device—the generic infusion pump (GIP). In the introduction to CMU/SEI-2009-TN-018, the author's state:

> "The SEI began talking with the FDA on the subject of assurance cases in 2005-2006. By late 2006, Advamed, an advocacy group for the medical device industry, became interested in the subject and invited us to talk to them in early 2007."

Later in the document, the authors make the statement that:

> "Typically, safety requirements arise from an understanding of hazards that need to be addressed; each safety requirement, if satisfied, mitigates one or more hazards. But if the case just addresses safety *requirements*, the link to the hazards mitigated by the requirement can be lost; it can become difficult to decide if the requirement is adequate to address the underlying hazard(s)." [Weinstock, 2009]

This assertion is arguable, since a properly constructed traceability matrix would show a requirement's origin as a risk control, marketing requirement, user need, etc.

The authors present the following major challenges to the adoption of assurance cases by the device industry and the FDA:

- A process definition that includes
  - How much evidence is enough
  - How the evidence is used
  - Evidence ownership (may contain trade secrets)
  - How to submit both the assurance case and the evidence supporting it
- Fair evaluation of submissions by manufacturers that use assurance cases vs. those that do not
  - Forced adoption may create industry backlash

From Traceability Matrix to Assurance Case

The traceability matrix is a standard method for demonstrating that a device design fulfills its stated requirements. [Robertson, 1999] The safety traceability matrix consists of direct links between safety risk controls, product requirements and test results proving successful implementation of the risk controls. [Eubanks, 2010] Battelle uses the IBM Rational DOORS requirements management system to maintain the traceability links, thus automating the generation of the traceability matrix. A fragment from a typical DOORS traceability matrix for an electromechanical drug delivery system showing the risk controls for electrical shock appears in Table 1.

Table 1: Safety Traceability Matrix – Electrical Shock

Hazard	Cause	Required Risk Control	In-links at depth 1	In-links at depth 2	In-links at depth 3
1 Electrical Shock	1.1 User contacts live parts during operation	1.1.1 D: Design IAW IEC 60601-1; Clause 5.9.2 [HA9]	PR26 The design and operation of the device shall conform to the requirements of IEC 60601-1, Clause 5.9.2.	PVTP50 Verify device conforms to the requirements of IEC 60601-1, Clause 5.9.2.	PVTR22 IEC 60601-1 Compliance Test Report #TR6605-092
	1.2 Excessive patient leakage current	1.2.1 D: Design IAW IEC 60601-1, Clause 8.7 [HA14]	PR27 The design and operation of the device shall conform to the requirements of IEC 60601-1, Clause 8.7.	PVTP51 Verify device conforms to the requirements of IEC 60601-1, Clause 8.7.	PVTR22 IEC 60601-1 Compliance Test Report #TR6605-092
	1.3 Short to external components	1.3.1 D: Design IAW IEC 60601-1, Clause 8.9 [HA19]	PR28 The design and operation of the device shall conform to the requirements of IEC 60601-1, Clause 8.9.	PVTP52 Verify device conforms to the requirements of IEC 60601-1, Clause 8.9.	PVTR22 IEC 60601-1 Compliance Test Report #TR6605-092

Developing the assurance case is not as straight forward, as it involves translation of safety risk assessments, controls, requirements and design rationale into claims and arguments. From Table 1, we start with the first 3 columns, which originate in the product hazard analysis, as shown in Table 2.

Table 2: Hazard Analysis Excerpt

Hazard	Cause	Risk Control
Electrical Shock	User contacts live parts during operation	Design IAW IEC 60601-1, Clause 5.9.2

Hazards and causes can be translated into claims as shown in Table 3.

Table 3: Hazard/Cause Translation Example

Hazard: Electrical shock	Claim: Device is free of electrical shock hazards
Cause: User contacts live parts	Sub-claim: Live electrical parts isolated from user contact

Risk controls then become arguments traced to evidence, which in this case would be a compliance test report, as shown in Table 4.

Table 4: Risk Control Translation Example

Argument: Compliance with IEC 60601-1; Clause 5.9.2 minimizes risk of user contact with live parts during operation	Evidence: IEC 60601-1 Compliance Test Report #TR6605-092

We can see that an assurance case built on this approach would have limited depth, but may have large breadth (see Figure 1) if, for example, all applicable sub-clauses of the standard are addressed.

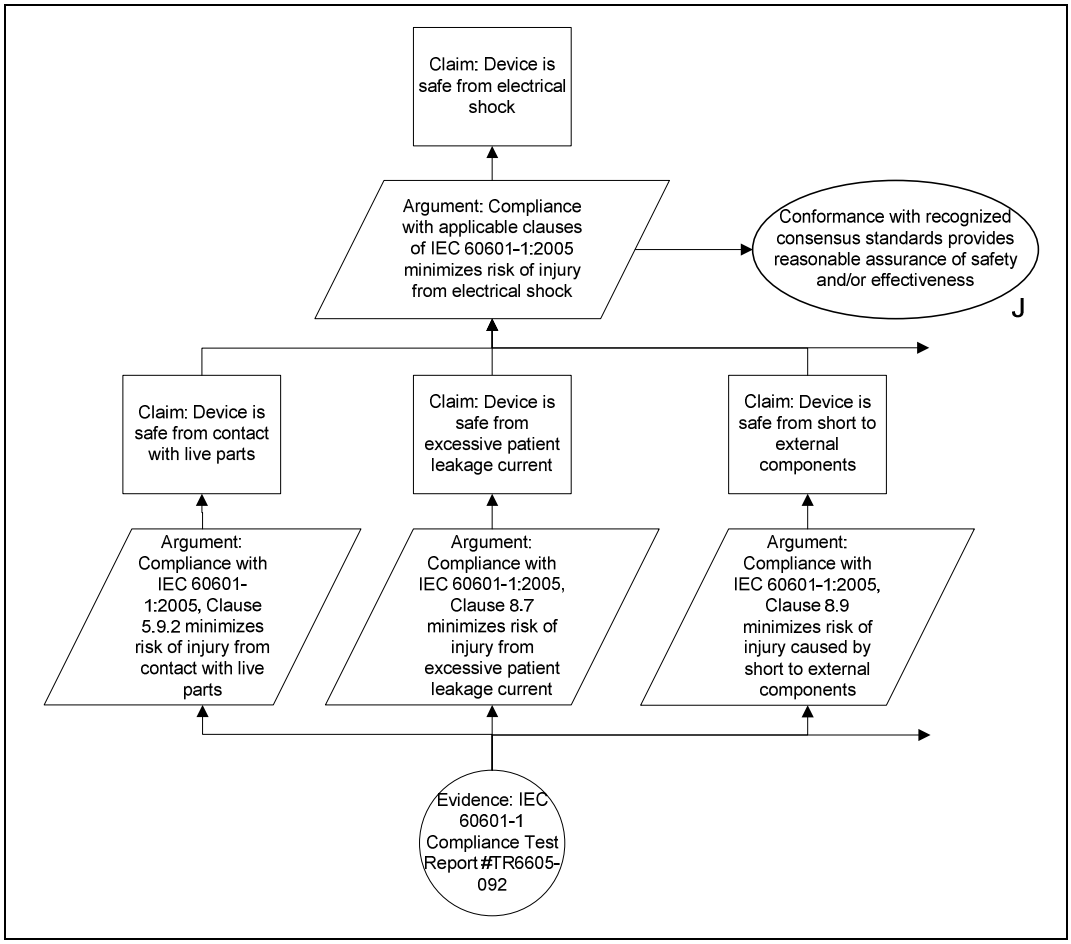

Figure 1. Assurance Case Diagram – Electric Shock

What is not clear at the time this paper was written is whether the depth of argument shown above is sufficient to prove the top-level claim. Examples appearing in some of the literature suggest that additional arguments and claims (i.e, rationale) would be expected. However, the justification that compliance with an FDA recognized standard, such as IEC 60601-1:2005, assures a reasonable level of safety should obviate the need for additional explanation as to why the device is safe from electrical shock.

In the more general case, we can expect to see cases with larger depth. Continuing the example of an electromechanical drug delivery device, another fragment from the DOORS traceability matrix showing a software-based risk control for overdose appears in Table 5.

Table 5: Safety Traceability Matrix – Overdose

Hazard	Cause	Required Risk Control	In-links at depth 1	In-links at depth 2	In-links at depth 3	In-links at depth 4
2 Overdose	2.1 Device is overfilled	2.1.1 D: Software monitors delivered dose and ends delivery when proper dose delivered [HA107]	PR35 The device shall deliver the target dose volume to within ±0.5%	SRS86 The device shall monitor the delivered drug volume with an accuracy of ±0.4%. SRS87 The device shall terminate drug delivery within 100ms of reaching the target volume.	SWTP191 Verify delivered volume is within ±0.4% of reported volume SWTP202 Verify piston velocity is 0 mm/sec within 100ms of receiving shut-down signal from motor controller	SWTR15 Verification of dose monitor accuracy SWTR16 Verification of motor shut-down time

Proceeding as before, the information in Table 5 is used to build another leg of the assurance case diagram as shown in Figure 2.

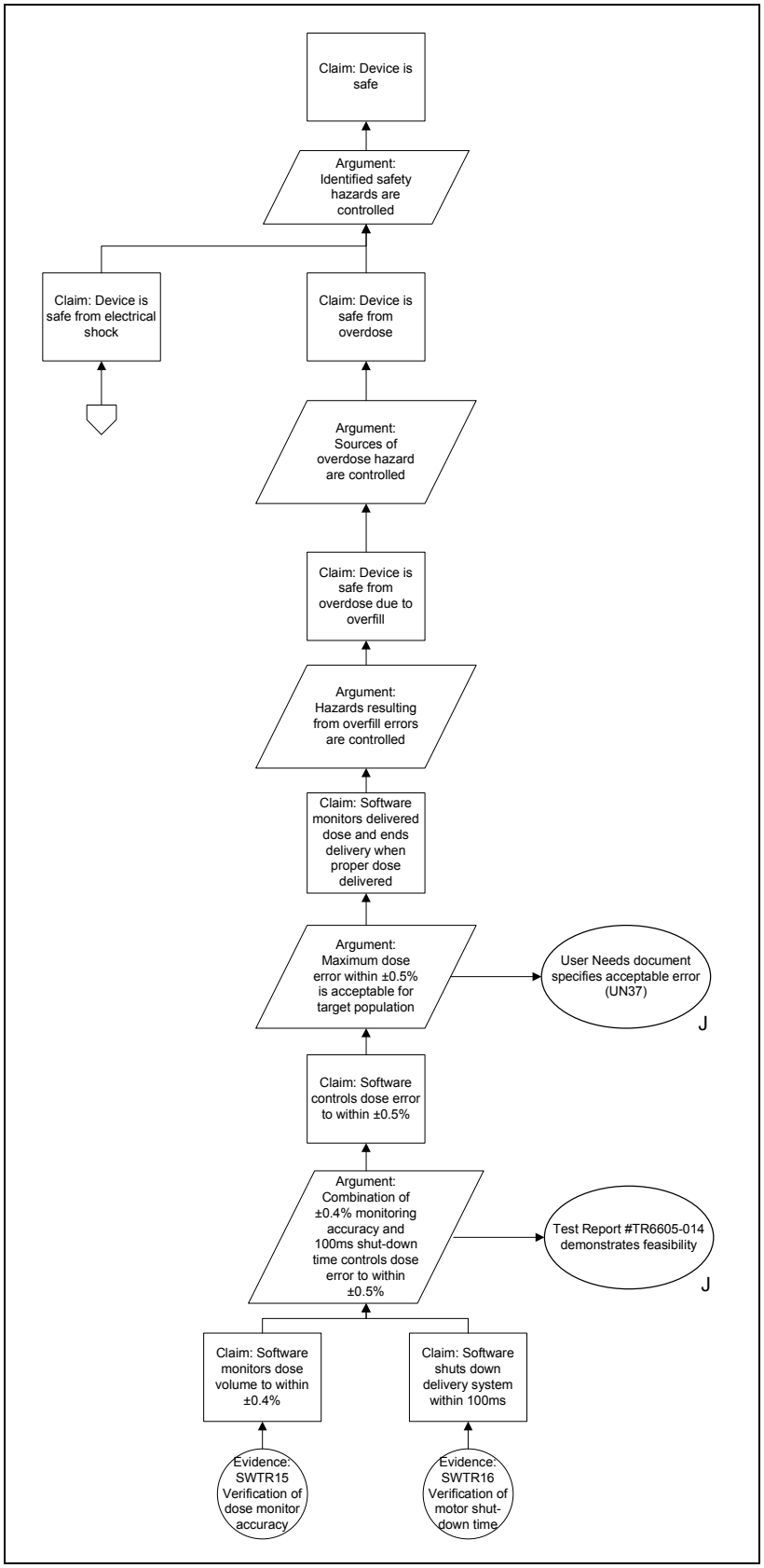

Figure 2. Assurance Case Diagram – Overdose

The claims generally appear in the risk control documents, requirements documents, and test reports of a typical medical device traceability matrix, albeit with some rewording to fit the assurance case format. However, the arguments would likely not appear as part of the requirements traceability, and would have to be generated as a separate exercise.

System Engineering Challenges

Few tools are available to aid system engineers in the development and management of safety cases. A web search identified a tool called GSNCaseMaker by CET Advantage, Ltd, located in Cardiff, Wales, UK. The company's website claims that "GSNCaseMaker is able to import and export data in an XML file that complies with the GSML Document Type Definition (DTD) data format." Whether this provides a means of interfacing to SysML is unclear. Tool requirements are listed as Microsoft Visio 2002+ and either Internet Explorer 6.0+ or Microsoft XML 3.0+. Weinstock [2009] cites two tools – "one an informally supported set of Visio macros," which may now be GSNCaseMaker. The other is the Assurance and Safety Case Environment (ASCE) available from the London, UK firm Adelard. A web search also identified a tool call Atego GSN Modeler by Atego, located in San Diago, California, USA.

Fault tree analysis (FTA) is a good example of the level of tool sophistication necessary to construct, maintain and reason about the information contained within a hierarchical structure. Even then, the hierarchy represented is structural as opposed to the semantic representation of an assurance case.

Integration into existing requirements tracking tools will present significant challenges, particularly the time involved to structure and maintain the cases. It may be possible to use the object-oriented approach of DOORS to generate a tabular form of assurance case, [see Adelard, 2006] by noting that the evidence supports a claim that we would expect to see as a requirement. However, the rationale (arguments) and sub-claims that provide the propagation through the hierarchy would have to be incorporated in the DOORS object link path, possibly as attributes associated with risk controls and requirements, or as objects in intermediate design documents. Also, the semantic nature of the assurance case elements, along with the multi-tiered hierarchical format would require careful wording of hazards, causes, controls, requirements and rationale statements in order to generate a human-readable representation that remains true to the GSN format.

Habli [2010] presents a safety case implemented in SysML using an automotive electrical/electronic safety-related system as an example. The model developed in the paper uses the SysML models of the system to determine how system failures could lead to hazards, and addresses those potential failures by defining required fault management behaviors, which are captured in activity diagrams. It is possible that tools that claim to support SysML could be utilized to build an assurance case. In this case, these tools often interface to requirements management tools. This interface could be very beneficial in the maintenance of the assurance case, risk management analyses, requirements etc.

Surveying the literature, it is apparent that the precise form of a safety case is fluid. Bishop [1998] presents examples where each claim is supported by an argument, and evidence at the leaf nodes are used to directly support arguments (claim-argument-evidence). Weinstock [2009] uses arguments very sparingly, preferring instead to go straight from claim to sub-claim in most cases. He also structures his examples with evidence at the leaf nodes directly supporting claims (claim-argument-claim-evidence). Chapman [2010], while citing Weinstock [2009], provided the FDA's view of the assurance case logical schema patterned after Bishop [1998]:

- "Each claim:
  - Must have at least 1 child argument
  - Can have zero or more subsidiary child claims
  - Must have no child evidence
- Each argument:
  - Must have one or more parent claims
  - Must have one or more child evidence
  - Can have zero or more child claims
- Each bit of evidence
  - Must have one or more parent arguments
  - Must have no child evidence, child claims or child arguments"

An additional challenge that was touched on earlier is the determination of what depth is sufficient to prove the top level claim. This assessment could be based on the level of risk associated with the device or the claim being supported. Perhaps the evidence only needs to show compliance with a clause in an FDA compliance standard and this should be sufficient. This is an issue that many medical device companies are discussing and asking the FDA for additional guidance. Time will tell as more companies submit 510(k)s that require an assurance case is developed.

Conclusions

The increasing complexity of medical devices and the user interaction required to operate them have been identified as complicating factors in the safe and effective use of infusion pumps. To this end, the FDA identified an initiative in April of 2010 to address these concerns by requiring device manufacturers to perform an assurance case. The adoption of assurance cases as a component of medical device submission packages to the FDA presents significant challenges to the system engineers responsible. Existing documentation tools will have to be adapted or replaced in order to support creation, management and maintenance of the safety cases during the device design and development. Medical device manufacturers will need to develop documentation processes and practices to ensure that the resulting safety cases are complete and accurate.

References

Adelard. 2006. ASCAD – Adelard Safety Case Development Manual. Adelard, Northampton Square, London. ISBN 0953377105.

Bishop, P. and R. Bloomfield. 1998. "A Methodology for Safety Case Development," in Proc. Safety-Critical Systems Symposium, Birmingham, UK, Springer-Verlag. ISBN 3540761896.

Chapman, R. 2010. "Assurance Cases for External Infusion Pumps," downloaded from http://www.fda.gov/downloads/MedicalDevices/NewsEvents/WorkshopsConferences/UCM219685.pdf

Eubanks, F. and C. Gibson. 2010. "Managing Patient and Operator Safety throughout the Life of a Medical Product," In Proc. INCOSE International Symposium 2010, Chicago, IL.

FDA. April 2010a. Infusion Pump Improvement Initiative

FDA. April 2010b. Total Product Life Cycle: Infusion Pump – Premarket Notification [510(k)] Submissions.

Habli, I, et.al. 2010. "Model-Based Assurance for Justifying Automotive Functional Safety," In Proc. 2010 SAE World Congress, 2010.

Kelly, T. P. 1998. Arguing Safety – A Systematic Approach to Managing Safety Cases. Doctoral thesis, University of York, UK.

Roberson, S. and J. Roberson. 1999. Mastering the Requirements Process. ACM Press, Harlow, Essex, UK. ISBN 0201360462.

Toulmin, S. 1958. The Uses of Argument. Cambridge University Press, Cambridge, UK.

Weinstock, C., J. Goodenough and J. Hudak. 2004. "Dependability Cases," Carnegie Mellon University Technical Nore CMU/SEI-2004-TN-016.

Weinstock, C. and J. Goodenough. 2009. "Towards an Assurance Case Practice for Medical Devices," Carnegie Mellon University Technical Note CMU/SEI-2009-TN-018.

Biography

Fritz Eubanks has more than 20 years experience in engineering support both internal and external to Battelle, and has worked in medical device development at Battelle for 13 years. He is involved in system-level design and analysis of both medical and commercial products, with emphasis on safety risk management, requirements management and testing, system reliability analysis, and design for manufacturing and assembly. He serves as Safety Risk Management Lead Engineer for Battelle's Medical Device and Diagnostics product line, is an ASQ Certified Reliability Engineer and a member of INCOSE. He received a B.S. in Mechanical Engineering from Kansas State University in 1982, and M.S. and Ph.D. from Ohio State University in 1992 and 1996, respectively.

Melissa T. Masters is an Engineering Manager with Battelle's Medical Device and Diagnostics group. Her experience spans product development, project management, systems engineering, and software and hardware development. Her responsibilities have ranged from software design, software performance analysis, software configuration management, and software verification. Other responsibilities have included project management, task management, writing and testing subsystem specifications, testing of clinical and prototype devices, and conducting clinical trials involving human subjects. In addition, Ms. Masters has a working

knowledge of domestic and international regulatory requirements for medical devices. She graduated with a B.S. in Electrical Engineering from The Ohio State University. She is a member of INCOSE, the Association for the Advancement of Medical Instrumentation, the Healthcare Business Association, and the Regulatory Affairs Professional Society