A Model-based Reference Architecture for Medical Device Development

Steven Corns, Ph.D.
Missouri University of Science and Technology
1870 Miner Circle
Rolla, MO 65409

Chad Gibson
Battelle Memorial Institute
505 King Ave
Columbus, OH 43201

Abstract. The application of systems engineering within the medical device domain must adapt to its unique challenges such-as the regulatory environment that these devices have to be designed within to ensure patient safety, and the nature of the interactions between the device and the patient. The sheer number of regulations imposed by government agencies such as the U.S. Food and Drug Administration and various international agencies adds to the complexity of designing these systems. This also presents an opportunity to implement a Model-Based Systems Engineering (MBSE) approach to capture the regulatory environment and map those specialized requirements to components within the system that address those requirements. In this study, we present a model of a reference architecture that can be used as a starting point for the system design of medical devices. Although the state of the model has not been fully matured, this approach offers the potential to more efficiently address the complex regulatory requirements, and reduce the time to design medical devices.

Introduction

Medical device manufacturers are challenged with managing the increasing complexity of both the regulatory environment and the inherent complexity of their devices, particularly due to the increased amount of embedded software. Medical devices must be designed using a regimented "design control" process that includes requirements, design specifications, verification, and validation. Effectively implementing a complex medical device while ensuring high levels of safety and effectiveness is a challenge, and has business, regulatory, legal, and human consequences if the requirements, design, and use environments are not fully understood.

The authors propose the use of Model-Based Systems Engineering (MBSE) as one solution to address these complexities. This work is an initial effort to develop a reference architecture that is ultimately intended to support the design of medical devices, which addresses the full life cycle considerations including manufacture, use, and disposal. This modeling approach leverages SysML to model the reference architecture in terms of the physical hierarchy of a generic device along with the interactions with the variety of environments it must operate within including the social-technical environment found in hospitals and clinics, and the user environment for devices that are integrated into the human system. The reference architecture also includes traceability to typical regulatory and compliance requirements. By establishing a reference architecture for

these devices it is possible to speed the development process while ensuring the safety and effectiveness of the devices.

Background

There are several factors in medical device development landscape that have made the conditions ideal for applying MBSE. Devices are becoming more integrated and complex. Advances in technology have laid the groundwork for "smarter" devices, including those that can diagnose illness and make decisions. In addition, the regulatory and compliance environment is becoming increasingly difficult to navigate, in part due to unique country- and region-specific requirements (e.g., US, EU) and emerging compliance standards that require a more systematic, risk-based approach to medical device development.

This project is part of the INCOSE MBSE initiative, and supports the activities of the INCOSE Biomedical Working Group. This project is one of four INCOSE MBSE Challenge Team projects currently being explored to determine the maturity of MBSE approaches and how they can be applied to the system design process by practicing engineers. The analysis of biomedical device development further extends the application of MBSE to address new considerations such as patient safety. However, this also offers the opportunity for sharing of the lessons from applying MBSE across application domains.

Medical Device Development

The development of medical devices is highly regulated in most countries and economic regions. The United States (US) governs the development and manufacture of devices via the United States Code of Federal Regulations; the European Union (EU) regulates devices through the Medical Device Directive, 93/42/EEC. Regulations typically include requirements around the development, manufacture, and sale of medical products. The EU requires compliance with a host of published standards. Although the US does not require compliance with most medical device standards, the Food and Drug Administration (FDA) established "recognized consensus standards" with which manufacturers may conform to help facilitate regulatory clearance or approval. The regulations and standards, in general, have been increasing in number and in development complexity. For example, an electrical medical device safety standard, IEC 60601-1:2005 (IEC, 2005), will soon become required for devices entering the European Community. This standard used to consist primarily of discrete tests (e.g., electromagnetic compatibility, drop testing, patient leakage), but has shifted to a much more patient-focused, risk-based approach. Recent regulatory focus has keyed in on usability and human factors. The medical device developer and manufacturer must also consider (and validate) the users' and patients' interactions with the device, and must do so throughout the system lifecycle process.

In parallel to the growing complexity of the regulatory and compliance landscape, devices are increasing in complexity and sophistication. The use of software in medical devices was relatively novel just twenty years ago, and is now commonplace in electrical medical devices. Processing power and data capacities have increased significantly; electronics footprints have

shrunk. New materials have been developed and are available to manufacturers, including those that replace body structures or elute pharmaceuticals.

Most regulatory bodies require requirements, safety risk management, design specifications, traceability, verification, and validation as a bare minimum of design documentation. These "design inputs" and "design outputs" (as they are typically termed in the medical device community) may be insufficient to efficiently or safely realize a system. Complex medical devices, particularly those that are a high safety risk or that contain multiple subsystems, become increasingly difficult to manage through a text-based system of risk identification and requirements development.

While the landscape of complex medical devices has many overlaps to the aerospace and defense industries, there are unique differences as well. Table 1 gives a comparison of typical attributes of medical device and defense system designs.

Table 1: Comparison of typical attributes of medical device and defense contract designs.

	Medical Device Development	Defense Contract Development
User Population	● Medical Professionals ● Home Users ● Caregivers	● Defense Personnel
Use Environment	● "Human-Compatible" Environments	● Land, Air, Water, Space ● Controlled on-site or remotely
System Complexity	● Tongue Depressors ● Highly Integrated MR Imaging Systems ● Closed-Loop Physiologic Control	● Highly Complex ● System-of-Systems
Regulatory and Compliance	● Heavily Regulated Environment	● Heavily Regulated from an Acquisition Perspective
Primary System Goals	● Safety and Effectiveness	● Mission Objective ● Cost Effectiveness
Acquisition Period	● 2-4.5 Years for Development of a New System (Lucke, Mickelson, and Anderson, 2009)	● 5-10 Years for System Design and Acquisition

Model Based Systems Engineering

Model Based Systems Engineering is a systems engineering concept that shifts the focus of the systems engineering effort from a document based paradigm to one in which the system information is stored, manipulated, and analyzed completely within a computer environment. By maintaining all of system information within computer models, information sharing is made seamless and the consistency of that information throughout the design process is easier to maintain. In addition, traceability can be maintained from requirements to system design, analysis, and verification. MBSE provides the systems engineer an integrated set of tools to plan and communicate the device design. The models may be used for both internal and external communication, making it possible to represent the information exchange between all of the interfaces of the device.

The OMG Systems Modeling Language (OMG SysML™) was adopted by the Object Management Group (OMG) in 2006 (OMG, 2011a). Using nine diagrams, SysML models can represent the system structure, behavior, requirements, and parametric relationships in a standard format that can be shared and re-used for the design of complex systems. SysML is a modified version of the Unified Modeling Language (UML) (OMG, 2011b), removing many of the software centric diagrams from the language and adding diagrams that capture information regarding requirements, structural elements, and the parametric equations that represent the system.

Model Development

A closed-loop drug delivery system was chosen as a basis for defining the reference architecture. This human-in-the-loop system adjusts parameters based on a physiological response from the patient. This particular reference architecture was selected to demonstrate the unique aspect of this medical device involving the interaction between the patient and the device. The systems engineer and development team must often consider the operators and patients from a variety of angles: usability, safety, effectiveness, and as a physiologic system.

The development pathway of the reference architecture model was intended to mirror that of a typical medical device. Although there are many pathways that could be taken for device development, this architecture was designed to maintain a sufficient level of abstraction to make it applicable across a wide range of design projects. A block definition diagram representing the domain for a drug delivery device (fig. 1) was developed to describe the stakeholders and necessary environmental concerns for the development of this type of device. The subsections below detail the key activities to complete this reference architecture following a logical sequence, although it should be noted that the process was iterative in nature; the device architecture began at a low level of complexity and was iterated to include more detail.

Stakeholder Requirements. An initial draft of user requirements was captured in the model to serve as a starting point for discussion, use environment investigation, and further refinement. Often, stakeholder requirements are passed down from other departments (e.g., marketing) and are refined prior to release. For example, a requirement may state “The device shall operate in an

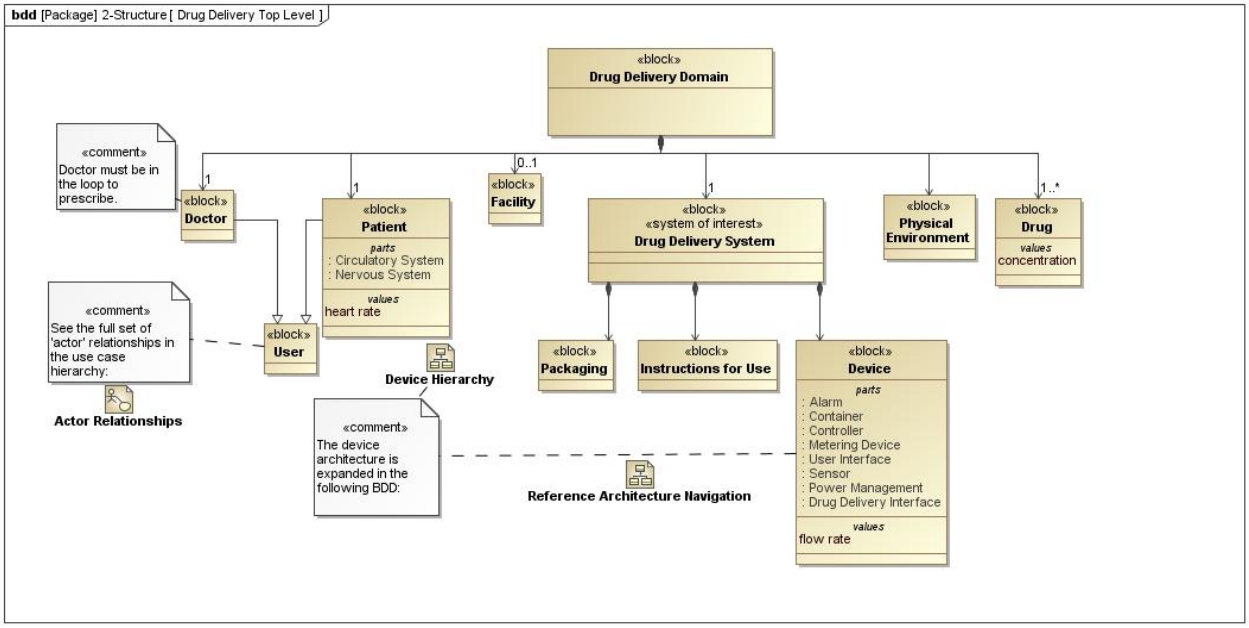

Fig. 1, Drug delivery device domain

ICU environment." A subsequent usability assessment may find that the use environments between a neonatal intensive care unit (NICU) and a cardiac intensive care unit (CCU) are extremely different. This may prompt refinement of the requirement to increase specificity, or may highlight the need for additional use cases and sequence diagrams to effectively design for both environments. Figure 2 shows a portion of the stakeholder requirements diagram, showing the regulatory, business, environmental, drug delivery parameter, and user requirements shown. Because of the size of the diagram, a portion is exploded to show a sample of the content.

System Level Use Case Diagram. Development of medical devices requires an understanding of the end-use environment (IEC, 2005). This drives early usability engineering and safety risk management activities which are primarily intended to identify and mitigate safety risks prior to implementation (ANSI/AAMI/ISO, 2007). System level use cases (i.e., the black-box system) were developed as a starting point for sequence diagram development. The identified users included the patient and caregiver(s) as well as more abstract users such as the Hospital Information System and regulatory bodies. The identified use cases covered the device's lifecycle from prescription to disposal.

Sequence Diagrams. The identified use cases served as the starting point for safety-critical sequence diagrams. The reference model focuses on those sequences which may have the most impact to safety and effectiveness, and on the interactions between the users and the black-box system. The intent of this step is to help identify safety hazards which may require risk control, or to simply identify use areas where the development team needs to validate their understanding.

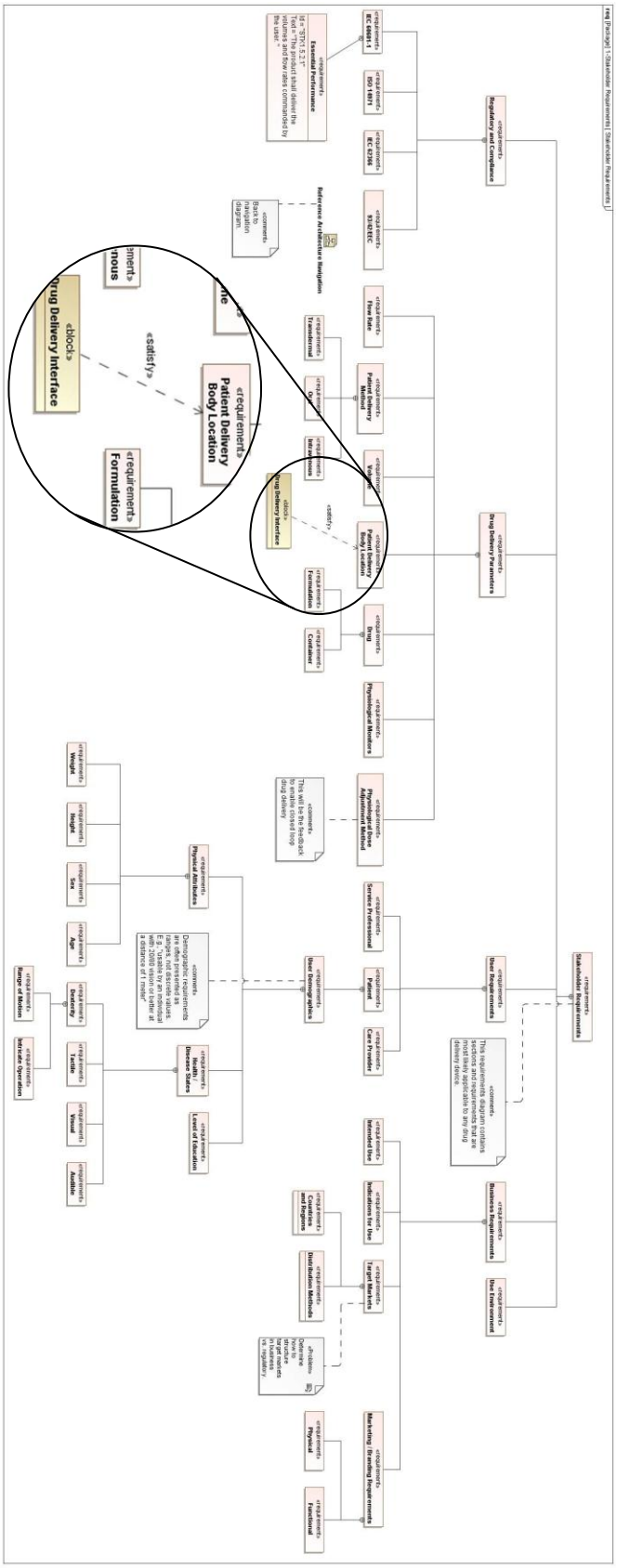

Fig. 2, Drug delivery device stakeholder requirements diagram

Hazard Analysis / Fault Tree Analysis. A "top down" hazard analysis is required for most medical devices, and was initially implemented in the reference model as a requirements diagram. The hazard analysis also includes a use error analysis, which is required by new regulations and compliance standards. The identified risks are identified and controlled via design, labeling, or training as needed. ISO 14971:2007 (ANSI/AAMI/ISO, 2007) provides a process framework for medical device safety risk management, and can be implemented in part through requirements diagrams. Required risk controls trace into system requirements and architecture, and are key to demonstrating safety and effectiveness. Since these model elements relate to patient or operator safety, they received greater attention and detail as they were implemented in the structure, behavior, and parametric models.

System Requirements. Stakeholder requirements, hazard analyses, and system requirements typically fulfill the "design inputs" prior to commencement of design activities. The requirements and risk management results will typically enter configuration management prior to a formal review of the design inputs. Based on the stakeholder requirements, system level requirements were created (fig. 3) to further decompose the system. While stakeholder requirements and the hazard analysis drive the system requirements, they may also be beneficial to System Structure.

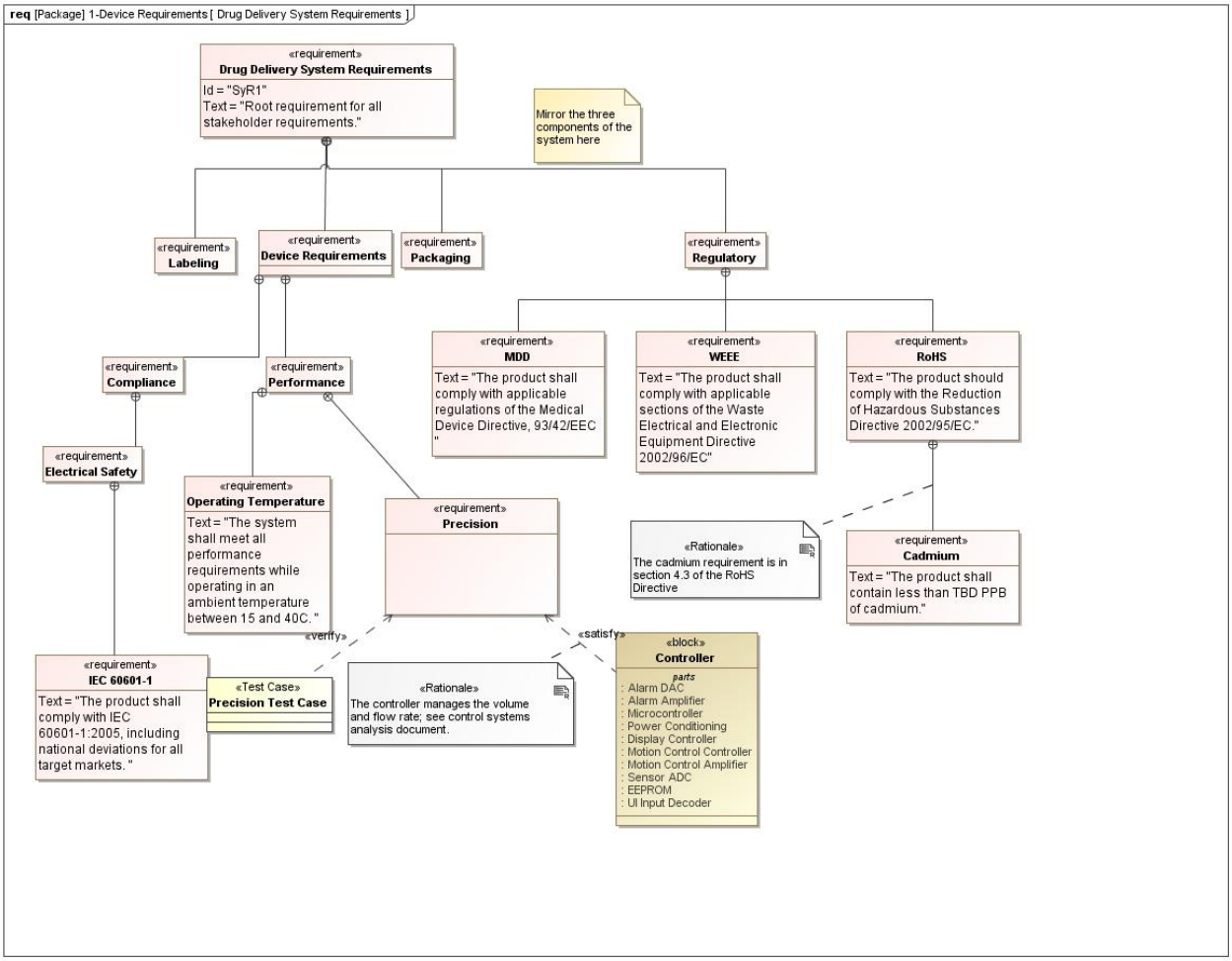

Fig. 3, Drug delivery device system requirements diagram

System Structure. Using the system requirements, a system structure was created using a block definition diagram (fig. 4). This structural representation was maintained at a high level of abstraction to allow for flexibility, but it encompasses all of the sub-systems that would be expected for a drug delivery device. Through the use of generalization of these components a unique device could be modeled and specified with increased confidence that all required devices are represented. These structural components are then linked to the functions and requirements they satisfy to allow for traceability throughout the device design process.

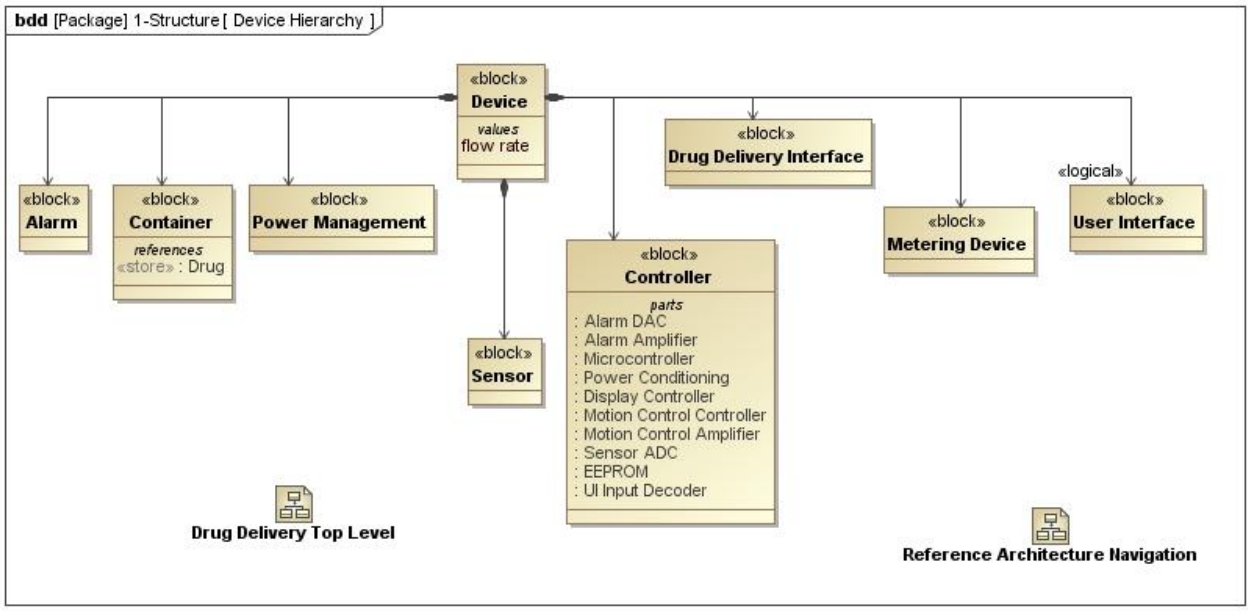

Fig. 4, Device hierarchy representing medical device sub-systems

Discussion and Future Work

The architectural framework presented in this paper makes it possible for medical device engineers to prepare designs on an accelerated schedule with additional confidence that the required components are present. In addition, by coupling the requirements to the functions and the requirements to the physical architecture it allows for a mapping that will link the validation procedure to this verification loop.

There are several additional areas to move forward with this framework. One of the issues of special consideration with medical devices is human factors. For most systems this pertains to the system usability, both in humans manipulating the system and the ability of human users to extract information from the system. Medical devices inherently have more complex human factor relationships, as the primary functions of these systems is to interact with a human, and often to enable one human to interact with another. Because of this, a larger focus on the usability of the system is necessary for this domain. Integrating these concepts into an architectural framework makes it less likely that an integration step will be omitted or incorrectly

applied. In the case of drug/device combination products, the human factors problem is further complicated by the potential for adverse reactions to the drug(s) being administered. The modeling of the human body or any system that is not fully understood presents a new set of challenges for the MBSE community.

This MBSE approach to device design allows for a more consistent design process with regard to inclusion of safety needs. The required safety features are automatically integrated into the design through the architectural framework, so that designers are informed of the necessary regulatory interfaces for safe device creation. In addition, different views can be created to solicit subject matter expert input for any of the safety requirements that may be optional. This also allows for the traceability of the system components/elements back to the safety requirements as well as the regulatory requirements.

The hazard analysis presented in this work is a preliminary effort, and further work is planned to provide additional details describing the hazards and how they might be addressed. Another set of behavior diagram examples would need to be completed to provide additional detail on the risks associated with these hazards, how the negative occurrences might occur, and elaborate on a mitigation plan. A method for performing this type of work can be found in fault tree analysis work performed by Douglass (1999) using UML.

Another next step is to test the framework by using it to design of an actual system. This will allow for a better assessment of the guidance provided and allow for the verification and validation of the system. As the specific device is proposed and development begins, the integration of the engineering analysis tools can be planned out along with the necessary hand offs to the MBSE representation. The analysis tools will be used to inform designers on the performance of the system and assist in creating methods for verification and validation. The creation of methods for validating the systems developed using this architecture is one of the important next steps to be developed in this process. System verification and validation typically requires painstaking attention to detail to ensure that the system performs all necessary functions and satisfies the customer's needs, including device safety and effectiveness. Verification can be accomplished with the above linkage of the structure to the requirements. The validation methods can similarly be linked to the structural sub-systems and associated requirements, with behavior diagrams such as state machine diagrams describing how the testing and evaluation will be performed to ensure system compliance.

The goal of this work is to use this reference architecture as a means to speed the development and approval of medical devices. To accomplish this, example medical devices will be designed using the modeling approach. The present modeling approach will be used, with the abstract components refined through instantiation of the elements that make up the system. By having the necessary regulatory issues identified in advanced and identifying how these issues impact the device design, the overall design process can be accelerated to meet increasingly aggressive schedules while providing cost savings.

References

IEC. 2005., *IEC 60601-1 Medical electrical equipment - Part 1: General requirements for basic safety and essential performance*, International Electrotechnical Commission.

ANSI/AAMI/ISO, *ANSI/AAMI/ISO 14971*. 2007, *Medical devices – Application of risk management to medical devices*, International Organization of Standardization.

Douglass, B. P. 1999. *Doing Hard Time: Developing Real-Time Systems with UML, Objects, Frameworks and Patterns.* Addison-Wesley.

Lucke, L., Mickelson, A., and Anderson, D. 2009. "Proving Experience Speeds Medical Device Time to Market," 31st Annual International Conference of the IEEE EMBS.

Friedenthal, S., Moore, A., and Steiner, R. 2008. *A practical guide to SysML: The Systems Modeling Language*, Morgan Kaufmann, San Francisco, 2008.

OMG 2011a. OMG SysML 1.2 specification, http:/www.sysml.org, Object Management Group, last accessed November 8, 2011.

OMG 2011b. UML 2.3 specification, http:/www.uml.org, Object Management Group, last accessed November 8, 2011.

Acknowledgments

The authors would like to thank Sanford Friedenthal for his contributions to the INCOSE Biomedical Working Group MBSE challenge team and his continued support of the work described in this paper.

Biography

Steven Corns is an Assistant Professor in Systems Engineering at Missouri University of Science and Technology. He received his PhD in mechanical engineering from Iowa State University in 2008. His main research interests are in the areas of evolutionary computation applications, the mechanics of information transfer in evolutionary algorithms, and model based approaches for complex systems design and analysis. He is an active member of INCOSE, leading the MBSE initiative challenge team for biomedical modeling.

Chad Gibson is a Systems Engineer with Battelle's Health and Life Sciences group. He has ten years of experience in medical and in vitro diagnostic device development, spanning across systems engineering, Design for Six Sigma (DFSS), and hardware and software design. He graduated with a B.S. in Electrical Engineering from The University of Cincinnati. He is a member of INCOSE and developed the SysML reference architecture for the biomedical model-based systems engineering (MBSE) project.