A Systems Approach to Medical Device Compliance with IEC 60601-1:2005

Chad Gibson; Fritz Eubanks, Ph.D., CRE; Felicia Hobson
Battelle Memorial Institute
505 King Ave
Columbus, OH 43201
(614) 424-6400

Abstract. The development of electrical medical devices requires compliance with a host of regulations and standards to help ensure their safety and effectiveness. One of the most notable additions in recent years is the 3rd Edition of IEC 60601-1 (IEC 60601-1, 2005), "Medical electrical equipment – General requirements for basic safety and essential performance." Medical devices sold to the European Community and Canada must comply with the standard in 2012, and devices in the U.S. and other countries must follow shortly thereafter. This standard represents a sea change in the way medical devices are typically developed, and includes a heavy reliance on safety risk management and usability engineering processes. This paper presents the systems engineer as the ideal candidate to lead these activities and facilitate device development; the standard impacts many areas (e.g., engineering, regulatory, human factors, and project management) and requires a methodical approach to implement in a cost-effective manner while ensuring safety and effectiveness of the device. This paper details techniques developed to efficiently comply with the standard, leveraging existing systems engineering practices and emerging methods such as Model Based Systems Engineering.

Overview of the Standard

In order to place medical devices on the market, many countries or regions require or recommend compliance to certain international standards. The 3rd Edition of IEC 60601-1 (IEC 60601-1, 2005), along with its national deviations, is one such standard. Even in countries where compliance is not mandated by regulations (e.g., the FDA in United States), compliance with this and other standards helps facilitate regulatory clearance or approval by providing regulators with a well-known framework that helps demonstrate the safety and effectiveness of the device.

IEC 60601-1:2005—hereafter referred to as the "3rd Edition"—is titled "Medical electrical equipment – General requirements for basic safety and essential performance." Mechanical-only medical devices do not fall within this standard. The standard focuses on safety and performance of the device, and presents a multitude of requirements, including safety risk management processes, usability engineering processes, electrical and mechanical safety testing, and labeling. The 3rd Edition points to other "collateral" standards which are required, and—depending on the type of medical device—"particular" standards which provide more specific tests and requirements.

Changes from the Second Edition

The 3rd Edition was a significant departure from the 2nd Edition of the standard. Most notably, the 3rd Edition:

- Expands upon the concept of "Essential Performance"
- Requires heavy reliance on the results of a Safety Risk Management (SRM) process
- Requires a Usability Engineering process
- Incorporates previously separate standards and requires compliance to additional standards.

Essential Performance. Essential Performance is defined in the standard as "performance necessary to achieve freedom from unacceptable risk". The Essential Performance must be defined by the manufacturer as part of their safety risk management process. Many of the clauses and tests of the 3rd Edition reference Essential Performance; for example, the manufacturer must mitigate the effects of radio frequency interference which may cause degradation of Essential Performance. This is a significant departure from the theme of the 2nd Edition, which relied heavily on a standard set of tests and inspections of the device (e.g., inspection of electrical labeling symbols, leakage current testing) that wasn't necessarily tied to the device's Essential Performance.

Safety Risk Management. Clause 4.2 of the 3rd Edition states that:

> *Compliance is checked by inspection of the risk management file. The requirements of this clause and all requirements of this standard referring to inspection of the risk management file are considered to be satisfied if the manufacturer has:*
>
> - *Established a risk management process*
> - *Established acceptable levels of risk*
> - *Demonstrated that residual risk(s) is acceptable (in accordance with the policy for determining acceptable risk).*

The 3rd Edition requires conformance to the risk management standard ISO 14971: "*Medical devices -- Application of risk management to medical devices."* The first two bullets above can be satisfied by explicitly stating the manufacturer's risk management policy via standard operating procedures or other forms of corporate policy that address the requirements of ISO 14971:2009, Clause 3. The third bullet is satisfied through the hazard identification, risk evaluation and risk control process defined in ISO 14971:2009, Clauses 4, 5, and 6.

Note that the identification of essential performance is also a risk-based process, except that it assumes that a sequence of events has taken place, such that the feature or function in question has been lost or degraded, resulting in a hazardous situation. The mechanics of this process will be covered in a later section.

Usability Engineering. Consideration of usability—the characteristic that establishes effectiveness, efficiency and operator learnability and satisfaction (IEC 60601-1-6, 2010)—is now required as part of 3rd Edition compliance. Many principles outlined in the 3rd Edition agree with those outlined in the "Safety" and "Survivability" Human Systems Integration domains outlined in the INCOSE SE Handbook (Section 9.12).

The 3rd Edition outlines discrete activities to address usability. Though only several pages in length, the usability collateral standard (IEC 60601-1-6) requires tight integration with the entire device development process. Usability should be considered early in the lifecycle to understand and "design out" potential usability issues before the products are realized in the

physical domain. The application of the device, its primary operating functions, and safety labeling serve as inputs to the usability engineering process (IEC 60601-1-6, 6.2.2). Usability must be verified, and validated in an actual or simulated end-use environment.

Compliance with other standards. The 3rd Edition references two types of additional standards—"collateral" and "particular" standards. Particular standards, denoted by 60601-2-x, are standards that apply to specific medical devices. For example, IEC 60601-2-52 applies specifically to medical beds. The particular standards often define specific tests and override clauses in the base standard. Collateral standards are denoted by 60601-1-x, and are required to be evaluated along with the base standard (IEC 60601-1). The 2nd Edition generally did not require collateral standards to be evaluated. The alarms and usability engineering collateral standards (-1-8 and -1-6, respectively) have not been previously evaluated by many medical device manufacturers, and will require consideration throughout the product's entire lifecycle.

Key Compliance Activities. Most medical device manufacturers contract with a Certification Body (CB) to assess a device to the 3rd Edition. The CB's role has changed significantly from their role in assessing products to the 2nd Edition. Most notably, the CB will review the manufacturer's usability engineering and risk management files in addition to product inspections and tests. The documentation provided to the CB is much more extensive than for the 2nd Edition; typically, 2nd Edition documentation consisted of labeling (e.g., Operator's Manuals) and a few critical drawings or specifications in addition to a product sample for physical testing and inspections.

Approaches to Complying with the 3rd Edition

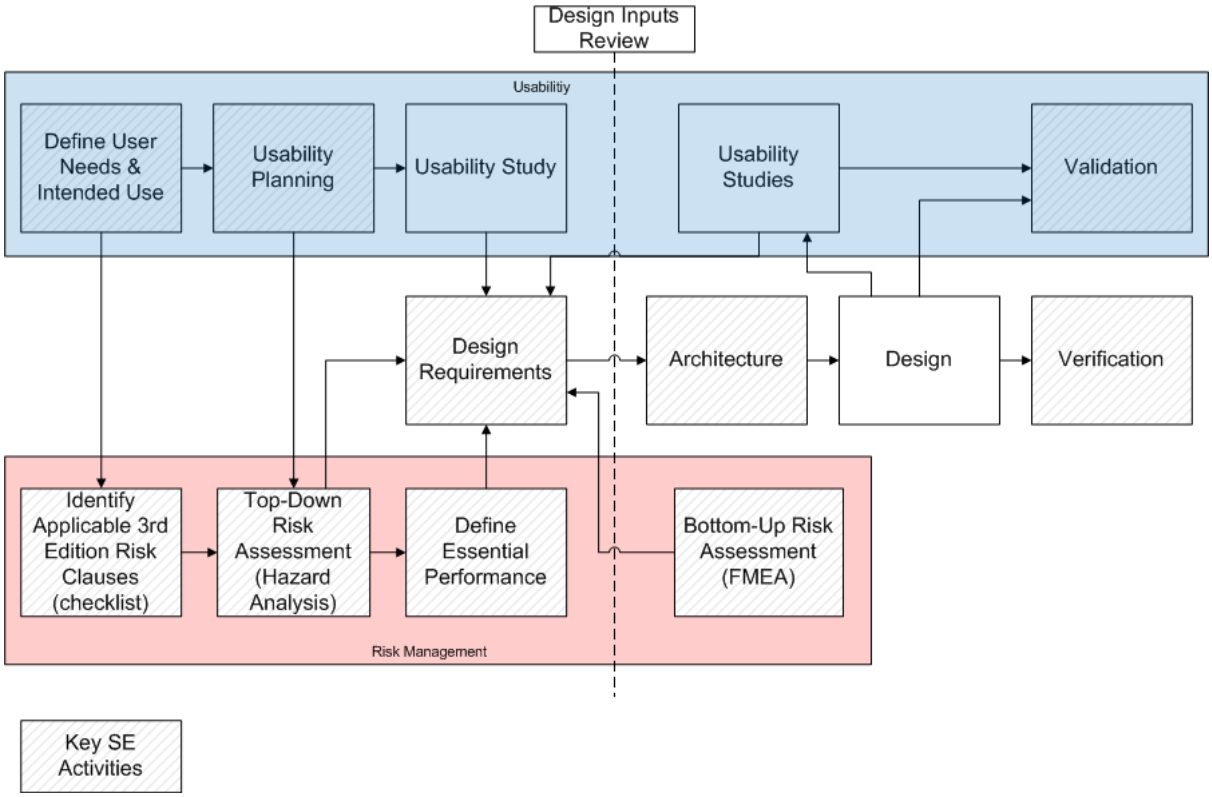
Medical device development which includes compliance with the 3rd Edition provides ample opportunities for the systems engineer. Many of the more difficult problems device manufacturers face with the 3rd Edition can be addressed by leveraging existing systems engineering practices. Compliance must be addressed by multiple stakeholders from the inception of device development; in particular, safety risk management and usability engineering span across the entire system lifecycle and impact many disciplines.

This section is split into two sub-sections: New Product Development and Addressing Gaps in "2nd Edition" Products. Many manufacturers are faced with the 3rd Edition adoption date of June 1, 2012 in Europe. This means that all medical devices placed on the market after this date—even existing medical devices—must meet the 3rd Edition of the standard. The United States, Canada, and many other countries and regions will follow shortly thereafter (though in some regions and countries, no 2nd Edition withdrawal date has been given).

New Product Development

The 3rd Edition requires a more process-oriented approach than compliance with the 2nd Edition. Compliance to the 3rd edition can be approached in a similar manner to the way risk is approached in ISO 14971 (details of this process are described in the risk management section below). The systems engineer is uniquely positioned to facilitate the 3rd Edition compliance process as the owner of the trace matrix and other key development outputs submitted and reviewed for compliance by the CB (e.g., the safety risk management file). Figure 1 shows the key activities that support 3rd Edition compliance for new product development and highlights where the systems engineer plays a central role. Arrows imply "provides input to."

Figure 1. Typical Medical Device Development Outputs and Relationships



The following subsections discuss the key elements in the compliance process to be facilitated by the systems engineer, with an emphasis on the new elements required in the 3rd Edition. The activities described below are often iterative in nature, requiring active monitoring and updating throughout the product lifecycle.

Definition or Acquisition of Stakeholder Requirements. Stakeholder requirements lay the foundation for subsequent design input planning. The systems engineer may or may not be the owner of this document—often these requirements may come from other divisions of the company. The systems engineer should ensure that all relevant information is included, particularly the intended use, indications for use, user population, and intended use environment. These requirements are often fleshed out in more detail as part of the initial usability assessment and use case definitions (outlined in subsequent sections).

SRM Planning. By one count, the words "risk management" appear in over 100 separate clauses of IEC 60601-1:2005. The phrases using those words include:

- Verified by review of risk management file
- As indicated in risk management file
- Risk associated with [ ] addressed in risk management process as indicated in risk management file
- As determined by application of risk management process
- addressed in risk management process as indicated in risk management file

What becomes clear is that the risk management file for the purposes of determining IEC 60601-1:2005 compliance will include not only the risk management plan, assessments and summary reports, but also product requirements, hardware and software specifications, and verification test reports. Traceability from the outputs of the safety risk management process to design and verification documentation will be an important element in the compliance

evaluation process.

The system engineer might prepare for the risk management process by determining which clauses of 60601-1 apply to the new product. A well-defined intended use statement, often in the stakeholder requirements, is an important input to this activity. The clauses that apply would then be ported into the hazard analysis and addressed as part of the risk management process. A justification should be documented for the clauses that are deemed not to apply to the new product. It will be necessary to provide this information to the CB for their 3rd Edition compliance assessment.

As stated in the "Background" section, the first two elements of IEC 60601-1:2005, Clause 4.2 can be satisfied by explicitly stating the manufacturer's risk management policy via standard operating procedures or other forms of corporate policy. The third element is satisfied through the hazard identification, risk evaluation and risk control process defined in ISO 14971:2007, Clauses 4, 5, and 6. The questions that the manufacturer must answer for the evaluator would be:

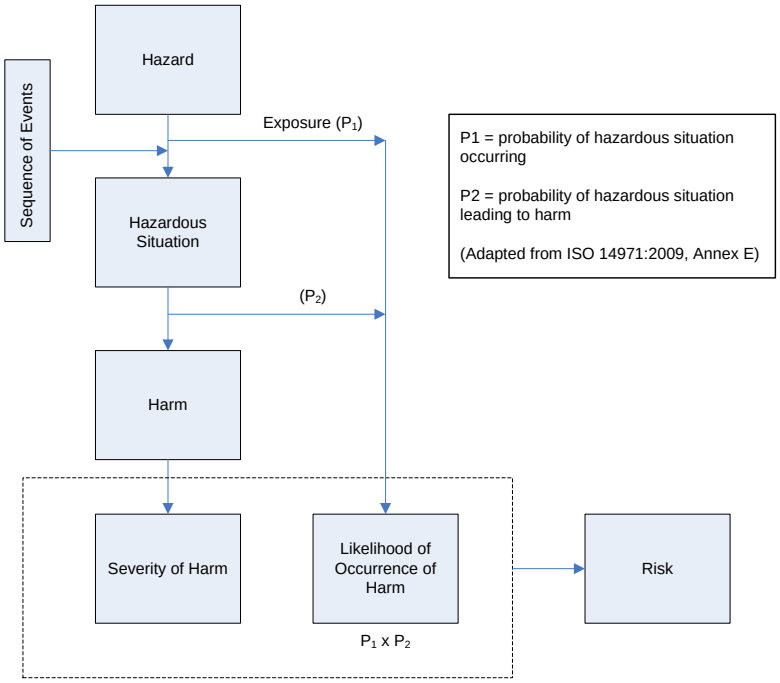
- Have all known and foreseeable hazards been identified?
- Have all known and foreseeable causes resulting in hazardous situations been identified?
- Have all unacceptable risks been either 1) controlled, or 2) shown to be as low as reasonably practicable by appropriate risk/benefit analysis?

Top-Down Risk Analysis. A typical "top down" risk assessment conducted in accordance with ISO 14971:2007, Clause 4, starts by identifying potential hazards (sources of harm), then proceeds to identify events or causes resulting in hazardous situations that in turn, have the potential to cause harm. Checklists and guide questions like those appearing in ISO 14971:2007, Annexes C and E, provide good tools for identifying general hazards associated with medical devices. Hazards that are not applicable to a specific device are usually not addressed in a hazard analysis or FMEA.

An additional checklist will be required that explicitly demonstrates that all clauses where inspection of the safety risk management file is required for compliance have been addressed as part of the safety risk management process. Clauses that are not applicable would be designated as such, where clauses that are applicable would contain pointers to the document containing the estimation and evaluation of the safety risk.

The risk is estimated as the combination of the severity of the harm and the composite likelihood that 1) the sequence of events (cause) results in a hazardous situation, and 2) the hazardous situation results in harm. The process is shown graphically in ISO 14971:2007, Annex E, Figure E.1, and adapted shown in Figure 2.

Figure 2. Relationship of Risk Assessment Elements
(adapted from ISO 14971:2009, Figure E.1)



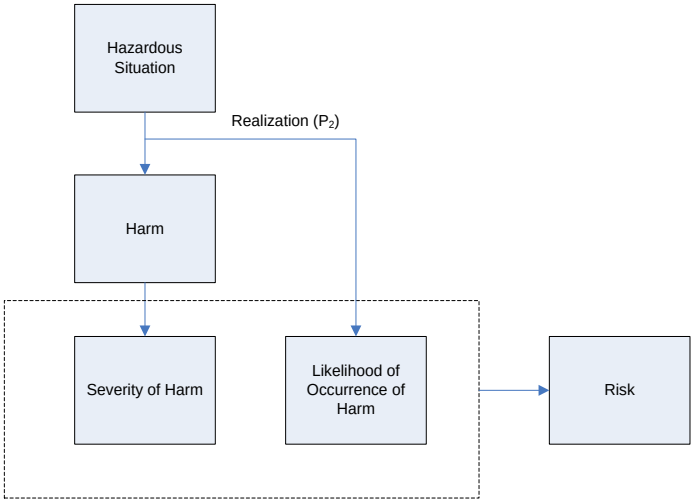
The estimated risk is compared to the risk acceptability criteria established by the manufacturer. Initial safety risks rated as acceptable do not require risk control measure implementation. If the initial safety risk is not acceptable, the next stage is to progress to the risk reduction via the implementation of risk control measures in accordance with ISO 14971:2007, Clause 6.

Definition of Essential Performance. The recommended method of identifying essential performance is stated in IEC 60601-1:2005, Annex A, Subclause 3.27, as follows:

> *Assessment of this risk is made on the assumption that the performance aspect in question has been lost or degraded, and takes account of the probability that harm would then occur (which in some instances could be 100%) and the severity of that harm. Application of the risk management process then ensures that the probability of loss of the performance aspect is low enough to make the residual risk acceptable.*

The identification of essential performance described above assumes that a sequence of events has taken place, such that the feature or function in question has been lost or degraded, resulting in a hazardous situation. Therefore, the level of risk used to determine whether essential performance is evaluated as the combination of the severity of the harm and the likelihood that the hazardous situation results in harm, as shown in Figure 3.

Figure 3. Essential Performance Identification Diagram



Note that the likelihood of occurrence for essential performance risk (P_2) is not the same as the composite likelihood of occurrence for safety risk (P_1 x P_2). If the manufacturer defines safety risk acceptability only in terms of the composite likelihood, a separate likelihood index will need to be developed for use in determining essential performance. Risk evaluation proceeds in accordance with ISO 14971:2007, Clause 5.

The process and criteria for determining essential performance (analogous to the safety risk acceptability criteria) are defined by the manufacturer and can be written into the Safety Risk Management plan or into a separate document and maintained in the Safety Risk Management file.

As in the case of hazard identification for safety risk, the analysis for essential performance must examine all known and foreseeable functional failures that could result in hazardous situations with unacceptable risk. Sources for compiling a list of functional failures include the statement of intended use, product performance requirements, and applicable regulations and compliance standards.

Usability Engineering. A usability engineering program is required for compliance to the 3rd Edition. IEC 60601-1-6, a collateral standard to the 3rd Edition, describes how to develop and follow a usability engineering process. It should be noted that IEC 60601-1-6 will eventually be replaced by IEC 62366; the standards are nearly equivalent, though 62366 expands the usability assessment to include non-electrical medical equipment. Compliance with one standard can easily be applied to the other. The primary evidence used to demonstrate compliance to the standard is a Usability Engineering File. This file provides evidence that the usability process was followed, and typically consists of "pointers" to other documentation.

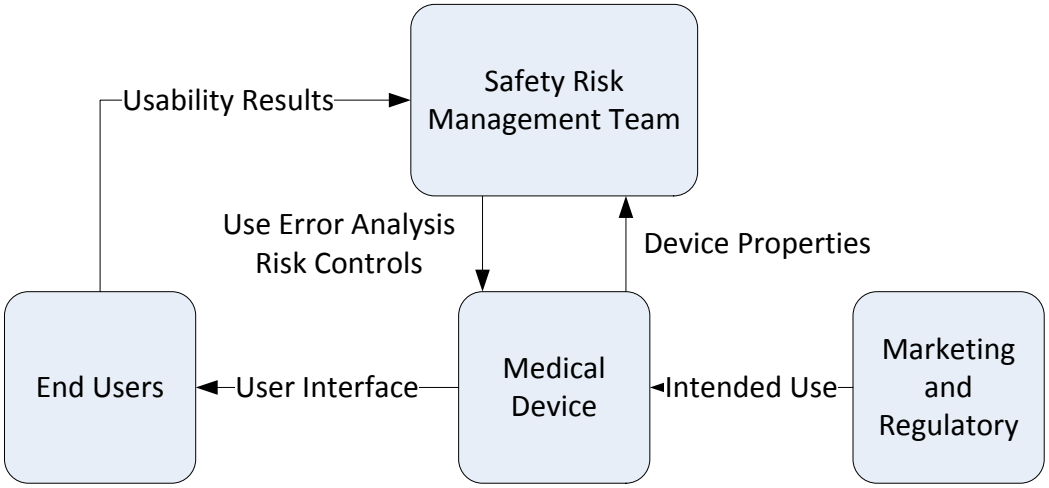
Understanding the use environment early in design will help design out potential usability issues reaching a stage where the device must be "patched" or mitigated through less effective means such as labeling or training. The systems engineer should incorporate usability early in the development cycle and as part of existing engineering lifecycle practices, and continue to track and manage the effort through verification and validation activities.

The usability engineering process may be incorporated with many existing medical device development activities. Since usability engineering is tightly integrated and concurrent with SRM activities, many required elements can be incorporated in existing SRM processes. For example, use error can be considered as part of a device hazard analysis. Once the device's critical functions are defined (i.e., the "Intended Use" of the device), use cases, sequence diagrams, and other architecture tools and practices (including those built into SysML) can be

used to understand and convey these user-device interactions. In most cases, usability engineering is best addressed through multiple validation efforts because "no validated techniques are known to exist to predict, in advance, the likelihood of a person committing a use error" (IEC 62366, 2008). An example may include an early validation of a graphical user interface (GUI) prototype to understand potential sources of error or confusion; this may help guide selection of a particular display technology which may be more difficult to re-design if the usability issue was discovered later in the process.

The systems engineer may be ideally suited to bridge the gap between the users and the design, with usability experts (e.g., cognitive psychologists or behavioral scientists) constructing the formative and summative validation efforts. Figure 4 shows the major relationships between the medical device and different usability stakeholders. Note that these flows may be iterative in nature.

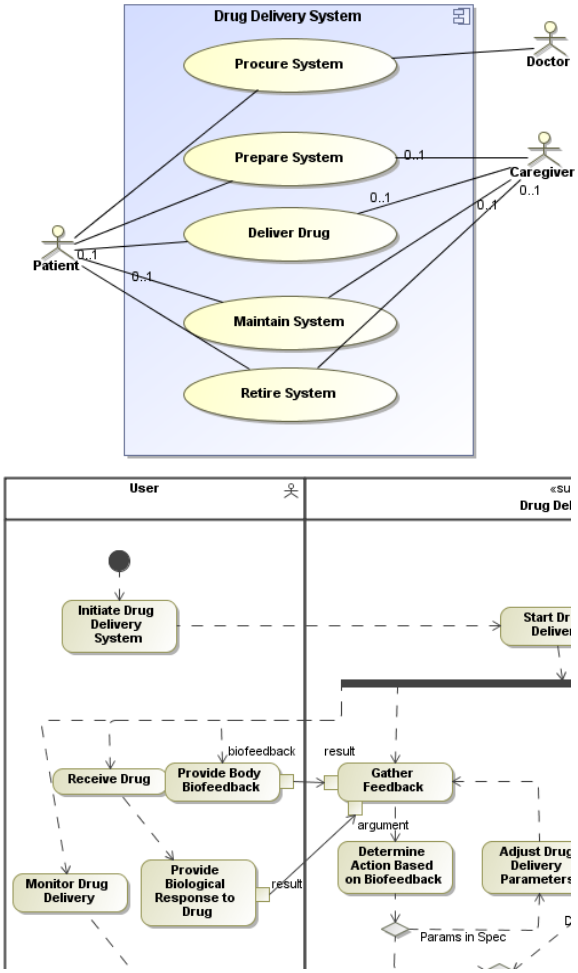
Figure 4. Usability Engineering Stakeholders



Requirements and Architecture. Management of compliance to the 3rd Edition can be a significant undertaking in a medical device development project. The sections noted above are only part of a medical device development effort. In many cases, particularly with complex electrical medical devices, a well-defined requirements and architecture package may help control an otherwise difficult to manage project. While design requirements are mandatory for most medical devices sold in the U.S., E.U., Canada, Japan, and other major markets, architecture is often not (exceptions include documentation for higher-risk devices with software in countries such as the U.S.).

Model Based Systems Engineering (MBSE), in particular, offers several advantages when managing compliance to the 3rd Edition. Usability engineering can be well documented through use case and sequence diagrams. These diagrams can be used (either directly or as input) for early validation activities. Physical or functional blocks considered to be user interface elements can be identified and tracked through the use of attributes. Design elements related to essential performance can be flagged as such to aid in design and prevent downstream manufacturing issues (e.g., swapping critical parts for cost savings). Figure 5 below shows examples of Model Based Systems Engineering used to model user-centric behavior.

Figure 5. Usability Definition Using MBSE



At Battelle, MBSE has been found to be quite effective when communicating with Certification Bodies (CBs), users, and other non-technical stakeholders. A thorough functional system walk-through using use case and activity diagrams helps set the stage without pouring through detailed requirements. This has helped end users and clinical experts provide early formative validation, and it has facilitated compliance assessments with Certification Bodies by allowing them to focus on meaningful activities as opposed to "getting up to speed" on product functionality.

Verification and Validation. Verification and validation results provide the evidence that the product requirements are met—including those identified through the risk management and usability engineering activities. The evidence completes the trace matrix (managed by the systems engineer), which is the roadmap central to a 3rd Edition compliance review.

Addressing Gaps in 2nd Edition Products

In most all cases, the design and documentation of a medical device designed to the 2nd Edition must change to comply with the 3rd Edition. Many manufacturers will have to perform this activity when countries and regions begin to require compliance to the 3rd Edition, particularly those regions (e.g., the EU) that do not allow existing products to be "grandfathered" in. As shown in Figure 1, the systems engineer is often the owner of design

inputs and outputs which demonstrate 3rd Edition compliance. The following subsections highlight the systems engineer's role in defining the scope and managing the implementation of changes.

Project Planning and Scope Assessment. The scale of the design and documentation deficiencies can vary widely between products; therefore, the recommended first step is to perform an initial gap assessment to identify both procedural (e.g., risk management) and design (e.g., new labeling) gaps in the current design. Experience in the evaluation of several "2nd Edition" products has shown that the primary drivers of cost and schedule will likely be:

- Essential Performance and assessment of risks outlined in the 3rd Edition will drive new risk controls, requiring product changes
- Usability engineering was limited to design validation, and will have to be assessed more fully as part of the risk management process
- Miscellaneous new design-level requirements—such as those related to alarm harmonics, fire enclosures, and/or mains supplies—may require significant device re-designs.

Unfortunately, the scope may not be fully known after the initial gap assessment, since the risk management process itself is intended to identify required risk controls. In general, the more thorough the existing risk management and usability processes are, the less potential there is for a significant risk control-related re-design.

Risk Management Process. The 2nd Edition did not specifically require an ISO 14971 compliant risk process, leaving the possibility that a manufacturer's risk management process may not strictly comply with all of the clauses of ISO 14971. In this case, the manufacturer should perform a gap analysis of their current risk management process against the specific clauses of ISO 14971 to assure that the requirements of Clause 4 of the 3rd Edition can be met. In most cases, risk assessments and traceability matrices will be in place to meet FDA filing requirements. Typical gaps are the lack of safety risk management plans and summary reports.

In addition, a gap analysis should also be performed to determine where the existing risk management file does not explicitly demonstrate that all clauses where inspection of the safety risk management file is required have been addressed as part of the safety risk management process. As stated in the previous section, an additional checklist will be required to show which clauses are not applicable, and which clauses that are applicable have not been specifically addressed in the existing risk assessment documents. If a clause is applicable, even though the associated risk was so low as to warrant no specific consideration in the past, it must be evaluated in the risk assessment process as evidence that the associated risk was evaluated.

Essential Performance. Because it was not required, the manufacturer may not have determined essential performance for their existing products, so the analysis described in the "New Product Development" section will have to be carried out. Even if essential performance is known, it may not be documented in the risk management file, so that risk management file documentation will have to be updated with the process and findings of the essential performance evaluation.

Usability Engineering. Since a usability assessment was not required in the 2nd Edition, most manufacturers will have gaps in their design history file for usability. If usability was considered as part of the initial development process, addressing the gaps may be as simple as creating a "pointer" file referencing existing documentation. If usability was not considered (aside from design validation), activities may be more significant and include both formative and summative user validations. Often, the systems engineer will lead the safety risk management portion of usability engineering, while more specialized individuals (e.g., human factors engineers or cognitive psychologists) may lead formative usability studies.

Conclusion

The 3rd Edition represents a significant change in the way medical devices have been developed. Compliance has shifted from a test-based approach to a process-based approach. Compliance now requires a systems perspective to ensure safety risk management and usability engineering is considered and integrated throughout the development lifecycle. The systems engineer is the ideal candidate to manage the interfaces between the end users, engineering, regulatory, human factors, and project management, and implement a methodical approach to comply with the standard in a cost-effective manner while ensuring safety and effectiveness of the device.

References

Haskins, C., ed. 2010. *Systems Engineering Handbook: A Guide for System Life Cycle Processes and Activities*. Version 3.2. Revised by M. Krueger, D. Walden, and R. D. Hamelin. San Diego, CA (US): INCOSE.

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

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

———. IEC 60601-1 *Medical electrical equipment - Part 1-6: General requirements for basic safety and essential performance - Collateral standard: Usability*, IEC, 2010.

———. IEC 62366 *Medical devices -- Application of usability engineering to medical devices*, IEC, 2007.

Biography

Chad Gibson is a Systems Engineer with Battelle's Health and Life Science's Medical Device Solutions group. His experience spans systems engineering, product development, Design for Six Sigma (DFSS), and hardware design. He has assessed multiple medical devices to IEC 60601-1:2005. He graduated with a B.S. in Electrical Engineering from The University of Cincinnati in 2002. He is a member of INCOSE and is the co-lead for the biomedical model-based systems engineering (MBSE) project.

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.

Felicia Hobson has over 10 years of experience in the design, development, and testing of

medical products at Battelle. She has led design teams of complex electromechanical systems from concept generation through integration and verification. Her experience spans project management, systems engineering, hardware design and development, and product testing. She earned a Bachelor of Electrical Engineering degree from the University of Dayton in 2000 and is a member of INCOSE.