July 2011
Volume 5, Issue 7

MEDICAL DEVICE RISK MANAGEMENT

Diablo Mountain Research Limited Liability Corporation (925) 256-0161

Risk Management with Diablo Mountain Research LLC:

- DMR has experience with full product life cycle Risk Management for Medical Devices and Software.
- The DMR has applied Risk Management techniques to a variety of Class II and Class III medical devices.
- DMR has expertise with FEMA, FEMCA, and FTA techniques as outlined in the ISO14971.
- DMR is up to speed with contemporary standards guiding medical device design and deployment such as the IEC62304, IEC61010-1, and IEC60601-1 3rd edition.
- DMR recommends FEMA techniques for Class III devices.

White Paper Highlights:

Introduction to Risk Management for Medical Devices

By S.E. Nickols III

Risk Management has become an unavoidable requirement as part of the process of developing Medical Devices. This white paper provides an introductory overview to Risk Management and Risk Analysis techniques that can be applied to medical devices.

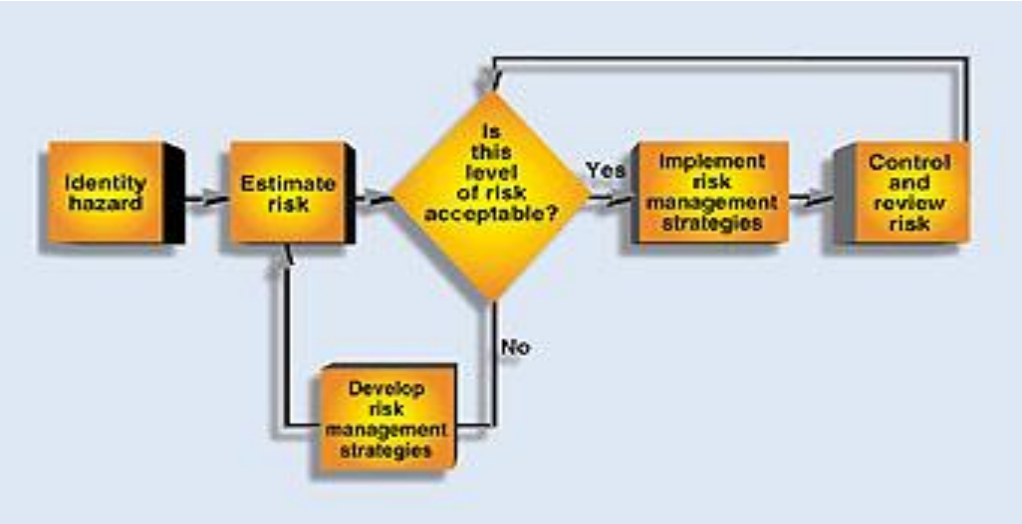
The FDA's quality system regulation (QSR) is intended to give manufacturers ***"the flexibility to determine the controls that are necessary to be commensurate with risk."*** The FDA sees risk analysis as an essential requirement of this regulation. The FDA gives little guidance on specific risk analysis approaches and procedures such as **Failure Mode and Effects Analysis** (FMEA) or **Fault Tree Analysis** (FTA).

In considering an approach to risk analysis, a medical device manufacturer, may find value in what other industries, including the automotive, aerospace, and defense, have learned about reducing risk. Medical device companies can manage and reduce risk more effectively by including "***risk planning"*** as early as possible in the design/development process. Revisiting risk issues systematically throughout the development and manufacturing process is a requirement to be compliant with the IEC62304 and IEC60601-1 3rd edition.

Overview of Risk Management

An overall risk management process involves the essential steps in Figure 1. In order to manage risk, hazards must first be identified. By evaluating the potential consequences of hazards and their likelihood, a measure of risk can be estimated. This value is compared to the company's risk-acceptability criteria and, if it is too high, the risk needs to be mitigated.

Figure 1. Sample flowchart showing risk management of identified hazards.



"***Early and continuous evaluation of a medical device's hazard potential increases the likelihood of correcting these faults and producing a device with a low probability of causing harm.***

Managing Risk

Risk with a medical device cannot be completely eliminated; the risk that remains must be managed. The following steps can be used in a risk management program:

- Write a Risk Management and Assessments Plan.
- Develop written definitions of what needs to be done and how to do it.
- Define responsibilities and accountability.
- Define what needs authorization and who is responsible for handling it. Risk Management involves a cross functional team approach.
- Define the skills and knowledge necessary to implement the Risk Management system and a provision for training those who do not possess these skills.
- Develop and maintain written "Standard Operating Procedures" (SOPs).
- Demonstrate conformance to policies and procedures.
- Incorporate measures to cross-check and verify that procedures are followed. (Traceability)
- Verify that systems are in place and functioning properly. (Periodic reviews and Audits)

Many medical device companies have good hazard and risk assessment programs. However, effective risk management throughout the product life cycle is not always in place. The ISO14971 standard calls out for continuous and planned Risk Management for Medical Devices throughout the duration of the device life cycle.

Risk Management Techniques

"The ISO14971 is the "Defacto" Standard for Risk Management as applied to Medical Devices.

HAZARD ANALYSIS

Before a final design has been developed, a ***"preliminary hazard analysis"*** can be conducted to establish the baseline hazards associated with a device. In essence, the analysis consists of listing the major components and operating requirements of the device and evaluating potential hazards. The components and operating requirements could include raw materials and wastes, hardware, monitoring and control systems, human-device interfaces, services, and the operating environment.

Some potential hazards that may need to be evaluated include are toxicity, flammability, reactivity of raw materials, and bio hazardous wastes. Take into consideration sensitivity to environmental factors such as temperature and humidity. Mechanical or electronic hazards; and human factors associated with the operator/device interface should be considered. The patient-device interface can also be hazardous because of unsafe or ineffective delivery of energy, administration of drugs, or control of life-sustaining functions. Also, incorrect information could lead to a misdiagnosis or wrong treatment or therapy being ordered.

When conducting a preliminary hazard analysis, ***use a "what-if" or "brainstorming approach"*** to identify possible failures. Evaluate potential consequences, and develop risk management strategies. These strategies lead to an improved lower-cost design. Generally, failure scenarios can be prioritized by the severity of each hazard.

At this stage, there is often insufficient detail to evaluate hazard likelihood accurately. However, comparisons may be made with similar devices and their histories in the medical device reports. An evaluation revealing severe hazard potential may prompt a radical change in the conceptual design. ***The goal is to eliminate all high-severity hazards and reduce as many medium- and low-severity hazards as possible.*** There is considerable flexibility at this early design stage. Major changes can make the device inherently safer at minimal cost. For example, if use of a chemical was determined to be a significant hazard, other less-toxic chemicals or a diluted form of the original chemical might be a reasonable mitigating measure.

During prototype development, more detailed hazard and risk analysis can be performed. At this stage of design, mechanical drawings and electrical schematics are available. The basic process operations have been defined. The device and its operation can be reviewed by a number of analysis techniques, including top-down and bottom-up approaches. A hazard and operability (HAZOP) study is a bottom-up approach ideal for new or complex designs involving a number of process steps. A HAZOP is conducted on individual steps, each of which has design intent.

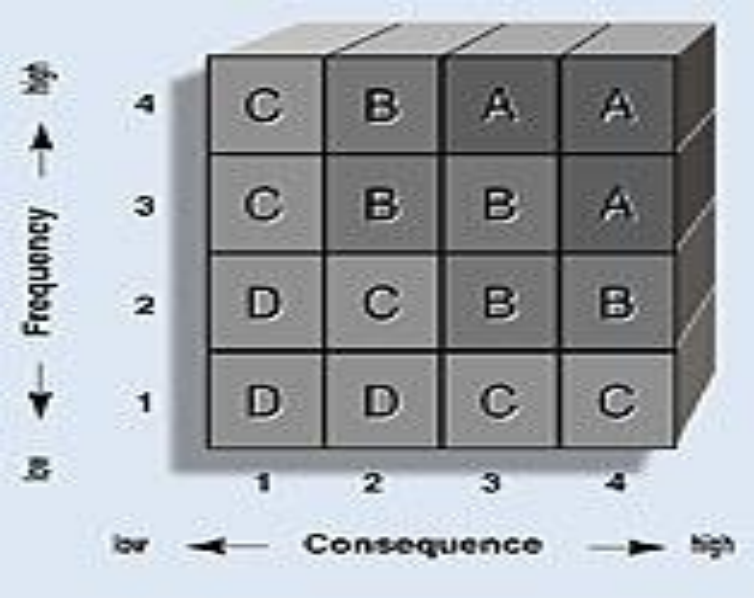
A simple HAZOP example: The **t**ransfer of 100 ml of saline solution from a bulk container to a blending container could be one step of the process for preparation of intravenous solutions. Deviations from the design intent are explored by applying a series of guide words to applicable design parameters, as shown in Table 1.

Table 1. Guide words used to determine deviations from design intent.

Design Parameter	Guide Word
Flow Temperature Pressure Level/weight Composition Reaction Time Sequence	More Less None Reverse Part of As well as Other than

If the deviation defined by the combination of a design parameter and guide word (e.g., more flow or less flow) can result in a hazard, potential causes and any existing controls are identified. The risk level can be evaluated using a risk matrix in which consequence and frequency ranges have been established according to a "***company's internal risk-acceptability criteria"*** (Figure 2). Those deviations that have category A or B risks should be reduced to level C or D risks.

Figure 2. Any item falling into high risk categories (A or B) should be redesigned.



Failure Mode Effects Analysis

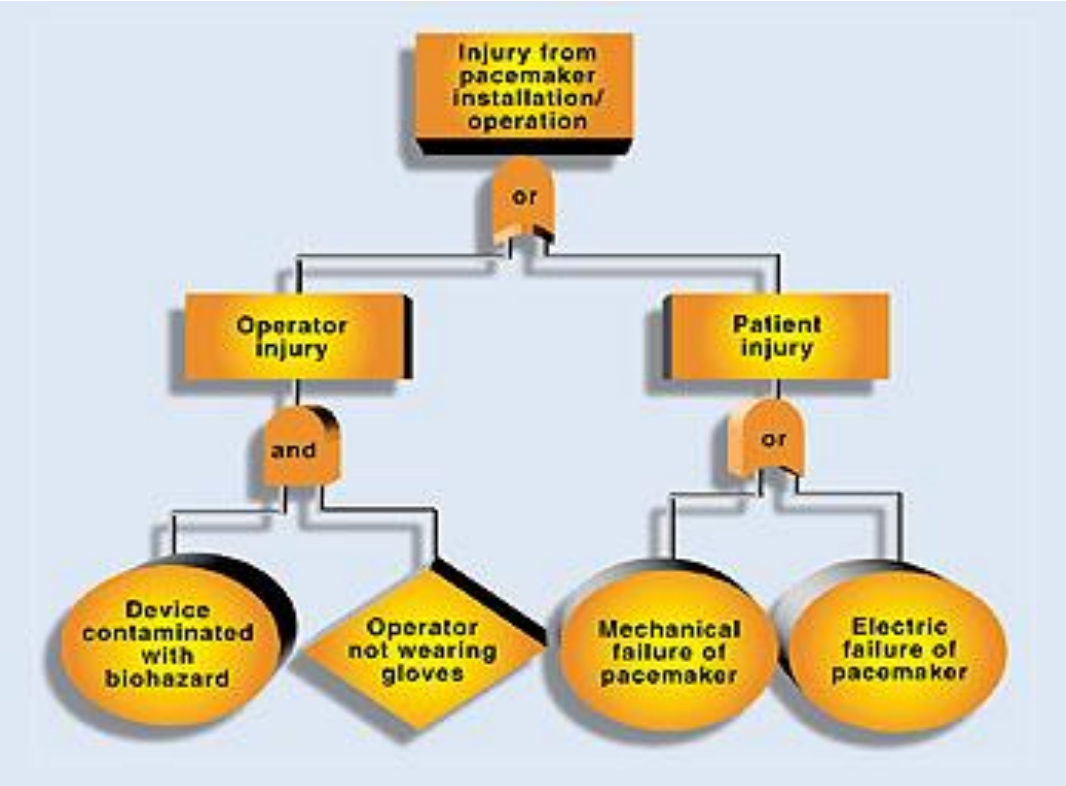
When a device contains many mechanical or electrical components, a FMEA (or FEMCA) should be considered. FMEA is time-consuming technique and is generally applied only to Class III devices or to the safety critical portions of class II devices. The FMEA is a bottom-up approach that focuses on a particular component of a medical device and explores the various failure modes that can occur. For each failure mode that results in an undesirable consequence or sequence of events, potential causes and existing controls are evaluated. The level of risk can be determined by using a risk matrix. (See reference 5)

Compliance with the IEC62304 and IEC60601-1 3rd Edition standards require Risk Management as outlined in the ISO14971 standard.

Fault Tree Analysis

"Fault Tree Analysis" is an effective top-down approach. The Risk Management team starts with the undesired consequence or top level event and identifies the initiating and contributing events that must occur to produce it. These events are combined using logic gates. A logic gate is the point at which two or more independent events are combined in order to produce a higher-level event. The logic gate determines whether the sub event probabilities or frequencies should be multiplied, with an AND gate, or added with an *OR* gate. If all events under a gate are necessary for the higher event to occur, an *AND* gate is used. If each of the events is sufficient to produce the higher event on its own, an *OR* gate is used. Both mechanical failures and human errors can be included in a fault tree. An example of a partial fault tree for a pacemaker is shown in Figure 3.

Figure 3. A partial fault tree analysis for a pacemaker.



If failure rates for each event on a fault tree are available or can be estimated from generic data, the top-event frequency can be calculated and compared to a company's internal risk-acceptability criteria. ***A fault tree is a powerful risk-analysis tool, but its greatest limitation is the availability of relevant failure data.*** Therefore, fault trees are generally best used to compare risks of various alternatives. The greatest benefit of a fault tree is that events that contribute most frequently to the top event can readily be identified, and mitigating measures can be focused on reducing the frequency of these events.

PROCEDURE ANALYSIS

Although HAZOP, FMEA, and FTA allow evaluation of human errors in design, operation, and maintenance of medical devices, it is often desirable to conduct a separate analysis focused on procedures. Typically, a **"what-if approach"** is used for this type of analysis. Procedures are grouped into **"process steps"** similar to those study sections used with **HAZOP**. Each process step is evaluated to determine if an undesirable consequence could result from incorrect procedures.

"***Checklists"*** are the simplest tools for conducting design reviews but are generally not sufficient. The true benefit of checklists is to support the other techniques described previously. For example, a checklist of potential hazards identified in previous reviews or from incidents associated with similar devices would be useful during a design review. After completion of the review, the checklist can be examined to ensure that the study evaluated all previously identified potential hazards. For example, during a HAZOP, possible human errors are evaluated; however, as a final check, a human-factors checklist is often used.

The risk analysis should include any risks associated with the manufacture and delivery of the device to its intended location. For devices that involve solutions or components that can be degraded by environmental factors (e.g., heat, humidity, cold, or light), storage and transportation methods need to be reviewed. Identified problems could lead to changes in packaging or warnings on storage or packaging containers.

It is important that any changes made during the design process be reviewed to ensure that safety hazards are not being introduced into the design. Small changes are generally reviewed using a "what-if approach", whereas larger changes may require a HAZOP or FMEA.

A final design or prestart-up review should be conducted before starting production. Extensive checklists ensure that all design specifications have been met and all previous design review recommendations have been addressed. The final design review should also include a physical inspection of the device in its intended workspace (e.g., laboratory, hospital, doctor's office) to identify any issues not readily apparent from looking at drawings, such as location of vents and drains, accessibility for maintenance, pinch points, and sharp edges. An ***" action item list"*** (findings or observations developed during a safety or design review) of final action items is typically generated and prioritized into items that need to be completed prior to start of production and others that can be incorporated into the next model.

Software used to control or monitor a medical device also needs to be reviewed. Software can be grouped into its primary functions (e.g., start-up, treatment, diagnostics, and maintenance) just as procedures can be grouped into process steps. Three generic sub functions are evaluated for each primary function:

- Function: The software component does not perform its intended function correctly per its original design intent.
- Timing: The software component performs its function at the wrong time.
- Data: The software component performs its function using incorrect or corrupt data.

Software errors can produce unexpected consequences, particularly those that involve corrupt data or false alarms. It is important to have a means of detecting software errors or a means to detect the effects of software errors on a device. For example, a software error resulting in a failure of the alarm notification system would disable all alarm systems. Separate redundant alarms or interlocks on critical aspects of a device need to be considered.

"The IEC62302 is the "Defacto" Standard for Life Cycle Management as applied to Medical Device Software. The FDA pushed for this standard to be ratified.

Conclusions

All of the techniques described in this white paper have been are referenced in the ISO14971 standard and have successfully used in design reviews of medical devices. FTA is being used by pacemaker manufacturers based on the FDA guidance for software aspects of 510(k) notification submissions for medical devices. Other computer-controlled medical devices will also need to be reviewed using FTA as a primary risk analysis tool.

For mechanical devices that are used away from the patient, such as plasma and blood viral inactivation devices, as well as devices for preparing intravenous solutions, an FMEA is a reasonable choice. However, for associated activities such as preparation of disposables, which are manual operations, a **"what-if approach"** is preferred. FMEA is used frequently with Class III surgical instruments.

The key to successful risk management in medical device design is to start early. As soon as conceptual designs are available, the risk management process can begin. A preliminary hazard analysis can be useful in selecting the concept with the highest level of inherent safety. Later, as the design is developed, design reviews at key points in the development process will allow changes to be made without significantly affecting the project schedule. The further along in the design process that changes are identified, the fewer choices are available to mitigate hazards without significant schedule implications.

Generally, risk management activities will identify opportunities to improve device performance. The benefits of conducting risk analysis during medical device design can be significant and can be used to offset some or all of the cost of implementing risk-mitigating measures. There is always a trade-off in how to manage risk. Hardware or software controls are generally viewed as more effective since they are more reliable than humans. However, since there is need for human interaction in the operation of all medical devices, the element of risk needs to be adequately evaluated. Minimizing the level of routine human intervention will reduce risk and improve efficiency. Such risk reduction must be weighed against the cost of automating tasks that can be performed by individuals.

REFERENCES:

1. Code of Federal Regulations, 21 CFR 820.
2. ISO14971-Application of Risk Management to Medical Devices.
3. IEC62304- Medical device software -Software life-cycle processes.
4. IEC60601-1 3rd Edition- Medical Electrical Equipment - Part 1: General Requirements for Basic Safety and Essential Performance.
5. IEC 60812- Analysis techniques for system reliability – Procedure for failure mode and effects analysis. (FMEA)
6. IEC61025- Fault Tree Analysis.(FTA)
7. DMR White Paper: "Risk Planning and Risk Quantification".

Diablo Mountain Research LLC

741 Buena Vista Place
Suite 10
Walnut, CA 94597

PHONE:
(925) 256-0161

E-MAIL:
science.dmr@gmail.com

We're on the Web!

See us at:

www.diablo-mountain-research.com

About Diablo Mountain Research LLC

Diablo Mountain Research was founded in September 2005 to serve the needs of fledgling medical device startup companies, inventors, and supply chain vendors. Diablo Mountain Research fills a gap that large and "expensive" Medical Device consulting firms seem to avoid. We serve customers with real budgets and tight time constraints.

Quotes to work by:

"With any Medical Device Product sold in the USA; Innovation, Creativity, and Patient Value are all meaningless notions unless the product is designed and manufactured in tune with the FDA QSR. Risk Management is a vital tool for a Medical Device Manufacturer's success."

"Compliance with the relevant standards is essential to the success of any medical device."

"Risk Management, by it's very nature, takes the rule of the Dice (Probability theory) away from "hopefull" design intent, and places control firmly into the hands of the design team." SEN circa 2012.