Value-Added Medical-Device Risk Management

Carl Schmuland

***Abstract*—The assessment of overall residual risk is the primary objective of performing risk-management activities and is required by ISO 14971:2000—Application of Risk Management to Medical Devices. Despite this requirement, much confusion remains among medical-device manufacturers and the various regulatory-approval bodies as to what is required. Today, many medical-device manufacturers do not formally address the subject. This paper will address the following questions: 1) What is overall residual risk? 2) Why is overall residual risk the most important measure of safety throughout the product life cycle? 3) How can overall residual risk be estimated? 4) What is an acceptable level of overall residual risk? 5) How can the concept of overall residual risk be used to manage safety after the product has been released?**

This paper will provide practical ideas that will allow medical-device manufacturers to begin assessing the overall residual risk of their products, and may also be helpful to regulatory bodies in formulating and communicating a consistent set of expectations. The concepts developed in the paper should be applicable to evaluating the safety of a wide variety of products as well.

***Index Terms*—Design input, design output, design transfer, harm, hazard, hazardous situation, ISO 14971:2000, overall residual risk, post-production, residual risk, risk analysis, risk control, risk evaluation, risk management, quantitative residual risk.**

IS RISK management just another fad or can it be a value-added activity beyond the need to satisfy a regulatory requirement? Based upon 27 years of experience in developing medical products, my answer is that, done properly, risk management can powerfully complement the overall product-development process. Product development focuses on efficiently designing a product that meets its design requirements. Risk management improves the overall process by identifying how the product could fail to meet the customer's requirements. In effect, risk management is another technique that enhances design robustness.

Risk management works best when it is integrated into the product-development process rather than being a separate process. At the present time, International Organization for Standardization (ISO) 13485:2003 has explicitly integrated risk management into the overall quality-system requirements, while the Food and Drug Administration (FDA) strongly implies the link in their Quality System Regulation. Recognizing there is no single agreed-upon recipe that will work for every company and product type, this paper will suggest some principles to help the reader tailor a risk-management process for their individual needs.

In order to create a value-added risk-management process, three important ingredients are required. I like to think of these as three legs on a stool. If one or more legs are missing, the stool falls over. First, the process philosophy must assure that the intent of the process is not lost in the details, nor does the process become so onerous that it is impractical. Second, process content must require a basic set of deliverables that actually add value. Third, the people who perform the activities must bring a certain esprit de corps, based upon some common characteristics that transcend the technical execution of the activities.

I. Process Philosophy

Albert Einstein observed that "The mere formulation of a problem is far more essential than its solution, which may be merely a matter of mathematical or experimental skills" and that "everything should be as simple as possible, but not too simple." We live in a world in which we are bombarded every day with the deception of "too simple" fixes for every imaginable problem. Let us be honest, there is no magic process that will work for every company on every medical device. The challenge before each medical-device organization is to formulate a process solution that is as simple as possible, but not too simple. In keeping with the spirit of "as simple as possible," this section will discuss some dos and don'ts to consider when defining what the author considers to be the most important elements of good process philosophy.

Governments exercise their responsibility to maintain order in society by a wide variety of means, one of which is the development and enforcement of regulations to guard against unsafe medical products. In today's world, one of the ways this has been accomplished is through the release of ISO 14971:2000. Compliance to this standard is required to sell medical devices in Europe, Canada, and Australia. Within the United States, the standard is recognized by the FDA as a way to meet the intent of the Quality System Regulation requirements for the development of safe medical products. Unfortunately, responsible organizations often overreact to these kinds of regulations, even though they have nothing to fear from the governments involved, and create overly elegant and detailed processes that they cannot practically follow. Internal-compliance audits that focus on the minutia and not the big picture often exacerbate the problem and lead to more, not less, process requirements. Ironically, the net result is that the organization can get into trouble with a regulatory body, despite their initial good intentions, because they are unable to follow

Manuscript received August 2, 2005.

The author is with the Safety Engineering Department, Medtronic, Minneapolis, MN 55432 USA.

Digital Object Identifier 10.1109/TDMR.2005.857860

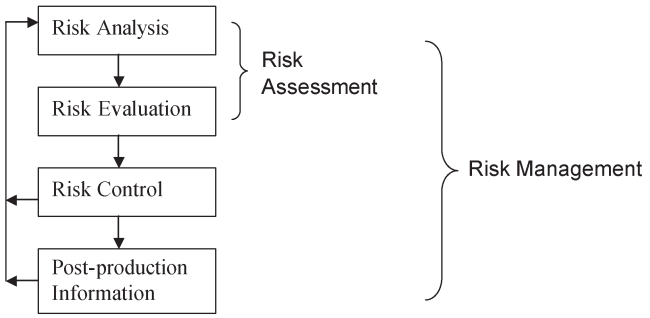


Fig. 1. ISO 14971:2000 schematic representation of the risk-management process.

their own process. The following guidelines are a starting point for integrating a practical risk-management process into your overall development process.

1) Detailed processes work best when you are trying to exactly reproduce an item (manufacturing) or offset a lack of skill. Product development is the opposite of this. You can get a consistent meal at your favorite fastfood restaurant, but if you really want an excellent meal, you go to a restaurant with a chef who does not use an off-the-shelf cookbook! The chef's meal is analogous to product development: Product development tries to make outstanding unique product designs using highly skilled people. It is more about craftsmanship than production. Relegating product development to an overly detailed process is more likely to achieve mediocrity (or worse) than excellence by stifling creativity. Too much detail is particularly dangerous when safety is involved. Reliance on a checklist mentality can lead to disastrous results when safety issues with a new product do not fall neatly into the checklist.
2) Too much process detail leads to an exorbitant number of tasks and deliverables that requires the expenditure of inordinate resources to track progress against the project schedule. Too many steps deflect the organizations energy away from essential activities. Ask of every process step if it adds any value.
3) On the other hand, too little process leads to confusion within the development team as it searches for the right combination of deliverables to satisfy regulatory bodies. Startup organizations with breakthrough technologies led by a visionary personality or initial attempts of a mature organization at outsourcing designs are particularly vulnerable to having too little process.
4) The ideal process should provide only a framework and enable you to document what you do in a format and words that mirror the applicable regulations and assure that quality, regulatory, and business needs are met. Organizations must find the balance point between seeing the big picture, while including enough detail to assure consistency and efficiency in bringing the project to a successful conclusion. Writing such a process requires a blend of visionary and detail-oriented personalities.

II. Process Content

At first glance, ISO 14971:2000 may appear as an overly detailed process. However, on closer inspection, it only lays out a framework and minimum boundaries. Given the importance of ISO 14971:2000 in the eyes of regulatory bodies, it is only prudent to structure your risk-management process around the framework and terms laid down in the standard. The process recommended by ISO 14971:2000 is shown in Fig. 1. The terms are defined by ISO 14971:2000 as follows.

Risk: Combination of occurrence of harm and the severity of that harm.
Harm: Physical injury or damage to the health of people, or damage to property or the environment.
Risk Analysis: Systematic use of available information to identify hazards and to estimate the risk.
Risk Evaluation: Judgment, on the basis of risk analysis, of whether a risk that is acceptable has been achieved in a given context based on the current values of society.
Risk Control: Process through which decisions are reached and protective measures are implemented for reducing risks to, or maintaining risks within, specified levels.
Postproduction Information: Systematic procedure to review information gained about the medical device or similar devices in the postproduction phase.
Risk Assessment: Overall process comprising a risk analysis and a risk evaluation.
Risk Management: Systematic application of management policies, procedures, and practices to the tasks of analyzing, evaluating, and controlling risk.
Residual Risk: Risk remaining after risk control measures have been taken.

A. The Essential Product-Development Risk-Management Process

From a practical perspective, the ISO 14971:2000 process can be reduced to the process depicted in Fig. 2.

There are several important points to be considered.

1) There are really two parts to the risk-management process: Activities that are performed during product development (depicted in Fig. 2) and periodic review of the actual field performance.
2) Management should be involved in decision making regarding the acceptability of residual risk throughout the product-development cycle. There is no point in knowing about a residual-risk issue early in the product-development cycle and then waiting until the product is ready for first human use to alert management to the issue.
3) What really counts is what actually happens in the field. Therefore, activities during product development are aimed at understanding the residual risk remaining after all risk-control measures are implemented.
4) During new product development, actual field performance of similar products should be leveraged whenever possible to assure accurate residual-risk evaluations and to avoid unnecessary evaluation of residual risk for which actual field performance already exists.

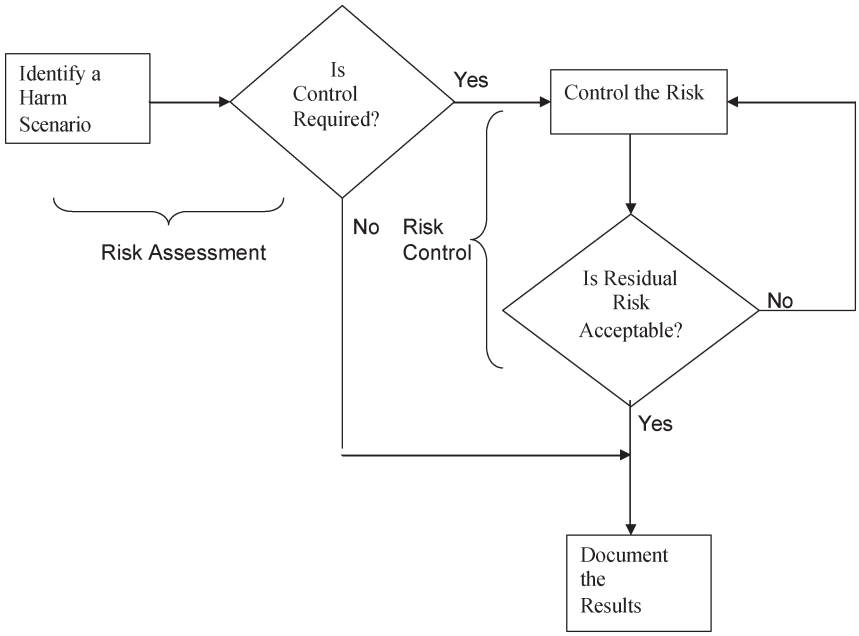


Fig. 2. Essential product-development risk-management process.

5) Periodic review of actual field performance should be primarily driven by other parts of the quality system, such as field-performance monitoring and corrective and preventive actions (CAPA). Risk management should be part of the quality-system periodic reviews to assure field information is fed back into the product-development cycle as appropriate and that field issues are properly addressed from a Risk-Management perspective.

B. Performing Risk Management Throughout the Product-Development Cycle

Before unpacking the process depicted in Fig. 2, consider the following example. Suppose someone runs a red light and collides with my car in an intersection, I could be killed, or have my leg broken, or be bruised, or maybe I was not injured at all, but my car was damaged to some degree, or my full fuel tank ruptures sending 10 gallons of gasoline into a stream. The person running the red light has created a hazardous situation. This, of itself, does not cause harm, unless my car is hit and then different severities and types of harm can result. For example, in the category of physical injury, severity can range from death to a broken leg, to bruises, to no injury at all. Property damage or environmental damage may also result in varying degrees. My car could be "totaled" or just suffer a dented fender; my gasoline tank could rupture and the gas spill into the spawning grounds of an endangered species of fish; or be contained in the roadway; or the tank may not rupture at all. This simple example illustrates some basic principles encountered when performing risk management.

1) We cannot avoid all hazardous situations, but exposure to a given hazardous situation does not necessarily result in harm. In the example above, running a red light is hazardous (a potential source of harm), but other things must also happen for harm to occur.
2) When harm occurs, the severity and type of harm can vary. The number of harm scenarios that could result from just the example of running a red light is limited only by the imagination of the person identifying the scenarios. In addition, there are unlimited numbers of other hazardous situations, such as brake failures, or icy roads, or drunk drivers, etc., which can translate into unlimited numbers of harm scenarios.
3) Harm does not always occur because there are usually a number of risk controls in place that limit the probability and/or severity of the possible harm. For example, there are hundreds of laws governing proper driving behaviors, police who enforce the laws, signs that warn of hazards, traffic lights and stop signs, driver's tests, safety equipment on vehicles, etc., not to mention all the emergency workers employed to intervene when harm does occur so that the severity of the harm may be limited. Unfortunately, all of these are imperfect, and sooner or later all the controls may fail in a given a scenario resulting in harm.
4) The overall residual risk ultimately is most important, i.e., the sum of all the probabilities for a given severity of harm (death for example). We perform risk management by evaluating each individual harm scenario (running a red light). However, there are many harm scenarios. No one wants to simply avoid death in an intersection accident. They also want to avoid death in accidents caused by icy roads, or by brake failures, or the myriad of other types of accident that can occur.

What does all this have to do with Fig. 2? Starting with the first box, as many harm scenarios as possible must be identified. However, since risk is the probability of occurrence of the harm and the severity of the harm, not all scenarios need to be followed through to controlling actions. Therefore, at the first diamond, the individual-harm-scenario risk is judged to

be either acceptable or unacceptable. Of those that are judged as unacceptable (first diamond), additional controls are put in place and the remaining risk is evaluated to determine if it is acceptable (second diamond). Controls are added until the harm scenario is reduced to a safe level (defined as freedom from unacceptable risk).

What is an unacceptable level of risk can be difficult to determine and is highly dependent upon individual values. In the United States, people rarely limit their driving for safety reasons, even though about 1 per 6200 people are killed annually in traffic accidents. This risk is judged to be acceptable based upon current values. However, at some time, a technological breakthrough may occur, making a risk of 1 per 6200 annually unacceptable.

Having, hopefully, clarified the concepts, let us get more specific and focus on medical products. Most of the time, a new medical product is preceded by a similar product that is normally judged to be safe. As a result, risk-management activities for the new product can focus on the differences between the previous and new product. This can significantly reduce the effort required, but it comes at the price of truly understanding the field performance of the previous product and documenting why the field performance is acceptable.

The determination of acceptable risk is a very important attribute of a medical-device risk-management process. This determination is left to the individual manufacturer. Regulatory agencies and ISO 14971:2000 are silent as to what is acceptable. Usually, it is best to evaluate the overall residual risk of a product from the perspective of the manufacturer, because the manufacturer bears the risk of every product made for the entire life of each product. Minimizing this risk will result in the lowest possible risk for the individual patient, the health professional, and the health care institution. In this case, the measure is the total number of injuries for each of the specific harms being evaluated over the entire field life of every released product. The measurement is made by estimating the probability of harm occurring on a given patient use (which could vary from seconds for a digital thermometer to years for an implanted device) multiplied by the expected total number of uses. Normally, a manufacturer should set a trip point that requires a management review when the total number of injuries exceeds the trip point. Exactly what trip point is selected depends upon the severity of the harm. Given all the interest today in Six Sigma, selecting a trip point based on these concepts might be acceptable, depending on how the measurement was stated. For example, meeting Six Sigma for the risk of electrocution from an ECG machine would be completely unacceptable (3.4 electrocutions per 1 000 000 ECGs), but Six Sigma for death within 30 days of an aortic-valve replacement would exceed current best practices. This points out that to some degree the trip point will be limited by best practices and or technology. Whatever trip point is selected, it is very important to justify why the trip point is acceptable.

The above discussion implies that the residual risk estimation is quantitative. Strictly speaking, ISO 14971:2000, or regulatory agencies, do not require a quantitative system. However, there are a number of reasons why a quantitative system is the best choice for your organization. The most practical and straightforward of these is that once your product is released to the field, any harm scenarios associated with it will occur in a definite quantity. Since Risk Management is attempting to limit the occurrence of harm, it only makes sense to estimate how many harm scenarios will occur, so that there is a way to assess the effectiveness of the Risk Management system. The second important reason is that if several harm scenarios are identified that lead to a particular harm (death for example), it is possible to add quantitative estimates, but qualitative estimates cannot be added and compared later to actual results. Using a qualitative system will limit your ability to assess field performance once the product is released to the field. On the other hand, use of a qualitative system is practical during risk assessment where the decision comes down to whether or not additional controls are needed.

Focusing your efforts in the most important areas is a key to successful risk management. You cannot afford to get bogged down with scratches when deaths can occur. A good method to sharpen your focus is to link your risk-management system to your complaints system. You probably have good criteria for filing medical-device reports (MDRs). Use the same criteria to define the significant issues you want to address with your risk-management system. If your complaint system also categorizes lower level issues, you could use these same criteria to define less severe harms to be addressed by the risk-management system.

Another important consideration is the method selected for the controlling action. The preferred method is always a design change controlled by specifications subject to verification as part of design controls. Beware of the trap of using labeling as a controlling action. Building a case for a safe product based upon the user following detailed labeling is a tenuous solution at best. Such controls are often limited in their effectiveness. However, there are some instances where labeling is the only practical method to achieve a safe result, for example, instructing everyone to stand clear of a patient receiving an external defibrillation shock.

An additional concept that is very important to consider is that it is possible to make a medical device long before all the science surrounding the device is understood. Blood transfusions are a good example of this concept. The first transfusions were performed in the early 1800's by connecting a tube from a donor's artery to a vein in the patient. This very inconvenient technique did appear to work in some cases, but the success rate did not offset the difficulty of the procedure and by the mid-1800's, the technique was no longer used. Then, in the early 1900's it was discovered that there were four types of human blood. Armed with this new information, transfusions were tried again, only blood types were matched and, of course, the success rate soared. This, in turn, eventually led to the sophisticated system we have today for storing blood. The point is that it was relatively easy to conceive of an apparatus to connect a donor's artery to a patient's vein to treat hemorrhage. Based upon the luck of the draw, blood types were matched some times and the procedure worked, but there was a huge piece of missing information, there are four types of human blood that must be matched! The same thing can happen today, in which a product can be developed

to meet a medical need, but not all the science is understood. Serious safety implications can arise in such circumstances. For example, suppose the missing information is a characteristic of a material used in a medical device. It could be very easy to receive multiple lots of the material in which the unspecified characteristic falls within acceptable bounds. Eventually, a lot is received in which the characteristic is outside the bound. When field problems arise, the ensuing investigation then discovers the missing information.

The task of actually performing the risk-management process in Fig. 2 can be accomplished by the following five-point strategy:

1) *Identify all the important scenarios:* Fallible human beings will never identify every possible scenario, but it should be possible to discover, the most severe and probable ones. A useful approach is to consider three categories of scenarios and creatively work through the process in Fig. 2 for each of the categories. The three categories are:
   a) Design Input: If you could consistently build products that meet the design input specification, would they be safe? There are two types of issues to consider:
      i) The specification of the product must not have any systemic safety issues designed into the product and must be complete enough that all safety requirements are specified.
      ii) Determine how the product could be improperly used or misused in a manner that compromises safety?
   b) Design Output: A perfectly specified product can still be a safety issue if it is not designed correctly. Two questions are important:
      i) Have any systemic failure modes been introduced because of the design implementation? In other words, are there scenarios that will always result in harm. Product operation that requires a particular sequence of events and/or logical decisions to result in safe operation are particularly vulnerable.
      ii) Is the product sufficiently reliable so that safety is not compromised because of "random" failures of the hardware.
   c) Design Transfer: ISO 14971:2000 does not specifically require a manufacturing analysis, but a perfectly specified and designed product with no safety issues could result in a huge safety problem if it were manufactured incorrectly. Therefore, it is important to consider how manufacturing the product could introduce product failure modes that result in harm. A good way to proceed is to leverage the manufacturing failure-mode effects analysis (FMEA) to identify scenarios that could compromise the safety of the product.
2) *Identify every possible scenario that could still cause harm after all control measures have been taken:* This key step has a lot of work that lies behind it (Fig. 2). The whole process begins by first identifying every possible scenario that could cause harm. The risk of each scenario is usually evaluated qualitatively to determine which ones either cause such minor harm or are sufficiently improbable that they can be disregarded. Any scenarios that remain following this step are then subjected to additional controls to either eliminate the scenario altogether, or reduce the probability of it occurring. Usually, it is not possible to reduce the severity of the harm. If the scenario has not been eliminated, then the residual risk for each scenario must be evaluated. If the residual risk is not acceptable, further reduction is required. Therefore, the only scenarios that make it through the process in Fig. 2 have each been reduced to an acceptable level of risk. Concluding that a risk is acceptable via a risk–benefit argument should be used cautiously and infrequently. Keep in mind that risk–benefit arguments will not pass muster if someone has a better product or if an entirely different treatment exists with at least comparable success, but without the risk (for example medication versus a device). According to ISO 14971:2000, risk/benefit can only be used when the risk is unacceptable, and cannot be reduced to a normally acceptable level, but that there is a substantial benefit. Normally risk/benefit will only be applicable with breakthrough products for which there is no other viable treatment for a serious medical condition. In this case, quantify benefit by the same method used to quantify risk when making the evaluation.
3) *Estimate the residual risk:* In order for harm to occur, some sequence of events must take place. Once the sequence of events is understood, a probability is assigned for each step in the sequence. Generally, there are three categories of events.
   a) Product specific: These factors are specific to the operation of the product but do not include use issues. As the device manufacturer, you will likely have good information regarding probabilities for most of these items. Examples are the percent of defective components, probabilities of encountering a systemic design error, etc.
   b) Medical information: There is usually a wealth of information about patient medical conditions or factors. Examples are the percentage of patients with a specific medical condition in combination with other exacerbating circumstances, likely medical consequences of exposure to given device failure, etc. This information is likely to be quite accurate.
   c) User behavior: Usually, there will not be a lot of information available as to how a user might respond in a given situation. For the most part, this comes down to expert opinion (field staff, customer service, etc.). The best guidance is to get many opinions, throw out the high and low and average the rest. Recognize that the more improbable an event is, the harder it is to estimate. In these cases it is best to focus the expert opinion by asking questions like is it 1/1000, 1/1 000 000, etc.? Examples are the percentage of users who would take specific action in the presence of device failure, the percentage of users that would recognize a specific anomaly before harm occurs, etc.

4) *Add the risk of each scenario and determine if the total risk is acceptable:* Addition is by type of harm: death, broken bone, contusion, etc. The addition, of course, assumes that each scenario is independent of every other scenario, which is normally the case.
5) *Periodically review field performance after the product is released:* It is necessary for medical-device manufacturers to reach an acceptable level of overall residual risk prior to releasing a product to the field, not only for the purpose of satisfying regulatory agencies, but also for the sake of conscience. However, once the product is released, the question becomes one of whether or not it is performing at least as well as predicted. The work of monitoring field performance is not of itself a risk-management activity. It is addressed by the quality system under complaint handling. The role of risk management is to determine whether or not the actual overall residual risk is acceptable. Therefore, risk management seeks to update the overall residual-risk estimate as field information becomes available and determine if the actual overall residual risk is acceptable.

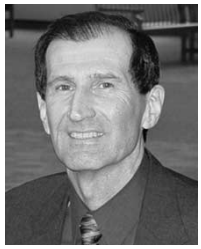
III. Common Characteristics

Successful risk management involves more than good process philosophy and content. The persons performing the activities must also have certain characteristics to assure an efficient and effective process.

1) *Product Understanding:* In order to recognize issues and understand what constitutes adequate solutions, applicable personnel at every level in the organization must first understand how the product works and how it will be used. They must also recognize the product's medical intent, as well as the medical consequences of device failures, improper operation, or improper use.
2) *Advocacy:* When we make risk management decisions, we need to put ourselves in the position of the customer (patient, medical professional, field staff...). A good question to ask is, "Would you use this on yourself or a family member?" Effective risk management decisions do not "gild the lily" or throw away business interest; but rather strike a prudent balance between business interest and customer interest grounded in the expectation that medical-device manufacturers are mindful of the customer's welfare.
3) *Passion:* Risk management will be most successful when employees have a passion to use their skills to substantially improve other people's lives. Do not halfheartedly look simply to produce a risk management report that will satisfy regulatory agencies. Instead, personnel should feel empowered to aggressively seek product-safety improvements that will minimize patient risk. This, in turn, will minimize corporate-liability exposure, improve regulatory compliance, and provide a competitive advantage in the market place.

IV. Finally

For some readers, this paper will have been too visionary with insufficient detail. To them, I apologize for trying to cover such a broad topic in a limited space. Others may find the details too demanding, setting forth a vision that seems unattainable. For these individuals, I hope you might dare to step out in faith and at least try implementing an idea that particularly rings true. My hope for the majority of readers is that this paper will stimulate a courageous and honest evaluation of your own risk-management activities to create a more efficient and effective process that better serves your customers.



Carl Schmuland is semiretired from Medtronic, Minneapolis, MN, after a career spanning 27 years, where he led a reliability-engineering group. He was a key participant in creating the development and risk-management processes for the Cardiac Rhythm Management Group. Prior to Medtronic, he worked as a Design Engineer in military and commercial applications. He has first-hand experience with development processes from several other organizations within Medtronic, as well as many original-equipment manufacturer (OEM) organizations that developed and manufactured critical subsystems for Medtronic. In addition to working half time at Medtronic, he has served as the Lead Instructor for Risk Management for the Association for the Advancement of Medical Instrumentation (AAMI).