Regulatory Issues

risk management

Grace Bartoo

Medical devices are required to be safe and effective before they are commercially marketed. However, there have been reports of adverse events, even deaths, due to unforeseen design errors. How can biomedical engineers minimize potential hazards to users and operators? Risk management is an essential engineering skill that all biomedical engineers should understand and use aggressively. Risk management is the systematic application of management policies, procedures, and practices to the tasks of identifying, analyzing, controlling, and monitoring risk. In this article, I will briefly outline the general steps you would take to anticipate failures, make safer products, and reduce liability costs.

Regulatory bodies have also recognized the value of risk management. The FDA's Quality System Regulations and the EC's Medical Device Directive require risk management. There are also international standards for how to conduct risk management. One of the most useful is "AAMI/ISO 14971 – Risk Management – Application of risk management to medical devices," which can be obtained through www.aami.org. The process outlined in this article follows this standard.

Overview

Risk management begins with the development of the design input requirements. As the design evolves, new risks may be identified. To systematically identify and, when necessary, reduce these risks, the risk management process is integrated into the design process. In this way, unacceptable risks can be identified and managed earlier in the design process when changes are easier to make and less costly.

An important part of risk management is to ensure that your company has a risk management procedure. The management, regulatory, and engineering heads should decide on the definitions of hazard severity and probability of occurrence. Most importantly, they should decide upon the risk acceptance criteria. Examples of possible definitions and criteria are shown in Tables 2-5. A template can be generated that will facilitate the conduct of risk management during the product lifecycle. Once a process and criteria for the company has been established, you would then integrate risk management with your product lifecycle processes.

The key steps to risk management are

- develop design inputs, including intended use, product features and requirements, regulatory and safety requirements, design constraints
- identify and analyze potential hazards, including their severity and probability of occurrence
- evaluate risk acceptability based on established criteria
- identify potential causes and control measures for the risks
- implement the risk control measures
- verify that the risk controls are implemented and validate their effectiveness
- determine the severity and probability of occurrence after risk controls (residual risk)
- determine overall risk acceptance
- update risk analysis and control measures throughout lifecycle of product.

Risk Analysis

The second two steps are commonly referred to as risk analysis (also known as hazard analysis). One of the best ways to start the risk analysis is to look up similar devices on the adverse event database at the FDA's Web site on similar devices (MAUDE database). The other technique I highly recommend is to hold a "brainstorming session" with a multidisciplinary group to identify potential hazards. This group might include hardware and software engineers, system engineers, regulatory and clinical staff, and marketing and service personnel. All known or foreseeable hazards for the subjects/patients, operators of the equipment, and bystanders should be considered. These potential hazards can include all sorts of things; some examples are hardware or software component failures, operator errors or misuse, tripping over cords, dropping the device on the operator or patient, and lightning strikes. One way to identify potential hazards is a top-down approach where you consider foreseeable hazards and then consider the causes. The other way is to assume failures in the components and then examine what hazards could arise from the component failures. These approaches complement each other and are useful for identifying hazards. The top-down and bottom-up techniques for risk analysis are known as fault tree analysis (FTA) and failure mode and effects analysis (FMEA), respectively. These techniques provide a more detailed method for risk analysis, and they can be used in conjunction with the risk management techniques discussed here.

A typical risk analysis template with example risks is shown in Table 1. Potential hazards are listed in each row. The next step is to provide a qualitative or quantitative categorization of the severity and probability of each hazard (see Tables 2 and 3 for a possible categorization scheme). With the severity and probabilities determined, the risk level can be determined. This can be

 0739-5175/03/$17.00©2003IEEE

TABLE 1. Example risk analysis template.

Hazard ID	Potential Hazard	Potential Causes	Severity	Probability of Occurrence	Unmitigated Risk Level
1	Broken bones or injury to operator or subject	Drop device or knock over device onto operator or subject	2	4	Low
2	Electrical shock	Lightning surge through power line.	1	4	Moderate
3	Incorrect treatment of patient: too much energy applied	Software error in timing for treatment.	2	3	Moderate
4	Ineffective treatment of patient: too little energy applied	Hardware component failure in output current circuit.	3	3	Low

TABLE 2. Example severity criteria.

Category	Severity	Description
1	Major	A failure or latent flaw directly affects the patient and/or operator and could result in death or serious injury to the patient and/or operator, or indirectly affects the patient and/or operator such that incorrect or delayed information could result in death or serious injury.
2	Moderate	A failure or latent flaw directly affects the patient and/or operator and could result in nonserious injury to the patient and/or operator, or indirectly affects the patient and/or operator where incorrect or delayed information could result in nonserious injury.
3	Minor	A failure or latent flaw would not be expected to result in any injury to the patient and/or operator.

TABLE 3. Example probability criteria.

Category	Probability of Occurrence	Description
1	Frequent	Likely to occur at least once a month in the operating life of the system.
2	Probable	Likely to occur less than 12 times per year in the operating life of the system.
3	Occasional	Likely to occur at least once in the life of the system.
4	Remote	May occur in the life of the system.
5	Improbable	Unlikely to occur in the life of the system.

accomplished by a mathematical algorithm (e.g., multiply severity and probability) or by a lookup table (see Table 4). Finally, use predetermined risk acceptance criteria as shown in Table 5 to determine the required actions for each risk level.

Risk Control

As shown in Table 5, some risks are low enough that no further risk reductions are necessary, but other risks may require one or more risk control measure(s) to reduce the risk to an acceptable level. Ways to reduce risk should be considered in the following order:

- inherent safety in design (e.g., design device to run on battery power rather than line power)
- protective measures in the device or manufacturing process (e.g., self-tests upon start up)
- information for safety (e.g., warning labels on device and/or instructions for use).

Typically, the risk analysis team makes recommendations on which risk control measures to implement. If the control measures are related to the design, you should incorporate these requirements in the design inputs. You should verify that the risk control measures were indeed implemented (e.g., are the specific warnings in the operator's manual?) using formal methods (e.g., documented verification procedures). You should also validate that the risk control measures are effective during beta testing with typical users.

You then reevaluate the severity and probability of occurrence of the potential hazards after consideration of the risk control measures and determine the risk level. This is known as the residual risk. Ideally, all potential hazards have a residual risk level that meets the criteria for no further risk control measures. However, if the residual risk is judged to be unacceptable as per the predetermined criteria and further risk control is impractical, one should conduct a risk/benefit analysis using known data and literature. For example, if the residual risk level is moderate, but the device is shown to be effective in treating an otherwise untreatable condition, the moderate risk level may be acceptable.

TABLE 4. Example risk level lookup table.

		Hazard Severity		
		Category 1	**Category 2**	**Category 3**
		Major	**Moderate**	**Minor**
Probability of Occurrence	**Category 1 Frequent**	*High*	Moderate	Moderate
	Category 2 Probable	*High*	Moderate	Low
	Category 3 Occasional	*High*	Moderate	Low
	Category 4 Remote	*Moderate*	Low	Low
	Category 5 Improbable	*Low*	Low	Low

TABLE 5. Example risk acceptance table.

Priority	Risk Level	Required Actions
1	High	High-level risks must be reduced before the product is distributed to customers.
2	Moderate	Moderate-level risks should be reduced before the product is distributed to customers. A risk/benefit analysis can be considered if risk reduction is impractical.
3	Low	Risk control measures are not required for low-risk hazards. The product team should assess each low-risk hazard to determine if risk control measures are advisable, and to determine how and when to provide such controls.

Risk Management Matrix

	System Name:								
	Analysis Team:								
ID	Potential Hazard	Potential Causes	Severity	Probability	Unmitigated Risk Level	Implemented Risk Control Measures	Verification and Validation	Severity	Probability
1	electrical stimulation skin burn	high current density at electrode contact	2	2	moderate	**a.** Specify large electrodes (>40 cm2) as accessory to device **b.** Operator training on electrode placement and importance of patient monitoring addressed in Operator Manual **c.** Patient instructions to alert operator upon discomfort addressed in Operator Manual.	**a.** Test Case 002 Results **b.** Test Case 004 Results **c.** Test Case 004 Results	2	4
2	electrical stimulation skin burn	current setting too high	2	2	moderate	**a.** Final output current stage has been designed so that no more than 75mA can be produced; system self-tests before treatment, watchdog timers implemented. **b.** Patient instructions to alert operator upon discomfort addressed in Operator Manual	**a.** Test Case 003 Results **b.** Test Case 004 Results	2	4
3	electrical stimulation skin burn	no feedback from patient	2	3	low	**a.** Final output current stage has been designed so that no more than 75mA can be produced; system self-tests before treatment, watchdog timers implemented. **b.** Patient instructions to alert operator upon discomfort addressed in Operator Manual	**a.** Test Case 003 Results **b.** Test Case 004 Results	2	4
4	electrical stimulation skin burn	electrodes are reused	2	2	moderate	Warning in Operator Manual not to reuse electrodes	Test Case 004 Results	2	4

Fig. 1. An example of a risk management matrix completed for a fictitious product.

When risk control measures are implemented, it is possible that the risk control measures may add new potential hazards. Therefore, risk analysis and risk control are iterative processes; the risk control measures should also be analyzed to see if any new hazards might be generated. If so, they should be added to the risk analysis table and treated as discussed above.

We have been discussing individual potential hazards and their risk evaluations. However, it is also important to assess the overall combined risk of this device. How many low-risk-level items and/or moderate risk-level items are acceptable overall? One way to assess the overall combined risk is to count the number of each type of risk and to add them together as a weighted sum (higher risk gets larger weight). An overall residual risk evaluation must be conducted after all control measures have been implemented. Once again, predetermined criteria should be used to determine the overall risk acceptability. If the overall combined residual risk is unacceptable base on the criteria, conduct a risk/benefit analysis to see if the medical benefits outweigh the residual risks. If the risk/benefit analysis justifies the residual risk, then one can proceed with development.

Finally, generate a risk management matrix to document traceability of each potential hazard to the risk analysis, risk evaluation, risk control measure(s), the verification of the risk control measure(s), the residual risk, and the evaluation of the residual risk for acceptability. This matrix is the key document for risk management as it traces each identified potential hazard to a risk assessment, control measures, and residual risk analysis. Figure 1 shows a portion of an example risk management matrix completed for a fictitious product.

Postproduction

Risk management is an ongoing process throughout the lifecycle of the product. Postproduction information about the device and similar devices should be systematically reviewed for possible relevance to safety. Some sources of postproduction data could include the MAUDE database at the FDA, corrective and preventive action reports, customer feedback, literature, and adverse event reports. Some areas to watch for are previously unanticipated hazards, new information to change severity or probability of a risk, and invalidation of the original assessment of risk or risk/benefit analysis. If any of these are true, update the risk analysis and repeat the risk control and residual risk evaluation process.

Summary

All of the risk analysis tables, the risk control measures, verification results, risk/benefit analyses, risk evaluations, and traceability analyses need to be documented and available for inspection by auditors. One way to organize this documentation is to have a risk management file that includes or references each of these documents.

This has been a brief outline of the key elements in risk management for a medical device. Finally, I would like to leave you with the thought that this risk management technique can be used for much more than control of potential hazards of a particular device. A risk management approach can be used for design, business, or regulatory decisions as well. For example, you may need to determine how to qualify your vendors as part of purchasing control. Some vendors may need less rigorous assessment (e.g., label provider), whereas some may provide critical components. Risk analysis can be done where each row is a vendor, and the severity of poor quality or service from the vendor from the regulatory and business perspectives can be assigned. From these severity numbers, a risk level can be assigned and the proper assessment protocol can be determined. Risk analysis can be applied whenever you need a systematic method to analyze and prioritize tasks.

Grace Bartoo is the Region 6 Representative for EMBS and is the vice president for regulatory and clinical affairs at Instruments for Science and Medicine. She can be reached at grace @ismtech.com.

---

about. It is normal to suspend judgment for a while; life goes on, and eventually he sees price-fixing as an ordinary feature of his life as a manager, not as an unethical practice. He has learned to focus on what matters in the organization and omit what does not. Just as Milgram's subjects overlooked or discounted the danger to the learners when asked to do so by a person of authority, the manager learns to overlook or discount practices that would otherwise be seen as unethical or illegal.

Learning to focus on what is important is what Davis calls "microvision." Unlike tunnel vision, microvision is like looking through a microscope, seeing what is important by excluding everything else from the visual field. This is essential for any kind of professional role. Physicians learn to ignore certain features of their patient's lives in order to focus their attention on the medically significant ones. Engineers know what features of a design to pay attention to and which ones to set aside. This is the reason, Davis suggests, that we have stereotypes of professions, the pushy surgeon, the aggressive lawyer, the caring nurse, the professor who lectures rather than engaging in conversation, but not of plumbers and shoemakers. Professional training shapes personality in ways that other kinds of work do not. Similarly, becoming an effective manager requires learning organizational culture, including what is regarded as right and wrong. (For a dark look at ethics in organizations, see R. Jackall, *Moral Mazes: The World of Corporate Managers*. New York: Oxford Univ. Press, 1988.) The danger is that unreflective individuals may simply lose their ability to see organizational matters through the lens of ordinary law and ethics. Like the sales representatives who can no longer see the shortcomings of the products they sell, unreflective individuals have been captured by their roles. One of the most important things I do as an ethics consultant is to tell managers how their actions will look when seen by people who are not immersed in their organizational culture and will view their actions with a critical eye.

Conclusion

The individuals who violated legal and ethical norms in recent cases of corporate wrongdoing are responsible for their actions and should be punished accordingly. But keep in mind how organizational culture shapes our sense of right and wrong and makes it more difficult to evaluate actions from the point of view of ordinary morality. And remember that these cases are hardly anomalies in a market system that fosters social irresponsibility and strongly resists the regulatory means to make it more socially responsible. A recent *Wall Street Journal* cartoon shows two corporate executives sitting side by side at a table, smoking cigars, of course. One leans over to the other and says "This ethics bubble will eventually burst."