Medical Device Life Cycle Risk Management

by GM Samaras

Safety is the continual application of effective risk management activities, not the momentary absence of known hazards. Avoiding unintended harms requires continuously managing all the risks associated with your product. Ignoring product use errors overlooks a large number of hazards. Acquisition of user complaints is the basis for use error identification and postmarket product risk management. Actively harvesting user complaints is a basic defense against unintended harms and product recalls.

Introduction

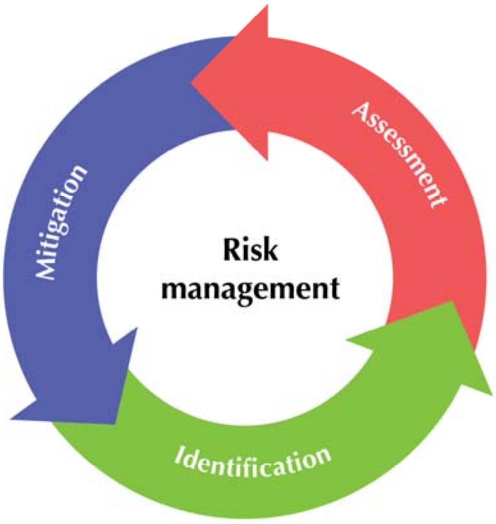
A product manufacturer's obligation for product safety extends across the whole product life cycle—from concept to salvage/disposal. In the United States, manufacturers and retailers of consumer products are obligated to report certain product safety issues to the Consumer Product Safety Commission; manufacturers and operators of aircraft are obligated to report certain aviation safety issues to the Federal Aviation Administration; manufacturers and user facilities of medical devices are obligated to report certain medical device safety issues to the Food and Drug Administration.

Safety is the continual application of effective risk management activities, not the momentary absence of known hazards. Risk management is applied across the complete product life cycle. The principle is enshrined in many well-recognized industry standards (e.g., for medical devices, ISO 9001, ISO 13485, and ISO 14971) and is a fundamental engineering best practice. Correct application of life cycle risk management is your primary tool for minimizing unintended harms to patients and providers, reducing product recalls, limiting product liability, and protecting employees and shareholders.

Risk Management

Figure 1 shows the general approach to risk management. Risk is future uncertainty of the deviation from an expected outcome. In product risk management, complaints of desirable deviations are rare and we are typically only concerned with undesirable (unsafe/ineffective) deviations. Risk is generally quantified as some combination of the severity of harm of the identified hazard and the frequency of occurrence of that identified hazard.[1]

Figure 1



Nearly every senior executive understands financial risk management: "The identification, analysis, assessment, control, and avoidance, minimization, or elimination of unacceptable risks. An organization may use risk assumption, risk avoidance, risk retention, risk transfer, or any other strategy (or combination of strategies) in proper management of future events."[2] But the strategies for **financial** risk management do not map well to **product** risk management; risk avoidance and risk transfer (from manufacturer to customer[3]) ultimately result in unintended risk assumption and risk retention by

[1] Samaras, GM. "Use, Misuse, and Abuse of the Device Failure Modes Effects Analysis." *MD+DI Online* (and later print Magazine August 2013).

[2] http://www.businessdictionary.com/definition/risk-management.html Accessed 6/11/15.

[3] Minimizing Type II errors (Producer Risk) at the expense of Type I errors (Consumer Risk).

cont. on p. 16

the product manufacturer. Furthermore, from a sales and marketing perspective (the background of many senior corporate leaders), if there is no consumables "tail" once the product is sold and delivered, there is strong motivation to shift focus to the sale of the next product, rather than focusing on managing risk for product already sold. This makes eminently good sense, but only from a myopic financial perspective.

Sales and marketing move product, but they are also the firm's principle interface for customer satisfaction and product safety information. They are essential for generating revenue, but also foundational for protecting that same revenue by identifying complaints and supporting timely product life cycle risk management. Motivate them to sell product and to acquire satisfaction and safety data. This will reduce delays managing product risks; the rapid response will reduce unintended harms, product recalls, and product liability actions.

Modern Western expectations and industry standards demand that manufacturers eliminate essentially all product safety hazards. But eliminating all known and unknown hazards is, by definition, an impossible task. What is possible is creating product safety by continually implementing effective risk management practices. Eliminate risks from hazards that can be identified during premarket development and manufacturing. Then, follow by rigorously and systematically searching for and managing new or previously unrecognized hazards in the postmarket phase, until the product is replaced or disposed. This is the well-established *"cradle-to-grave"* risk management engineering best practice identified in textbooks, in international consensus standards, and required by many federal agencies for a variety of products.

Setting Boundaries

Identifying hazards requires an understanding of use context. Engineers set operational boundaries (the design envelope) followed by conducting worst-case analyses to inform their design validation testing. Well-known examples of boundaries include operating voltages and currents for consumer electronic devices, operating ceiling and descent rate for aircraft, and encapsulation for software components. Engineers typically try to steer clear of unbounded problems because they are not generally amenable to closed solutions and product realization. This is the reason that operationalization of product requirements (design inputs) is crucial to efficient engineering design. By operationalization we mean (a) defining what to measure, (b) defining how (and with what) to measure it, and (c) what measurement results in a pass or fail. Carefully established boundaries reduce the complexity of product design and risk management, thus decreasing time to market. Not establishing clear boundaries frequently results is arbitrary, and potentially undesirable, assumptions about the required boundaries … yielding unintended consequences.

For medical devices, one important set of boundaries is defined by the intended use, the intended user(s), and the intended use environment(s). This constrains the context, but does not fully eliminate risk complexity. There are two types of product use errors: system use errors and individual user errors.[4] A well-known example of an *individual user* error is driving while intoxicated. A well-known example of a *system use* error is the set of mistakes operators make as a result of a poorly designed interface. Hazards arise not only from how the device is designed, manufactured, and deployed, but also from how the device is used after it is sold. The manufacturer can reasonably expect (see Table 1) intended use, novel use, misuse, and abuse of their device, as well as active, latent, and drift errors from product development, manufacturing, and deployment processes.[5] One cannot reasonably assume their product will be used exactly as they envision it. Ignoring the full spectrum of potential use errors in product risk management is not adequate, reasonable, or technically correct. It only delays effective internal risk management and invites external risk management in the form of product recalls and expensive lawsuits.

[4] Samaras, GM. "Medical Device Mechatronics Maturity." *Medical Electronics Design Online* (and later print Magazine, January 2013).

[5] Samaras, GM. "Reducing latent errors, drift errors, and stakeholder dissonance." *WORK: A Journal of Assessment, Prevention, and Rehabilitation*, 41(s1):1948-1955 (2012).

cont. on p. 17

Table 1

	Human error category	
Error-producing behavior	**System use error**	**Individual user error**
Expected behavior	Active (known bugs)	Routine use
Unexpected behavior	Latent (unknown bugs)	Novel use
Misguided behavior	Drift (beyond design envelope)	Misuse
Malicious behavior	Sabotage	Abuse
Locus of control	**Development and deployment organizations**	**Individual human(s)**

Elements of Life Cycle Risk Management

Managing product risk involves both administrative and engineering activities. There are administrative standard operating procedures that must be managed and reports that must document the required activities. However, the documentation only serves as evidence of the occurrence of engineering activities.[6] You can envision five discrete engineering activities for risk management: (1) identification of a potential hazard, (2) recognition or acceptance of an identified hazard as relevant for the specific product, (3) evaluation of the risk, (4) application of a proposed risk control measure, and (5) verification or validation of the risk control measure(s). Risk management is well described in standard texts and various consensus standards; what is not well described is the correspondence between premarket and postmarket risk management activities (see Table 2). Understanding the correspondence and terminology differences are important elements in promoting complete and correct product life cycle risk management. Product risk management does not stop with the end of development and the beginning of sales; it stops when the product is no longer sold and used.

Premarket (or design) risk management generally uses terminology familiar to engineers. First, you have to identify a potential hazard. Then, you have to recognize it is a hazard affecting your specific product (it is not outside your boundaries). Once you have accepted that a hazard is relevant, you have to evaluate the risk by determining (or estimating) the probability of the hazard occurring and the severity of the harm that can result. If you deem that risk is acceptable, then you accept the risk (you cannot accept risk for someone else)

Table 2

Iteration steps	Premarket development	Postmarket vigilance
1	Hazard identification	Complaint management
2	Hazard recognition	Sentinel event recognition
3	Hazard risk evaluation	Health hazard evaluation
4	Risk control application	Corrective preventive action
5	Risk control verification/validation	CAPA verification/validation

[6] Samaras, GM. "The Use, Misuse, and Abuse of Design Controls." *IEEE Engineering in Medicine and Biology Magazine* 29(3):12-18, 2010.

cont. on p. 18

or you can attempt to transfer the risk to your customer; if you decide the risk is not acceptable, then you are obligated to implement an effective risk control measure. There are four types of premarket risk control measures: (a) redesign, (b) guarding, (c) transfer of control of the risk to the end user through labeling or training, and (d) not selling the product. Once a candidate risk control has been agreed and implemented, you are obligated to verify or validate that the risk control (a) actually reduced the targeted risk and (b) did not create any new hazards;[7] risk control verification or validation is always required, even if you chose to employ labeling or training.

An important consideration in evaluating and controlling design risk, especially if you are relying on *detectability* for prioritizing resources for risk management, is that detectability does not alter the actual design risk. Detectability is a risk control measure, not an element of risk, and only available internally to the product manufacturer before the product is shipped. Once in the hands of users, you have no knowledge or control over what a user can or will detect. Even if they detect a design defect hazard, you have no knowledge or control of whether they will remember how to properly respond to the hazard. And, even if the user recalls the correct response, you have no knowledge or control over whether they have adequate time or expertise to properly implement your recommended risk control. Detection is a design risk control measure for manufacturers, not users.

Postmarket risk management does not differ from premarket risk management, except in the terms used. Complaint management (acquiring and analyzing complaints and other postmarket information) is foundational; it is your primary mechanism for getting information on potential, previously unidentified, hazards. A deficient complaint management system negates your premarket risk management efforts and undermines all remaining postmarket risk management activities. Sentinel events (sometimes called *safety signals*) are the occurrence (or the possibility of occurrence, such as from a “near miss”) of unexpected events involving death or serious injury not related to the natural course of an injury or illness.[8] Sentinel event recognition corresponds to premarket hazard recognition and is, by definition, an accepted hazard. Postmarket evaluation of the risk associated with this hazard is often called a “health hazard evaluation”[9] and is used to determine whether risk control (corrective and preventive action [CAPA]) is warranted. If you decide CAPA is not warranted, you are deciding to accept the risk. But, if you decide that a CAPA risk control is warranted, then the options include (a) redesign, (b) guarding, (c) transfer of risk control to the end user using labeling or training, and (d) removal of the device from the market. As in premarket risk management, you have to verify or validate that the risk control (a) actually reduced the targeted risk and (b) did not create any new hazards.

The “PA” in CAPA includes public reporting, which is itself a validated risk control. It is a regulatory obligation in the United States[10] and it is the means of informing the public of death or serious injury *associated with the use* of your product. It is a critical element in postmarket risk management that expands the risk management process beyond the manufacturer to external agencies. This crucial risk control is defeated by manufacturer reporting noncompliance.

Conclusion

Product life cycle risk management is an engineering approach for increasing product safety and reducing unintentional harms, product recalls, and product liability. Unlike financial risk management, product risk avoidance and risk transfer ultimately result in manufacturer risk assumption and risk retention. The terminology used for premarket risk management and postmarket risk management differ, but the underlying engineering activities are essentially the same. Not doing complete and correct premarket risk management undermines the viability of your product in the marketplace; not doing complete

[7] See, for example, ISO 14971:2003 §6.3.

[8] http://www.jointcommission.org/Sentinel_Event_Policy_and_Procedures/default.aspx Accessed 6/9/15.

[9] See, for example, 21 CFR 7.41.

[10] 21 CFR 803.

cont. on p. 19

and correct postmarket risk management negates your premarket efforts and increases your firm's financial risk. Fundamental to successful postmarket risk management is an effective and efficient complaint management system that actively harvests customer satisfaction and safety data. Motivate your primary connection to your customers—your sales personnel—both to sell your product and to quickly feed back to you user complaints and field observations. The commissions you pay will reduce unintended harms, reduce product recalls, protect your shareholders, and allow you to innovate new, improved products for everyone's benefit.

[redacted]