Use, Misuse, & Abuse of the dFMEA

GM Samaras Pueblo, CO

In 2004, MDDI published a seminal article by MW Schmidt entitled “The Use and Misuse of FMEA in Risk Analysis”[1] warning of the improper use of “detectability” in the DESIGN FMEA. While his article significantly reduced the incidence of this erroneous practice in medical device risk management, it still has not been eradicated totally.

A Quick History

Most of us working in some capacity related to FDA-regulated firms have heard of the 1937 *Elixir Sulfanilamide* disaster that killed over 100 Americans and is credited with hastening congressional passage of the US Federal Food, Drug, and Cosmetic Act. This beneficial antibiotic was dissolved in diethylene glycol, a poison that is a principal component of antifreeze. You might think that was the end of it, but it is not! It has appeared more or less regularly throughout the world in human-ingestible substances, even as recently as a few years ago.

Those of us who work with medical device software are well aware of the radiation therapy software disaster[2] in the mid-1980s that prompted FDA-regulation of medical device software. You might think that was the end of it … but it just happened again. It is well established that even the simplest software can have complex and unpredictable behavior, even when it is developed in the structured systematic manner prescribed by the principles and practices of modern software engineering. Risks creep into the best designs. Your best defense is a robust risk management process with valid decision-making[3].

Complete and correct risk analysis is the basis of risk management for medical device design. It always has been, and will continue to be, crucial to the safety and effectiveness of medical devices, so long as we continue to develop new or modified products. You cannot ever let down your guard. You are not just protecting your family, friends, and neighbors who use your products. You are also protecting your organization, your colleagues’ jobs, and your own job. This is personal.

Medical Device Risk Management

At the end of the last century, there was a recognized need to codify engineering best practices for risk management, so it was available to the largest possible medical device engineering audience. The first comprehensive international consensus standard for risk management of medical devices (ISO 14971) was published in 2000, amended in 2003, and a second edition was published in 2007. It has been a FDA-recognized risk management consensus standard since 2001[4]. In 2005, the Global Harmonization Task Force (GHTF) – a voluntary international group of representatives from medical device regulatory authorities and trade associations from Europe, the US, Canada, Japan, and Australia – issued their final guidance on implementation of risk

---

[1] Schmidt, MW. The Use and Misuse of FMEA in Risk Analysis. MDDI. March 2004. Accessed 2/24/13: http://www.mddionline.com/article/use-and-misuse-fmea-risk-analysis

[2] Casey, S. Set Phasers On Stun And Other True Tales Of Design, Technology, And Human Error, 2nd Edition, Aegean: Santa Barbara. 1998

[3] Telson, S. Develop Defensively: Control Risk and Predict Results. MDDI. May 2005. Accessed 2/24/13: http://www.mddionline.com/node/1226

[4] 66 FR 23032

management within a medical device quality management system[5]. Both of these documents provide medical device manufacturers with a structured, systematic approach to risk management.

Medical device risk management (see Figure 1) is a necessary, although not sufficient, component of medical device design control[6] (see Figure 2). We can envision risk management as consisting of iterative risk analyses, followed by evaluation of the overall residual risks and generation of a risk management report. Risk analysis proceeds iteratively (see Figure 3) as the medical device design evolves. It consists of:

- risk identification (*is there a potential source of harm that is known or foreseen*[7]*?*),
- risk evaluation (*do I really care?*), and
- risk mitigation (*can I adequately control the targeted risk?*).

Once the design is frozen, the acceptability of the overall residual risks is determined to evaluate whether or not this is a viable product.

There are a wide variety of tools that can be used for risk analysis (see Figure 4 for some examples); your choice of tool depends upon two critical factors. First, are you trying to do an inductive (bottom-up) or deductive (top-down) risk analysis? Second, what kind of data do you have available to you? Is your data objective (*historical, quantitative, failure rate data from clinical or actuarial sources*) or is your data subjective (*you are giving it your best guess, using what you hope are expert opinions*). Correct risk management is essential for medical device innovation. For many medical device manufacturers commercializing new or improved devices, an economically reasonable inductive risk analysis can be only accomplished with mostly subjective data. The alternative is exhaustive clinical, field, and accelerated environmental testing.

Two important elements of both ISO 14971 and the GHTF guidance are:

- TOP management, not the design engineer, is responsible[8] for incorporating effective risk management in the quality management of medical devices, and
- Nowhere in the ISO standard or GHTF guidance does it state that only a bottom-up risk analysis is necessary and sufficient; the combination of top-down and bottom-up analyses gives the greatest and most economical risk coverage.

The dFMEA

The design (or device) FMEA (dFMEA) is an inductive risk analysis tool that addresses design-related risks to the end-user (e.g., the patient, the patient's family, and the patient's healthcare providers). Annex C and Table E1 of ISO 14971:2007 provide a set of critical questions and a convenient listing of hazards that need consideration in an FMEA. Annex A of the GHTF guidance provides a convenient tabulation of risk values for an FMEA, segregated by whether they are (a) low, (b) medium, or (c) high. Given these, examination of Figure 4 suggests why the choice of the FMEA is a popular tool. There is an important caveat regarding these convenient questions, tables, and risk categories. They are generic, they are not comprehensive, they do not necessarily all apply to your particular

[5] GHTF/SG3/N15R8: Implementation of risk management principles and activities within a Quality Management System, May 20, 2005
[6] 21 CFR 820.30 & ISO 13485:2003 §7
[7] Foreseeable risks include those associated with expected use, unexpected use, misuse, and abuse. They include the full range of use activities from acquisition through disposal.
[8] ISO 14971:2007 §3.2; GHTF/SG3/N15R8 §4

medical device, and the clear expectation is that you critically will think through what is and is not relevant to the safety and effectiveness of your device and its users.

Risk is defined in both ISO 14971:2007 §2.16 and the GHTF guidance (§2) as the "*combination of the probability of occurrence of harm and the severity of that harm*." Severity of harm (S) is how critical is the hazard; will it kill you or will it be simply annoying. The probability or frequency of occurrence (O) is an estimate of how often you expect that hazard to occur. The product of these (SxO) is the practical measure of risk and the numerical value is a risk prioritization number (RPN=SxO) that can be used to decide the order in which to mitigate these risks (i.e., highest first, lowest last). The RPN also may be used as a mechanism to allocate the engineering resources required to deal with each risk. What we are trying to accomplish in the dFMEA is the management of design "RISK". Design risk originates from the specific design of a product, not from its manufacture, distribution, or maintenance.

Nowhere in the standard or guidance is "*detectability*" (D) included in the definition of risk ... because detection is NOT an element of risk, but a risk mitigation or risk control measure. The use of detectability, which legitimately can be used in a process FMEA (pFMEA) is NOT permissible in a dFMEA. The ingress of detectability in the dFMEA may have been the result of misunderstanding the difference between a pFMEA (development, manufacturing, distribution, or maintenance) and the dFMEA (final risk to the end-user). It has persisted in some quarters because it appears to offer a convenient means of showing acceptable design risk. It does not! The use of detectability in the dFMEA is not only the use of a faulty risk management process in your quality management system, but is also the use of a flawed corporate decision-making process. Detectability does NOT change the actual design risk; only redesign may accomplish that.

When you are managing risk multiplied by detectability, you are NOT managing design risk. The whole purpose of ISO 14971 is to provide a framework "*to manage the risks associated with the USE of medical devices*[9]." Unless the end-user is able to detect the specific risk in a sufficient amount of time to avoid the risk AND recall the correct procedure for avoiding that specific risk, detectability is not even useful as a risk control measure.

Conclusion

Risk consists of severity of harm (S) and frequency of occurrence (O). Do not include "detectability" (D) in your design FMEA, because it corrupts your risk analysis and causes you to underestimate the REAL risk to the users of your medical device. Reducing design risk requires either (a) changing the design, or (b) designing engineering controls or, as a last resort, (c) designing effective warnings. Yes, lowering the risk prioritization number (RPN=SxO) with detectability (RPNxD) certainly reduces your engineering workload and reduces your time to market, but it does nothing for reducing the risk to your patients, their family members, and their healthcare providers ... or the subsequent risk to your organization and your job.

NOTE: Interested readers will find an ISO 14971:2007 compliant dFMEA template in the RISK MANAGEMENT section of my website.

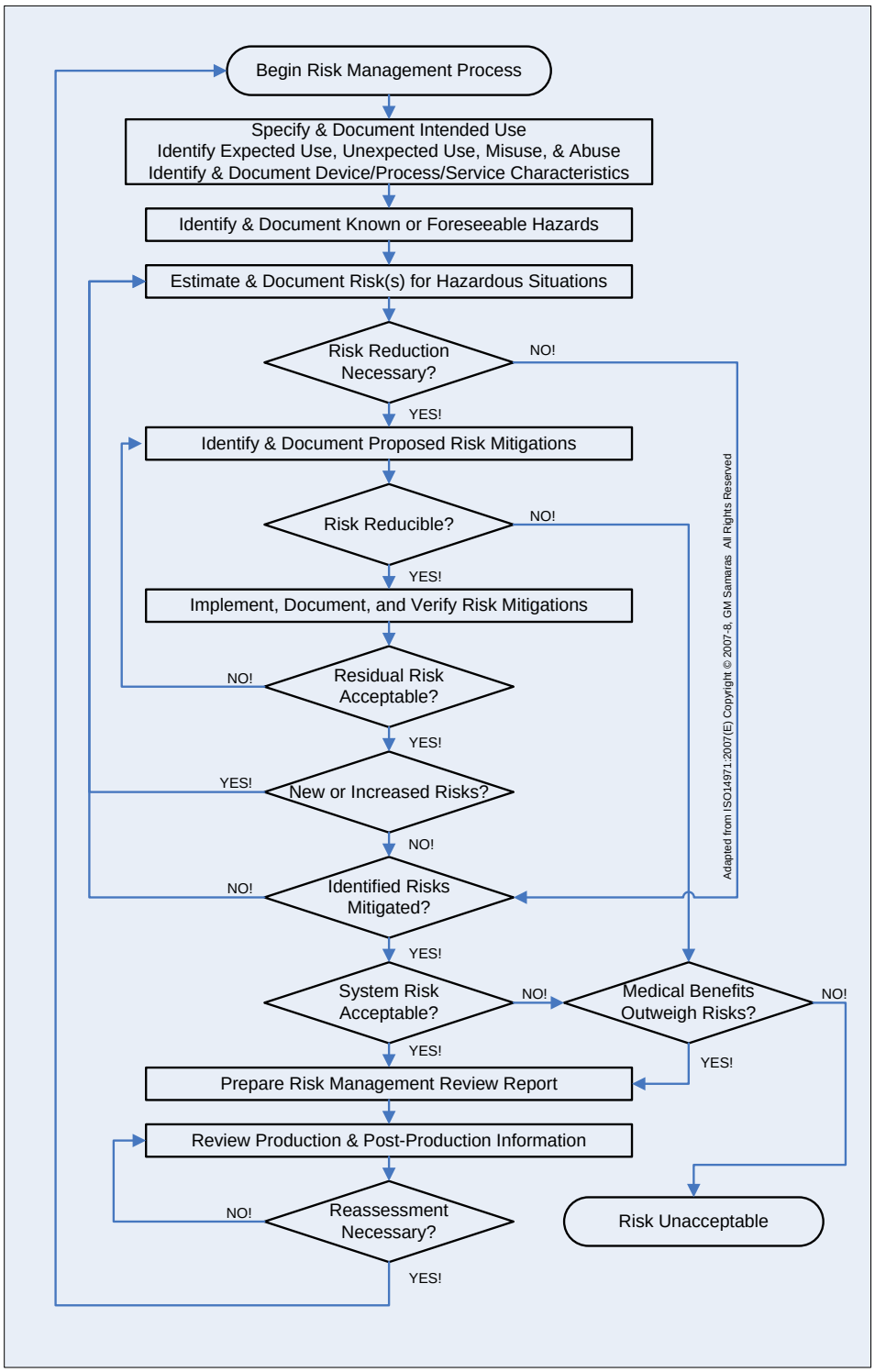
[9] ISO 14971:2007, Introduction

Author Bio

GM Samaras is a biomedical scientist/engineer currently in private practice (Pueblo, CO). Trained as an electrical engineer, he has doctorates in physiology and industrial engineering; he is a licensed professional engineer (PE), board-certified human factors engineer (CPE), and an ASQ-certified quality engineer (CQE). He has a number of biomedical patents and publications in physiology and engineering (hardware, software, human factors, and quality). He has worked at the FDA/CDRH as a reviewer & manager, he was a medical school and engineering graduate school professor, and founded an engineering firm that he ran for a decade.

Figures

Figure 1: The Medical Device Risk Management Process



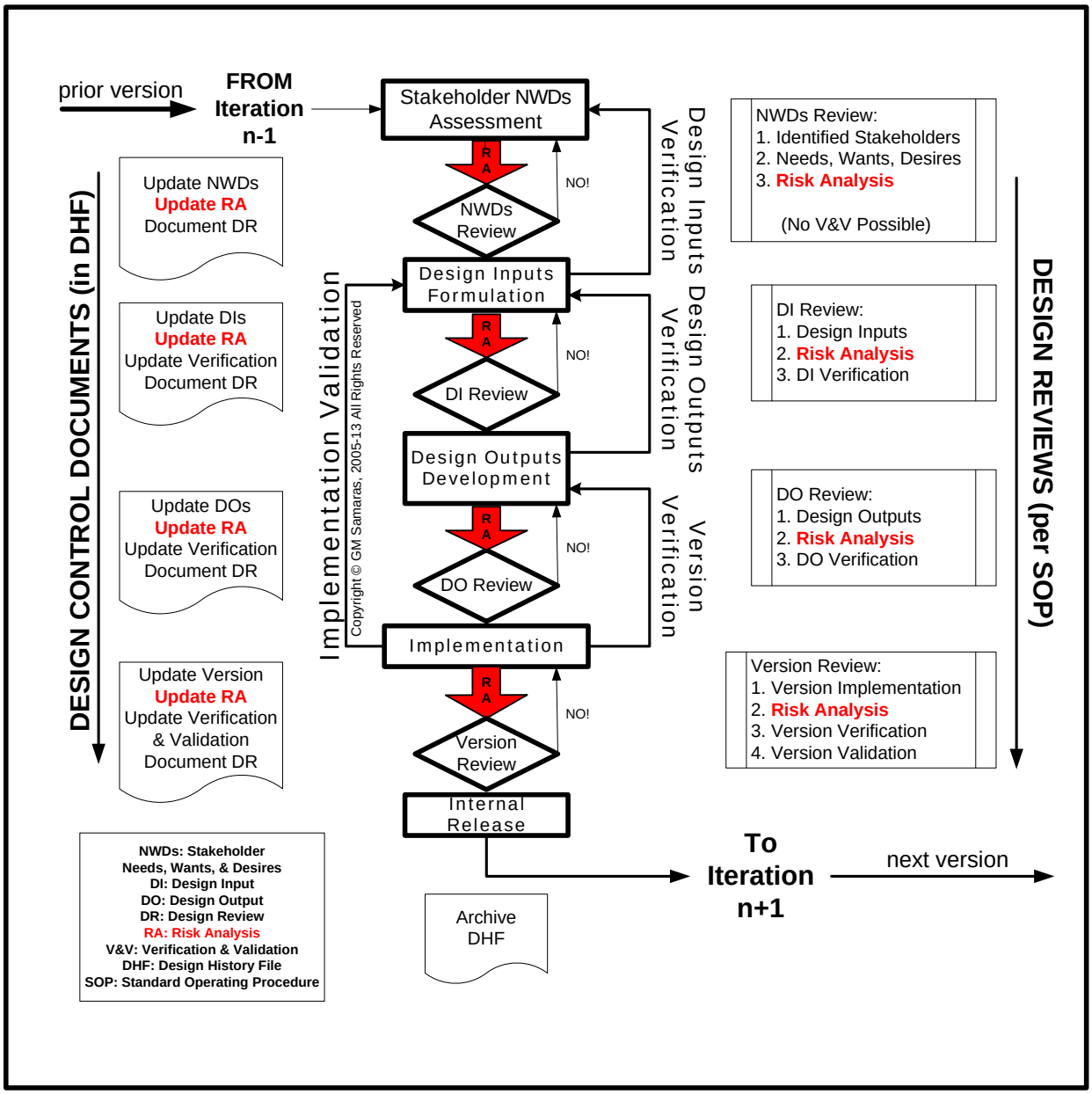


Figure 2: Risk Analysis in Design Control

Figure 3: Iterative Risk Management

Type of Risk Analysis	Type of Input Data: Quantitative, Historical	Type of Input Data: Subjective, Experiential
Inductive *(Bottom Up)*	Failure Modes, Effects and Criticality Analysis (FMECA)	Failure Modes Effects Analysis (FMEA) Hazard & Operability Studies (HazOp) Hazard Analysis & Critical Control Points (HACCP)
Deductive *(Top Down)*	Fault Tree Analysis (FTA) Event Tree Analysis (ETA)	Root Cause Analysis (RCA)

Copyright © 2007-2010, GM Samaras All Rights Reserved

Figure 4: Examples of Risk Analysis Tools