An Introduction to Risk/Hazard Analysis for Medical Devices

By Daniel Kamm, P.E., C.Q.A.

Risk analysis, or hazard analysis, is a structured tool for the evaluation of potential problems which could be encountered in connection the use of any number of things, from driving a car, riding on public transportation, taking a drug, or using a medical device. We live in a world full of risks, with varying likelihoods and consequences. Risk analysis is now routinely used during the design phase for medical devices.

Why should we perform risk analysis?

1. Risk analysis is now required by law (Revised GMP, see below)
2. Identification of device design problems prior to distribution eliminates costs associated with recalls.
3. It offers a measure of protection from product liability damage awards.
4. Regulatory submissions checklists (PMA and 510k) used by the FDA now call for inclusion of risk analysis.
5. It is the right thing to do.

Unless you have been living under a rock, you now know that the FDA has revised the Medical Device Good Manufacturing Practices Regulation, 21 CFR Section 820. It took effect on June 1, 1997. The Safe Medical Devices Act of 1990 gave the FDA the express authority to enforce what it had been strongly advising since 1987 (in "Pre-production Quality Assurance Planning Recommendations For Medical Device Manufacturers"), the use of "design controls" during the development of new medical devices. Section 820.30 (Design Controls) calls for:

"§820.30(g) Design validation…. Design validation shall include software validation and risk analysis, where appropriate." (Emphasis added)

Historical Reasons for the Addition of Risk Analysis to the GMP

The origins of the inclusion of risk analysis are real incidents of harm to the patients receiving treatment by medical devices, such as electric shocks, over-infusion by infusion pumps, and over doses of radiation by radiotherapy devices. Too many of these incidents resulted in the deaths of patients. For example, between June, 1985 and January, 1987, a computer controlled radiation therapy machine called the Therac 25 massively overdosed six people. The results were deadly. See: Nancy Leveson, *Safeware: System Safety and Computers*, Addison-Wesley, 1995.

Overview of the Tools

"Pre-production Quality Assurance Planning Recommendations For Medical Device Manufacturers" identifies three tools for risk analysis: Failure mode effects analysis (FMEA), Fault tree analysis (FTA), and Failure mode effects criticality analysis (FMECA)

Failure Mode Effects Analysis (FMEA) and Failure Mode Effects Criticality Analysis (FMECA)

Failure mode effects analysis (FMEA) is a "bottom up" approach which assumes a basic defect at the component level, assesses the effect, and identifies potential solutions. It should be conducted at the beginning of the design effort and as part of each design review to identify potential design weaknesses. Failure mode effects criticality analysis (FMECA) adds probability of occurrence and severity of failure to the FMEA process. In the discussion below, the term "FMEA" will include criticality analysis.

The primary purpose of FMEA is the early identification of potential design inadequacies that may adversely affect safety and performance. Identified inadequacies can then be eliminated or their effect minimized through design correction or other means before they reach the customer. There are two main types of FMEA: Design FMEA which focuses on what could go wrong with a product in both manufacturing operation and in service as a result of a weakness in the design and- Process FMEA which concentrates on the reasons for potential failure during manufacturing and in service. This is a result of non-compliance to specification and/or design intent. The FMEA can be documented in a table as shown below:

Format for FMEA Table

Function or Component	Failure Mode	Effect on System	Possible Hazards	Risk Index	User Detection Means	Applicable Control(s)
Isolation transformer T1	Primary to secondary short circuit	Other failures in power supply, loss of system operation	Shock to patient, fire, damage to other system components	5	Front panel lights will not illuminate indicating power supply fault.	Primary fuses, transformer uses UL approved materials. Chassis is safety grounded.
(Etc.)						

Note the use of "Risk Index" in the fifth column. One way of assigning a risk index is to use a table similar to the one below:

Risk Index Table

Probability of Occurrence	Severity I Catastrophic (Death, serious injury)	Severity II Significant (Reversible serious injury)	Severity III Marginal (Inconvenience)	Severity IV Negligible
Frequent	1	3	7	13
Probable	2	5	9	16
Occasional	4	6	11	18
Remote	8	10	14	19
Improbable	12	15	17	20

Risk index criteria will determine what to do if the risk index (the numerical value) falls in a given range:

Risk Index Table

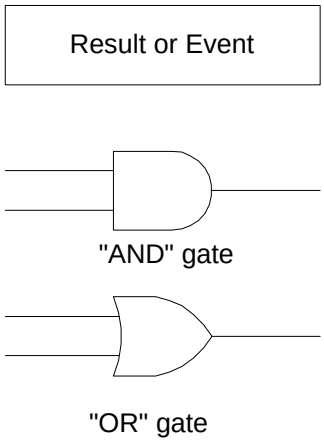
HAZARD RISK INDEX	ACCEPTANCE CRITERIA
1 to 5	Unacceptable
6 to 9	Undesirable: Written and reviewed decision required to proceed
10 to 16	Acceptable upon completion of quality assurance review
17 to 20	Acceptable without review

The steps of the FMEA process:

- *Define the function of the unit being analyzed.*
- *Identify all potential failures.*
- *Determine the causes of each failure types.*
- *Determine the effects of potential failures.*
- *Assign a risk index to each of the failure types.*
- *Determine the most appropriate corrective/preventive actions.*
- *Monitor the implementation of the corrective/preventive to ensure that it is having the desired effect.*

Fault Tree Analysis

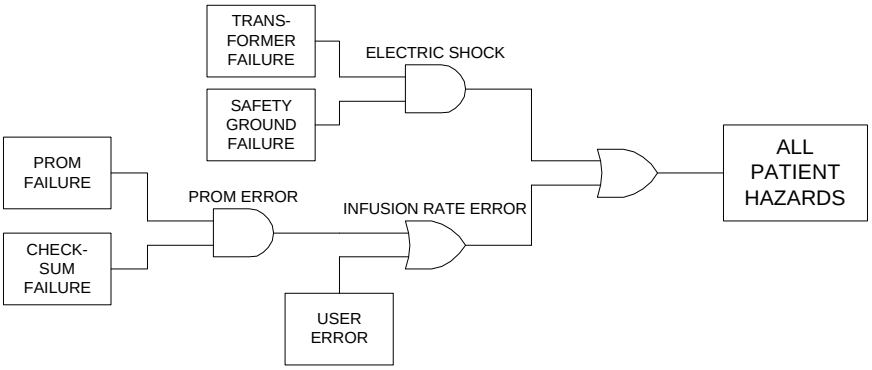
Fault tree analysis (FTA) is a deductive, "top-down" approach to failure mode analysis. First, one identifies a failure or safety hazard, then an attempt is made to identify all possible ways to create that hazard. An example of a safety hazard would be electrical shock Usually, a chart is constructed using logic symbols such as "and" plus "or" gates:



The steps for conducting a fault tree analysis are-

- *List the possible hazards, such as:*
  Fire, electrical shock, mis-diagnosis, injury, etc.
- *What failures, or combination of failures, will lead to the named hazards?*
- *Diagram the fault tree.*
- *Use the tool to intercept or design out unacceptable consequences.*

Example of a Simplified Fault Tree Diagram for an Infusion Pump



Summary

Whatever method is employed, it is now mandatory to conduct a risk or hazard analysis during the design phase of a medical device. Also, if a design change results in the decision to file a new 510(k), remember that the FDA's own checklists call for the inclusion of a risk analysis, especially if the product has software in it.

References:

1. "Applying Hazard Analysis to Medical Devices" Parts I and II, Medical Device and Diagnostic Industry Magazine, January 1993 pp 79-83 and March 1993 pp 58-64.

2. *Failure Mode and Effect Analysis, FMEA from Theory to Execution* D. H. Stamatis, ASQC, 1995. ISBN 0-87389-300-X

3. The Center For Devices and Radiological Health (CDRH), Food and Drug Administration. You can visit their Web Site at http://www.fda.gov.cdrh/index.html

4. Military Standards and Handbooks:
   MIL-HDBK-781A: Handbook For Reliability Test Methods, Plans, And Environments For Engineering, Development Qualification, And Production
   MIL-STD-1629A Military Standard Procedures For Performing A Failure Mode, Effects And Criticality Analysis

   Military Standards (MIL-STDs) and Military Handbooks (MIL-HDBKs) can be obtained from:
   Standardization Documents Order Desk
   Bldg 4D, Customer Service
   700 Robbins Ave.
   Philadelphia, PA 19111-5094

Telephone for information: (215) 697-2667 Fax: (215) 697-1462
You can visit their Web Site at http://www.dtic.dla.mil/