Aggressive Risk Management Combining FTA and FMEA

FDA Medical device recalls hit an all-time high again in FY2017. The 21st century cure for this "recall epidemic" is the method presented in this paper, more so when supported by a project management platform using social media software technologies.

Richard L. Bollinger (rick@menloparkassociates.com)

Back in 2016 MDDI published a paper titled "What's Behind MetTech's Recall Epidemic?" by Joshua R. Dix, Suraj Ramachandran, and Darin S. Oppenheimer.[1] They reported that FDA recalls hit an all-time high in 2014.

Figure 1 shows it has happened again in 2017. This fiscal year now holds the record.

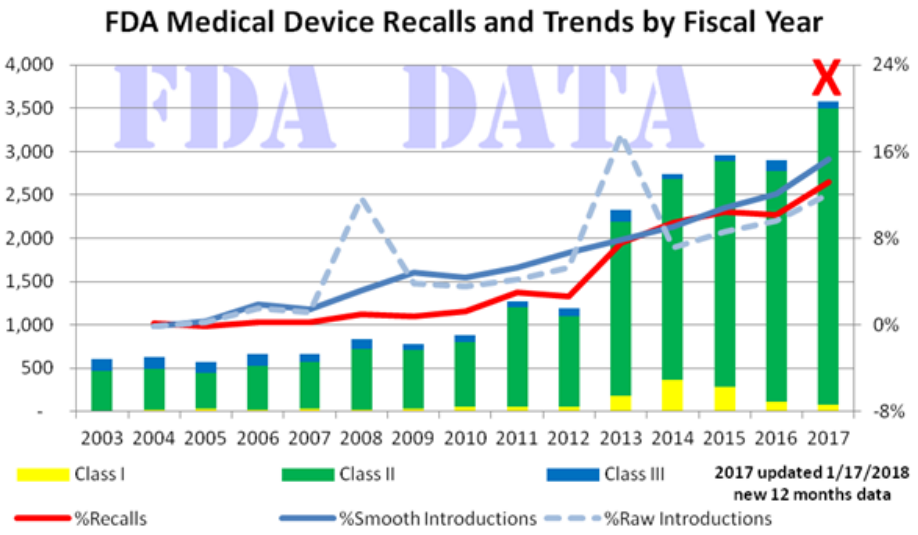

Figure 1 - Medical Device Recalls

The 2016 paper blamed risk management by manufacturers: the culture, the shallow understanding industry-wide, the inability to tie risk management into quality management systems. This is not fair. They should not be so critical if they can't show a better way.

Using the method in this paper, your products will have better safety and reliability because aggressive risk management combines Failure Mode and Effects Analysis (FMEA) and Fault Tree Analysis (FTA). Also, it is iterative so it can attack faults and incrementally reduce their probabilities with each cycle. In addition, this method will prevent the fade of safety-related behaviors by anchoring them to global standards and absolute risk management goals used in each Benefit-Risk Assessment (BRA). All of that is what makes this method "aggressive."

FDA (non-binding) recommendations identify factors for assessment of medical device risks:

> "Likelihood of risk considers risk factors related to the potential number of patients at risk of experiencing harm: the likelihood that a medical device will

have problems, the likelihood of a patient experiencing harm, and the total number of patients exposed.[2]"

Improve the precision of your risk management.

It can be appropriate to follow non-binding recommendations. They often point in new and useful directions. Note that the assessment risk factors are all mathematical probabilities. This is necessary to express the uncertainly and risk in human terms and be compared to benefits. The good news is that this method uses FTA to calculate fault/failure mode mathematical probabilities which can be used directly in these human impact calculations.

FTA is a top-down analysis process. Iteratively parsing the structure of a product and its faults/failure modes, it derives quantifiable probabilities of failure and harm. It seeks to understand the vulnerabilities of the structure overall and find new configurations that improve safety and reliability. And, find new faults/failure modes that fit into the structure.

Improve the accuracy of your risk management.

FMEA is a discovery and bottom-up process. It iteratively works to better understand each fault/failure mode in isolation to control its severity, likelihood and detectability. Also, to understand its causes and probabilities, and find new faults/failure modes and causes. It deals with ordinal or qualitative quantities. This is appropriate to manage the attention and resources applied to individual risks, improving depth of understanding and applying it towards more accurate mathematical probabilities. Which is why FMEA is used in this method.

Improve the outcomes of your risk management.

This method iteratively invokes FMEA and FTA to understand vulnerabilities, prioritize efforts, and work to optimize safety and reliability. It was inspired by a very complex technical article.[3] Their method was a mash up of FTA and FMEA. It did not include Benefit-Risk Assessment.

It can help to reduce the number FDA recalls and the effort and cost of preventing them.

This method can also establish confidence that recalls are being proactively prevented and that lack of recalls is not just by good fortune. The goal of risk management here is to improve device safety and reliability by moving all risks into the 'Accepted' category until marginal returns set in. The method works by making risks incrementally smaller and less likely by changes in design (or manufacture, etc.), or application of controls, in each iteration. (This can be seen in Figure 2, below). The trail of analysis, changes, and risk acceptance will provide such confidence.

Automation in the transfer of failure modes for FMEA or FTA calculations will speed up iterations and reduce clerical errors. Also, software that can increase risk management collaboration between risk specialists and development team members will produce synergy in the understanding of failure modes and discovery of new ones. Especially, if meetings can be designed to bring people together that are remote or part of outsourced solutions.

Internet facilitated meetings can remove the requirement that attendees need to be in the same room. This can reduce the cost of outsourcing and travel, or the need for any altogether.

INTEGRATE RISK MANAGEMENT AND DEVELOPMENT

Aggressive risk management uses the simplified model below for integrating risk management and quality management. You can use it to improve your results by embedding it in your own proprietary processes. The method is used in the small box in the middle of the RSKM loop on the left: FTA & FMEA.

The model of integration in this method (Figure 2) might be familiar. At least the right half. It was on the FDA website on a page about Software Development Life Cycle (SDLC) for medical devices.

Use of it is certainly appropriate given the 2016 paper's worry about software-controlled devices and a "***disconnect between the availability of [FDA] guidance and risk information to manufacturers, and the ability of those manufacturers to actually mitigate issues***."

Use this new method to break out of the status quo. Use the SDLC model to also stand in for non-software related System Development Life Cycle. It can still be used as a guide to tie Risk Management into your medical device development cycles. There should be analog processes for development of devices with no software at all; devices with embedded software; and devices that are all software. And, for traditional software development and all flavors of Agile.

Your challenge is to understand the theory of this method, make the connections in your current processes, and make it all operational in the context of your system of development.

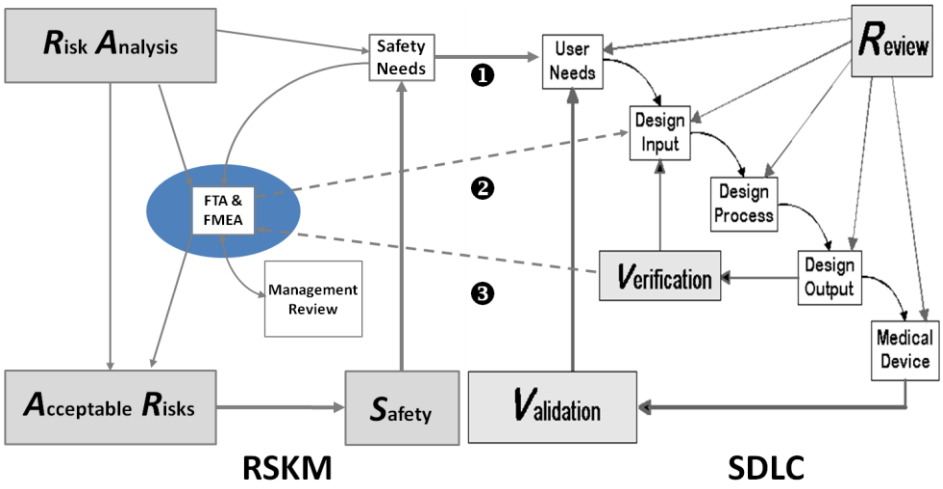

Figure 2 - Integration of Risk Management and Development

How it works.

There are two loops operating in Figure 2. The one on the right half, labeled SDLC, goes clockwise. It starts at **User Needs** and goes around to **Validation**. The one on the left, labeled

RSKM for Risk Management runs counterclockwise. It starts at **Safety Needs** and goes around to **Safety**. The SDLC loop terminates at **Validation** when its criteria are reached. RSKM terminates when all risks are acceptable and Safety is achieved.

The RSKM loop begins by contributing **Safety Needs** to **User Needs** ❶. This is the first connection from RSKM to SDLC. These 'needs' are expressed within SDLC design and development.

Risk Analysis monitors all risks (i.e. faults, failure modes) and acts by moving them into **Acceptable Risks**. Also, if needed, it updates **Safety Needs** and **FTA & FMEA**.

To start, **Risk Analysis** triggers **FTA & FMEA** so that the initial Fault Tree is built. After that, **Verification** triggers **FTA & FMEA** ❸ so the impact of design and development changes can be assessed on risks. This is another connection between RSKM and SDLC.

Changes from **Risk Analysis** and **FTA & FMEA** can trigger changes to **Design Input** ❷ to contribute requirements design and features that mitigate risks.

FTA & FMEA is monitored and controlled by **Management Review**. **Risk Analysis** depends on **FTA & FMEA** to analyze all risks from top to bottom, and mitigate all risks so they individually meet acceptance criteria to the greatest extent possible at the moment.

COMBINING FAULT TREE ANALYSIS WITH FAILURE MODE & EFFECTS ANALYSIS

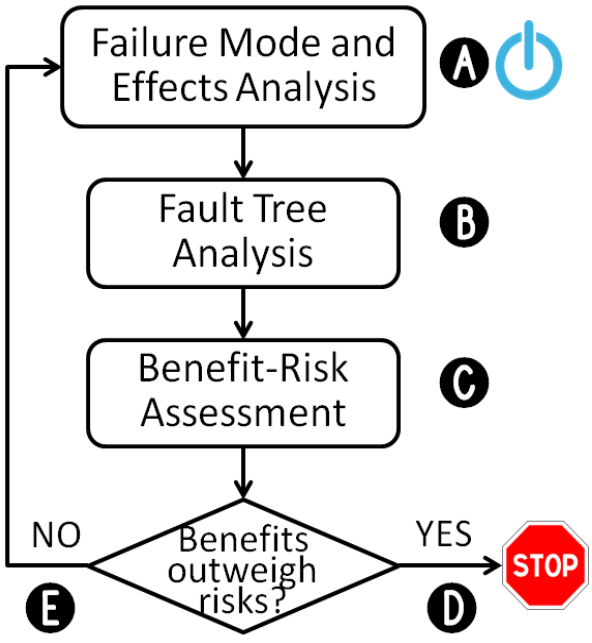

Figure 3 - Combine FTA and FMEA

Figure 3 shows the two techniques combined. The method starts with Ⓐ FMEA because it can be done while design is just beginning and risks are not all known. No tree or partial fault tree is needed for analysis. It is done bottom-up on each new and current failure mode with a fresh understanding of structures and probabilities from the last FTA and device sensitivities to complex failures. Each iteration looks more deeply for detections, controls and mitigations that would make a risk more acceptable.

Ⓑ Fault Tree Analysis is done next. It's a top-down process to create and maintain the device fault tree. Its purpose is to understand the overall structure of the product and calculate the mathematical failure probabilities needed for the next step.

Ⓒ Benefit-Risk Assessment is performed to keep the overall goal in mind. It applies the probabilities to the harms and balances outcomes against absolute safety and reliability goals.

Ⓓ If all the risks have been considered, and all are outweighed by the benefits with an acceptable margin, then the process can stop.

Ⓔ If not, then the loop returns to the top and FMEA is done again to get a deeper look at each failure mode for further mitigation. It can go around many times to ensure that all manner of detection and mitigation has been applied to current controls, thus driving down absolute probabilities of device failures.

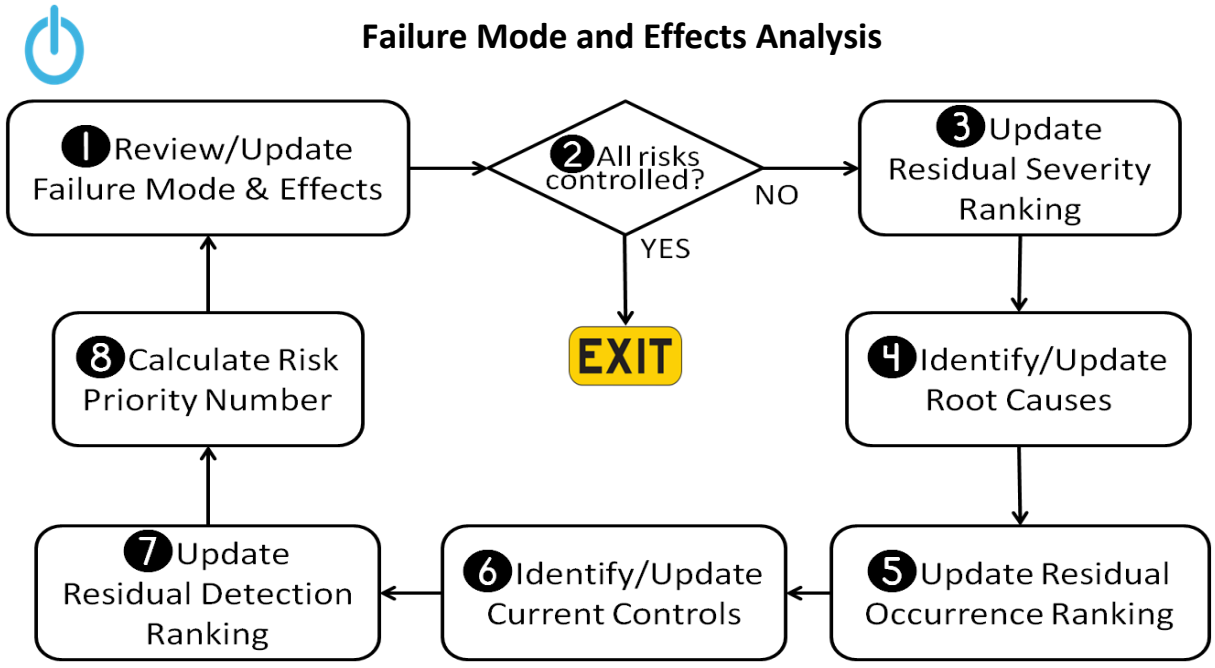

Figure 4 - Failure Mode and Effects Analysis

Ⓐ FAILURE MODE AND EFFECTS ANALYSIS

Figure 4 shows the steps in an FMEA. Its purpose is to evaluate and mitigate risks in a continual loop until marginal returns set in. To begin ❶ review or update all risks (failure modes), checking ❷ that each has been mitigated, controlled, and/or accepted in turn with fresh understanding of structures and probabilities from the last FTA and newfound device sensitivities to complex failures. If so, then EXIT. If not, ❸ update each risk's residual severity description, quantification, and ranking after mitigations or controls or detections are applied. With this information, ❹ identify new or update old root causes and new risks for new iterations. Also, ❺ update each risk's residual occurrence description, quantification, and ranking. Then ❻ review, identify or update current controls that are in place. Knowing this, ❼ update the residual detection descriptions, quantifications, and rankings, ❽ recalculate the RPN values, and ❶ review that all risks are ❷ mitigated, controlled, and/or accepted.

❽ FAULT TREE ANALYSIS

Fault Tree Analysis starts with the tree ❶. The first iteration will begin construction of the tree. Subsequent iterations will update and manage it. ❷ The goal here (Figure 5) is to evaluate the probabilities of all risk(s) and determine if they have all been controlled or their effects limited given the tree risk structure. If so, we EXIT. If not, ❸ top level faults are evaluated. Following that, ❹ system-wide structural mitigations, restructuring, reformulations are then investigated. FTA can see and make changes that FMEA cannot because it can see new perspectives, view fresh angles, and exercise new freedoms in its room to maneuver and innovate that FMEA does not have. From there, ❺ identify new risks and specify more mitigations for all the changes.

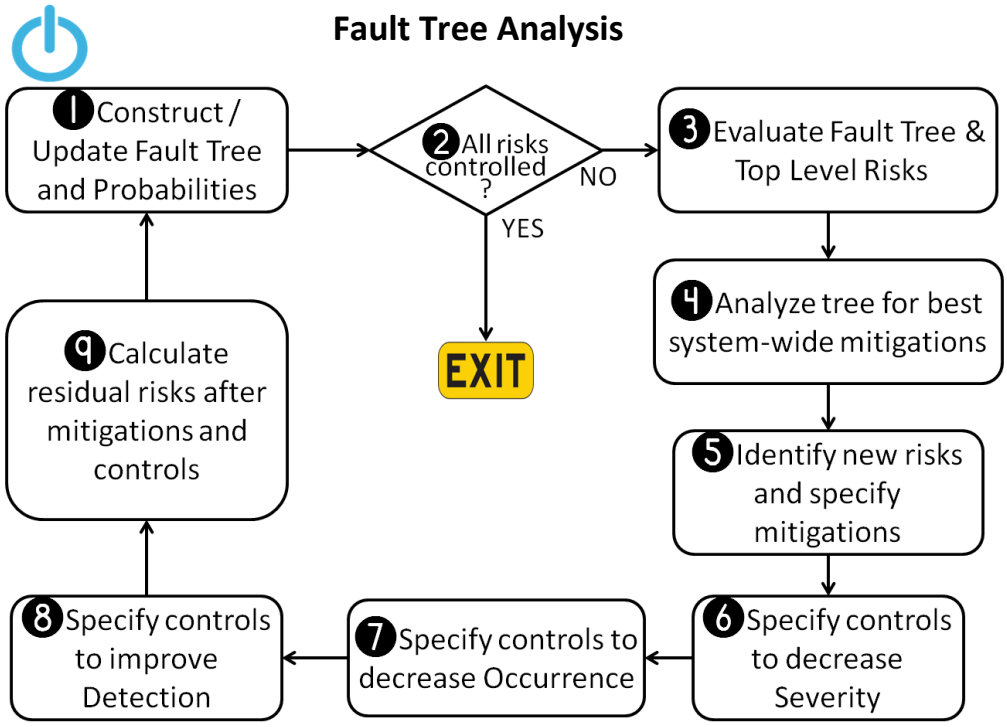

Figure 5 - Fault Tree Analysis with Detection

Continuing with this new information, then ❻ review and update controls with which to decrease severity of risks. Next ❼ review and update controls with which to decrease occurrence of risks. And, ❽ review and update controls with which to improve the detection of risks. When done updating control specifications, ❾ calculate the residual risk occurrences and severities after application of all controls and mitigations. Then ❶ update the fault tree again with the new data and recalculate risk probabilities. When all risks have been accepted, or been applied controls that need them, and all failure paths have been investigated ❷ then exit.

Often risks can be attributable to root causes. FMEA does this formally and often handles each risk individually. FTA can do this but it is more complex. All root causes become new risks that expand and reconfigure the tree to calculate the total effect.

FTA does not normally 'iterate' over risks. The methodology typically 'solves' for top-level risk probabilities based on causal risks lower in the tree. Like a harbor tide, as water recedes, new features are revealed that were hidden just below the surface of the water. The good news is that computer tools designed for this analysis are available that make it much easier to perform. So, a deep tutorial on FTA will not be found in this document.

#	Likelihood	%
10	Very Likely	20
9	Very High	10
8	High+	5
7	High-	2
6	Moderate+	1
5	Moderate	0.2

Figure 6 - Likelihood/Probability Table

Upon exit of a Fault Tree Analysis, risk probabilities can be translated into likelihood values using a mapping table like in Figure 6. This data should be established beforehand and maintained as a very valuable organization asset. It can be used to translate initial verbal and ordinal scale likelihood rankings into probability approximations. Later, when more accurate probabilities have been calculated, the situation reverses. Risk probabilities can be translated to ordinal numbers and verbal characterizations, and thus participate in RPN calculations and discussions.

PROBLEMS WITH SCORING METHODS AND ORDINAL SCALES IN RISK ASSESSMENT

Douglas Hubbard and Dylan Evans, both of IBM, are not fond of scoring methods based on ordinal scales in common use. They argue conclusively in the IBM Journal of Research & Development [4] that the "perceived benefit is probably illusory in most cases." And, explain why "risk assessment approaches should describe risk in terms of mathematical probabilities." Note that Fault Tree Analysis operates on, and delivers results, in terms of mathematical probabilities.

There is a companion article, 'Detection to the Rescue', that shows how avoiding use of Detectability rankings can be dangerous. It explains how hidden faults make hidden device defects. That is why this method recommends its use. And, especially recommends using FTA with mapping tables and dealing with mathematical probabilities whenever possible.

Ordinal scales are also useful to look at relative priorities and exposures. These can show where attention and resources should be budgeted. And, using different combinations, like simple RPN, weighted RPN, or just Severity alone, provides different looks at the data. Thus, making it harder for a risk to hide from scrutiny and mitigation.

IMPLEMENTATION PRACTICES SUMMARY

Now that you see how the pieces all work together, the following steps should introduce them into your standard operating procedures and proprietary work instructions, forms, templates and systems. Improve your risk management by making it aggressive.

1. Add Detection ranking to Risk Priority Number calculation. That should add depth to your risk understanding.
2. Add Fault Tree Analysis (FTA) to risk management with FMEA to deliver mathematical probabilities required for Benefit-Risk Assessment. Make use of FTA's top-down look and whole system view of the design and risk structure.
3. Make Benefit-Risk Assessment a permanent part of risk management. Keep safety-related behaviors from fading, and preventing other motivating factors to come to the fore.
4. Implement the RSKM loop and links to your SDLC into your Standard Operating Procedures.
5. Institute synergy by purposely bringing development team members, with product knowledge, together with risk management specialists having expertise. They should be able to do more than either alone.
6. Establish periodic risk management meetings with all hands, and in special groups, to make presentations and reap the synergy of sharing analogs of risks and mitigations between components; sharing cross-component failure modes and discoveries; and finding risks and mitigations in component interfaces and interactions.

Manufacturers that have been in business a while should have a proprietary risk vault of past risks detected and, better yet, not detected before reaching a user. This is a learning process. It creates a precious resource for future risk management, and future detection.

Your risk vault should drive planning and process design and product design. Any past problem is a potential future problem. This resource should gradually improve the safety and quality of your products. Every project should have a post-mortem where its history is mined for project risks, product faults, and lessons learned.

In addition to consulting, Rick teaches risk management. And all his students leave his classes knowing that risk management is special and powerful. This is because it can change anything: a product, a design, a plan, a project, a process and an organization. And, if more people understood the power of risk management, it could change the world.

If you found this article useful, or otherwise, feedback would be appreciated. Also, medical device practitioners are being interviewed about industry problems and how they are affected. Feel welcome to join the group of 100 experts diagnosing, and prognosticating a larger solution.

MY VISION

I was in the medical device industry some years ago. The world has changed. Please consider taking the survey and interview to characterize the current problems and solutions in the industry from your point of view.

You will get to influence the design of new methods and tools and make sure your needs are addressed exactly.

Also, you get to ensure your enterprise profits from the close match of needs to features and practices developed.

New methods and tools need to be spread all over the world to improve medical device safety and reliability globally. Your role can be that of a champion for quality.

Please feel free to nominate persons you respect and think would contribute much as volunteers in my research. Have them just send me an email at rick@menloparkassociates.com.

YOU ARE WELCOME TO JOIN ME IN THIS QUEST.

REFERENCES

[1] "What's Behind MetTech's Recall Epidemic?" by Joshua R. Dix, Suraj Ramachandran, and Darin S. Oppenheimer.

[2] Factors to Consider Regarding Benefit-Risk in Medical Device Product Availability, Compliance, and Enforcement Decisions (https://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm506679.pdf)

[3] Safety Analysis of Combined FMEA and FTA with Computer Software Assistance ± Take Photovoltaic Plant for Example
Chi-Tang Liu*, Sheue-Ling Hwang*, I-K. Lin**
**Institute of Industrial Engineering and Engineering Management, National Tsing Hua University, Hsinchu, Taiwan, ROC (e-mail: lililu525@gmail.com)*

[4] Hubbard, D. and Evans, D.; (2010, MAY/JUNE). Problems with scoring methods and ordinal scales in risk assessment. *IBM J. RES. & DEV. VOL. 54 NO. 3*, PAPER 2.