Detection to the Rescue

FDA Medical device recalls hit an all-time high again. So, let's try something new.

Richard L. Bollinger

Back in 2015 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 most recent fiscal year now holds the record. 24% higher than the year before.

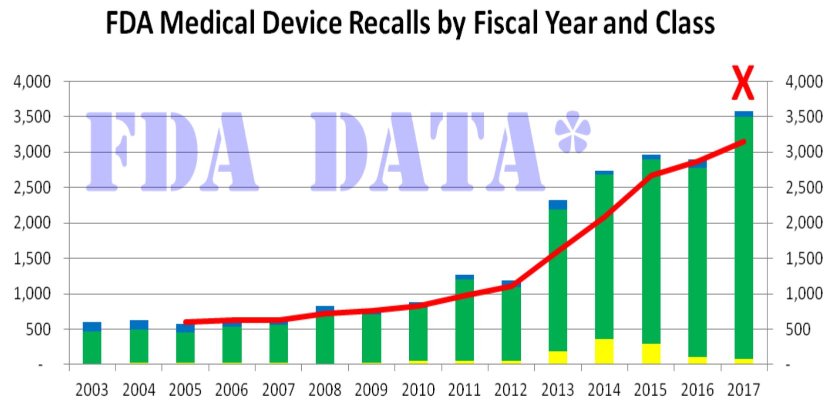

Figure 1 Recalls by Fiscal Year and Class

The 2015 paper blamed risk management: the culture, the shallow understanding industry-wide, the inability to tie risk management into quality management systems. I agree with them. But the FDA data does not reveal the problem in any depth. The article's implications carried good intentions, but pointed upwards, and bid the industry to climb the great mountain of risk management knowledge. Success should not come at so high a cost. Other FDA data might show the way.

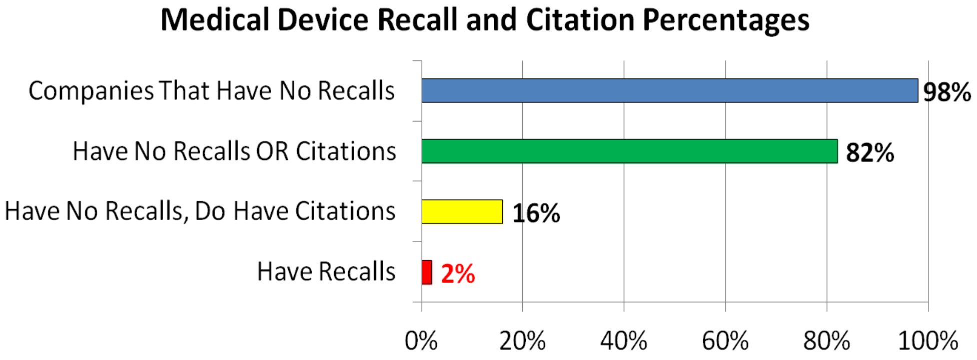

Figure 2 Company Recall and Citation Percentages

Figure 2 combines FDA recall and citation data. We might be able to read some meaning into the numbers. The top (blue) bar says 98% of companies have no recalls. That is not a bad number. And it does impart some faith to the medical device industry. But, that means that 2% of companies do have one or more recalls. The companion bottom (red) bar shows that. The second (green) bar shows that 82% of companies have no recalls and no citations. They have perfect records. Lastly, we can calculate the interesting third (yellow) bar. It shows that 16% of companies have citations, but do not have any recalls.

Detection to the Rescue

This begs a question. When companies get their first recall, A) did they come directly from the 82% with perfect records? Or, B) did they make a stopover in the 16% that had citations? And, come from there. Was it probability (A)? Or was it quality (B)? Put another way, does smoke mean there's a fire? Do citations forecast recalls?

That is an interesting question. It is not clear if FDA data has the answer in it. More importantly, do we need the answer to act? Probably not. When the symptoms are system-wide, shouldn't also be the remedies? Perhaps the best course of action is to take our most promising shot at the problem now. Plan a campaign with all the elements we can muster like Fault Tree Analysis (FTA), Failure Mode and Effects Analysis (FMEA). Climb down from the mountain (it should be easier), find and make new methods. Methods built, not just from the great body of risk management knowledge, but also from academic work on the subject. Like a way to combine FTA and FMEA.[2] Do them, check and act on the results.

Methods can also help us get the most from Detection Ranking and Risk Prioritization. There seems to be a lot of confusion about this. Some articles say Detection should not be used because it is bad, or it does not meet ISO standards. Others say FMEA requires it, but present a rote understanding of why and how Detectability should be used.[3]

My opinion has always been to DO MORE. I have been an auditor and I have never, ever, made an observation for actions in excess of what regulations require, as long as they did not subtract. ISO should also observe this principle. Otherwise an organization could be forced to choose between doing the best it can to make products safe or following ISO regulations to the letter and doing less. Who do you want making your next medical device?

Our best shot can use the model below for integrating risk management and quality management. You can use it to enhance your processes and improve your results.

INTEGRATE RISK MANAGEMENT AND QUALITY MANAGEMENT

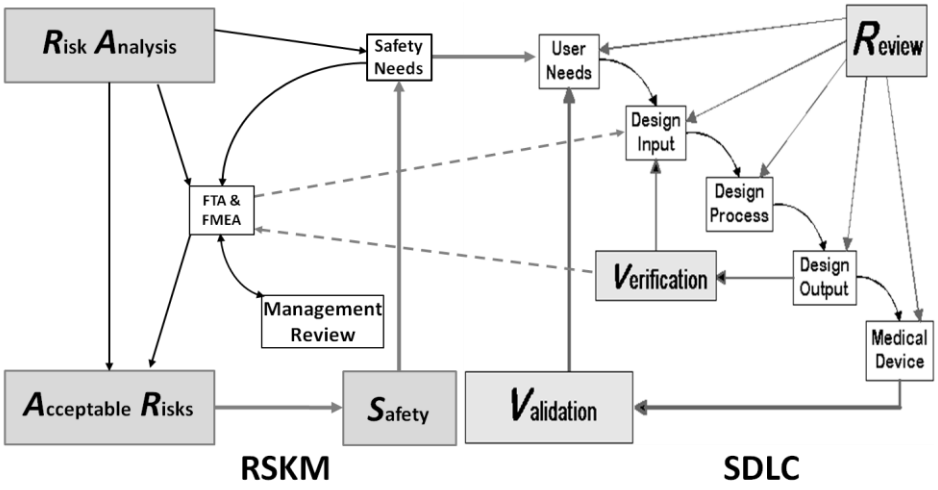

Figure 3 Integration of Risk Management and Quality Management

This model of integration (Figure 3) 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. Our use is certainly appropriate given the 2015 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.”

For our purposes, we can have it also stand in for non-software related System Development Life Cycle and use it as a guide to tie Risk Management into our 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.

There are two loops operating here. 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. Risk Analysis monitors all risks (i.e. faults, failure modes) and moves them to into Acceptable Risks. It also updates Safety Needs and triggers FTA & FMEA, which is also triggered by Verification. FTA & FMEA triggers Design Input to contribute requirements 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.

COMBINING FAULT TREE ANALYSIS WITH FAILURE MODE & EFFECTS ANALYSIS

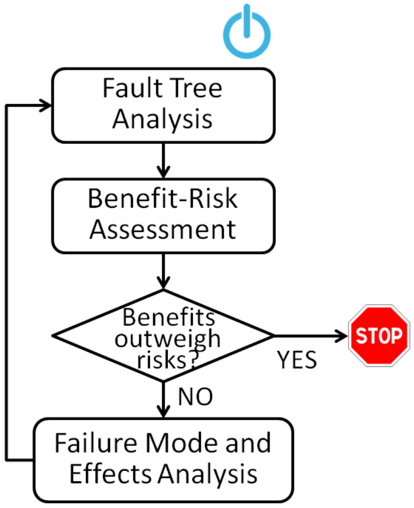

Figure 4 Integrate FTA and FMEA

Figure 4 combines the two techniques. Fault Tree Analysis is a top-down process to create the first tree, understand the overall structure of the product and calculate the initial probabilities. Benefit-Risk Assessment is performed to keep the overall goal in mind: Benefits outweigh risks. Failure Mode and Effects Analysis is done bottom-up on all risks to look deeply for detections, controls and mitigations that would make each more acceptable.

The loop returns to the top and Fault Tree Analysis is done again to get updated risk probabilities for further assessments. It can STOP when benefits outweigh the risks.

FAULT TREE ANALYSIS

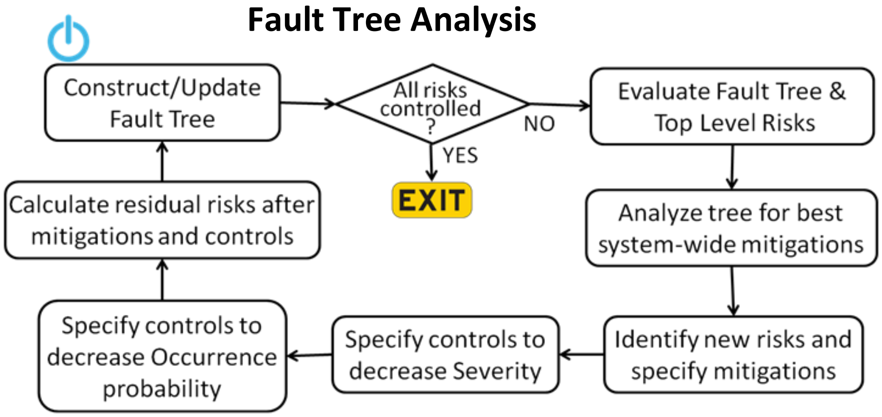
Fault Tree Analysis
Construct/Update Fault Tree
All risks controlled ?
NO
Evaluate Fault Tree & Top Level Risks
YES
EXIT
Calculate residual risks after mitigations and controls
Analyze tree for best system-wide mitigations
Specify controls to decrease Occurrence probability
Specify controls to decrease Severity
Identify new risks and specify mitigations

Figure 5 Fault Tree Analysis

Any Fault Tree Analysis starts with the tree. Its goal here (Figure 5) is to evaluate the probability of risk(s). Top level faults are evaluated. System-wide and structural mitigations are then investigated with which to identify new risks and specify more mitigations. Then review and update controls with which to decrease severity of risks. Next review and update controls with which to decrease occurrence of risks. Calculate the residual risk occurrence and severity after application of all controls. Then update the Fault Tree, resort risks by RPN and recalculate risk probabilities. All risks are controlled if all failure paths have been investigated.

FAILURE MODE AND EFFECTS ANALYSIS

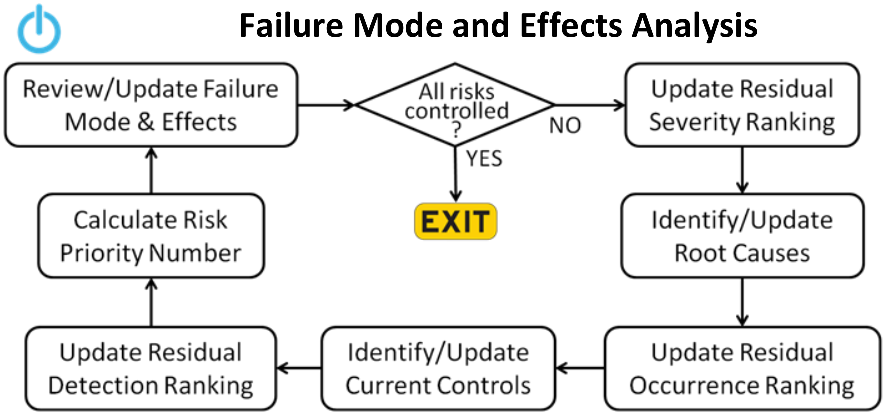
Failure Mode and Effects Analysis
Review/Update Failure Mode & Effects
All risks controlled ?
NO
Update Residual Severity Ranking
YES
EXIT
Calculate Risk Priority Number
Identify/Update Root Causes
Update Residual Detection Ranking
Identify/Update Current Controls
Update Residual Occurrence Ranking

Figure 6 Failure Mode and Effects Analysis

In Figure 6 an FMEA's purpose is to evaluate and mitigate risks in a continual loop until marginal returns set in. First, review or update all failure modes. Then all risks are controlled if each has been mitigated in turn. Next update each risk's severity ranking. What is residual after mitigations or controls or detections are applied? Identify new causes and new risks for new iterations. Update each risk's residual occurrence and ranking. Then identify or update current controls that are in place. Knowing this, update the residual detection ranking and recalculate the RPN. Lastly, review and make sure all updates have been applied, and newly identified risks have been analyzed and mitigated or controlled.

Detection to the Rescue

UNDERSTANDING DETECTION

Detection is the likelihood current controls will not detect risks before product reaches a user. (See sidebar for a more complete working definition.) A higher Detection rating does its job by raising the overall priority (RPN) of a risk so that it receives appropriate attention and resources to mitigate and/or control severity and/or likelihood of harm. Detection is never a mitigation of risk. Detection [-based] controls are intended to increase the likelihood that a risk will be detected before it reaches a user. Mitigation is what is done to reduce a risk's severity and probability.

Unfortunate examples can lead to confusion. Figure 7 shows a simple model with processes from Design to Use. In this model the product has two components. One goes inside the other during manufacturing. The two components have separate designs. In our fictitious model when assembled a potential problem arises. The red dot indicates where. "When" is another story. It could be introduced during any stage of development or manufacture.

"Detection" is a ranking number that reflects the likelihood your current best controls in their best configuration will not detect a failure mode, assuming it, or one of its causes, is present before the product reaches a user, regardless of when it fails, regardless of the likelihood the failure mode is present, and regardless of the severity when it fails. It is a relative ranking within the scope of the specific product or project.

The fault could be any kind of problem: material, dimensional, electrical, a software bug. (Big jet manufacturers combine all their system models, like electrical, signal, hydraulic, air and water to avoid dangerous conflicts.)

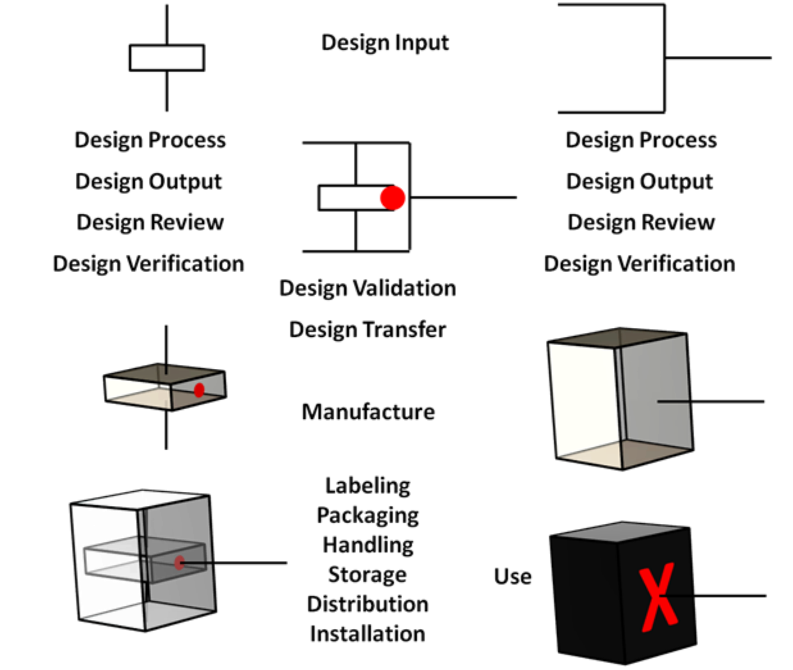

Figure 7 Detection Example

The two paths join for Design Validation and Design Transfer. It would be good to detect risks here. In fact, every process is an opportunity to detect risks. It should be built into their definition. The earlier a risk is detected, the easier and cheaper it is to remedy. 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. For future detection.

Detection to the Rescue

Your risk vault should drive planning and process 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.

Once a product is in the hands or use by a customer or patient, there is little chance of prevention. The opportunity of detection is gone. Detection was never about discovering harm from a failure after it occurred. It was always about discovering the fault before it occurred. Mitigation is doing something to prevent or reduce the harm. Like adding a requirement for software, or for a safety need. Maybe changing a process. Adding an inspection. Adding a test.

> Your risk vault has great economical value for your organization as well. In contract bidding, you only want to win when it would be profitable. Risk management plays a big part in this. Knowing your costs is a great asset.

In addition to consulting, I teach risk management. And all my students leave their 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.

REFERENCES

[1] “What’s Behind MetTech’s Recall Epidemic?” by Joshua R. Dix, Suraj Ramachandran, and Darin S. Oppenheimer.
[2] 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)*
[3] Carlson, C. S. (2012). *Effective FMEAs: achieving safe, reliable, and economical products and processes using failure mode and effects analysis, p.145*. Hoboken, N.J: Wiley.

Richard L. Bollinger is CEO of Menlo Park Associates, a management consulting firm. You can reach him at rick@menloparkassociates.com.