

Risk Management Series - Part 4: Transferring Risks from Fault Trees to FMEAs

Foreword

MEDicept is presenting this ongoing series of articles focused on the implementation and practical conduct of risk management in the medical device industry to provide practitioners with insight into how to apply risk management principles and tools to improve the safety and effectiveness of their devices; and, as an added benefit, to maintain compliance with risk management standards.

Our team at MEDicept, publishes these articles to capture best practices, to explore the more challenging aspects of maintaining risk management systems over the long term, and to elicit discussions among practitioners.

To this last point, if you have questions or comments on the issues discussed, or if you have recommendations for topics to consider in the future, please let us know: 508-231-8842.

In our last article, *Part 3: Using Fault Trees to Focus and Simplify Risk Analysis*, we described the basic approach for conducting a Fault Tree Analysis (FTA) and the benefits of using FTA to conduct a comprehensive analysis of the causes of device failures and use errors. We also identified a few weaknesses of the FTA approach – i.e., its structure can be un-wieldy, and there is no efficient way to track the implementation of needed mitigations, or to document that you’ve verified that the mitigations are effective. These weaknesses happen to be two of the strengths of the FMEA risk analysis format. Therefore, this article describes an approach for transferring risk information from a completed FTA to an FMEA so that you will be able to take advantage of the strengths of both.

I’ve finished the FTA . . . Now What?

As discussed in *Part 3: Using Fault Trees to Focus and Simplify Risk Analysis*, FTAs can be valuable tools as you work to improve the safety and effectiveness of your medical device. They help to ensure that your risk analysis is comprehensive, and they can help you set priorities for where and how to implement needed mitigations. Most companies, however, will want to take what they learned from the FTA and move it into a FMEA format. There are a few reasons for this:

- The FTA structure is not designed to support the easy evaluation of risk acceptability;
- FTA does not allow for easy tracking of the implementation and verification of mitigations; and
- Many companies require that final risk analyses be in the FMEA format.

However, you might ask, “Won’t you lose some of the important information from the FTA when you move its output into the FMEA format?” The answer is . . . “Yes, but not entirely”. When you move information from an FTA, which illustrates the relationships among causes, to the more linear FMEA format, the details of the causal relationships will not show up in the FMEA - but they won’t be lost. The FTA will be referenced in the FMEA (or at least included as an attachment), so you can always refer back

to it to understand the thinking that went into the analysis. All that you need to transfer to the FMEA is overall risks and the underlying causes that are associated with planned mitigations.

In the end, you'll be in a much better position than if you had gone straight to the FMEA. In most FMEA sessions, the details of the causal relationships may be discussed by the analysis team, but those details rarely make it into the FMEA. As a result, these important details will be maintained only in the memories of individual team members. With the FTAs included as attachments to the FMEA, your team will have a much better record of the original team's thinking when you go back and update the risk assessment in response to a design change or as part of a regular review.

When transferring FTA information into a FMEA, follow the two main steps:

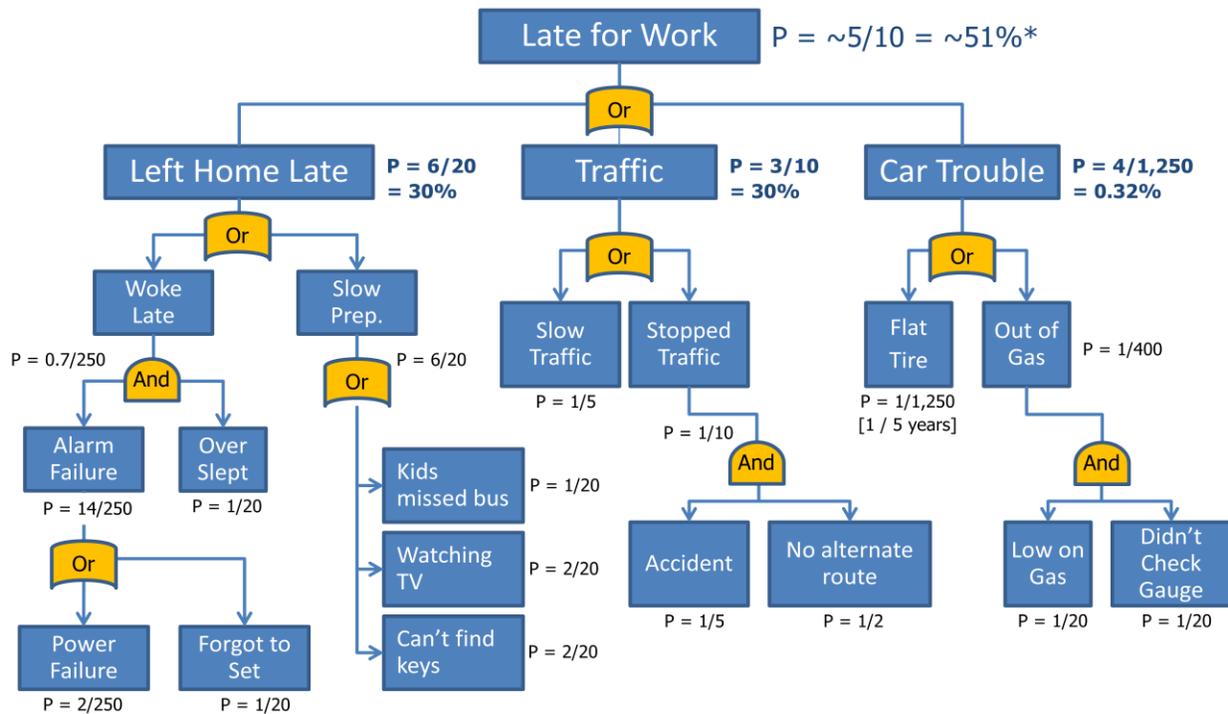
1. Complete the evaluation of risk acceptability (to confirm that a mitigation is needed); and
2. Record risk information in the FMEA relevant to the cause(s) and mitigations.

The balance of this article addresses these two points.

Transferring Risks from FTA to FMEA

To illustrate how to transfer FTA information into a FMEA, we'll go back to the "Late for Work" fault tree created in the previous article (see Figure 1).

Figure 1: "Late for Work" FTA



* $P(\text{Left Home Late}) + P(\text{Traffic}) + P(\text{Car Trouble}) - [P(\text{that combinations of the three events occur on the same day})]$

In this example, we identified three main causes for showing up late to work (left home late, traffic, and car trouble). We also identified the sub-causes and their relationships, and estimated the probability of occurrence for each cause. This is all good information, but there’s no context. Is showing up late for work 51% of the time a bad thing? Probably, but it depends a bit on the type of work you do and just how late you are. If you work independently and can make up your time by working through lunch or staying late, it’s probably not a big problem. If you’re a surgeon and a critical operation is scheduled for 9:00 am, it’s best to show up on time.

For a medical device company, risk acceptability criteria (pre-approved by management) establish the context for determining which risks are acceptable and which require mitigation. Figure 2 provides a simple table that we’ll use for evaluating the risks in our “late to work” example.

Figure 2 Risk Acceptability Matrix

Probability	Severity			
	1 Negligible/ Transient Effect	2 Delay in Treatment	3 Minor Injury	4 Serious Injury or Death
4 (> 50%)	Acceptable	UNACCEPTABLE	UNACCEPTABLE	UNACCEPTABLE
3 (26 – 50%)	Acceptable	Acceptable	UNACCEPTABLE	UNACCEPTABLE
2 (10 – 25%)	Acceptable	Acceptable	Acceptable	UNACCEPTABLE
1 (< 10%)	Acceptable	Acceptable	Acceptable	Acceptable

For the purpose of our example, let’s say that our surgeon’s late arrival will cause a “Delay in Treatment,” which has a severity score of “2.” When transferred to the FMEA format (see Figure 3), we are able to see that the overall risk of “Late for Work” (i.e., a 51% chance of a “Delay in Treatment”) is not acceptable.

Figure 3: Sample FMEA, Un-Mitigated Risk

Failure Mode	Effect of Failure	Severity	Cause	P(Occur.)	Un-Mitigated Risk
1. Late for Work	Delay in Treatment	2	Overall	4	UNACCEPTABLE
-	-	-	Left home late	3	Acceptable
-	-	-	Traffic	3	Acceptable
-	-	-	Car Trouble	1	Acceptable

There’s no need to transfer any additional information from the FTA to the FMEA. All of the lower-level causes identified in the FTA can be left in the FTA. Any selected mitigations associated with a branch of

the FTA (i.e., left home late, traffic, or car trouble) can be identified and assessed within those rows of the FMEA.

Seeing the Forest from the Trees

This example also illustrates one of the benefits that you will gain when working with data from an FTA. By using the FTA approach, you are able to identify the probability of occurrence for the top-level “Late to Work” fault (51%), which is not generally captured in a typical FMEA. In an FMEA, the top-level fault is usually broken down into lower-level faults – each with a smaller probability of occurrence. As a result, each lower-level cause might be considered “Acceptable”, even though when you add up all the individual risks the overall risk is “Unacceptable.”

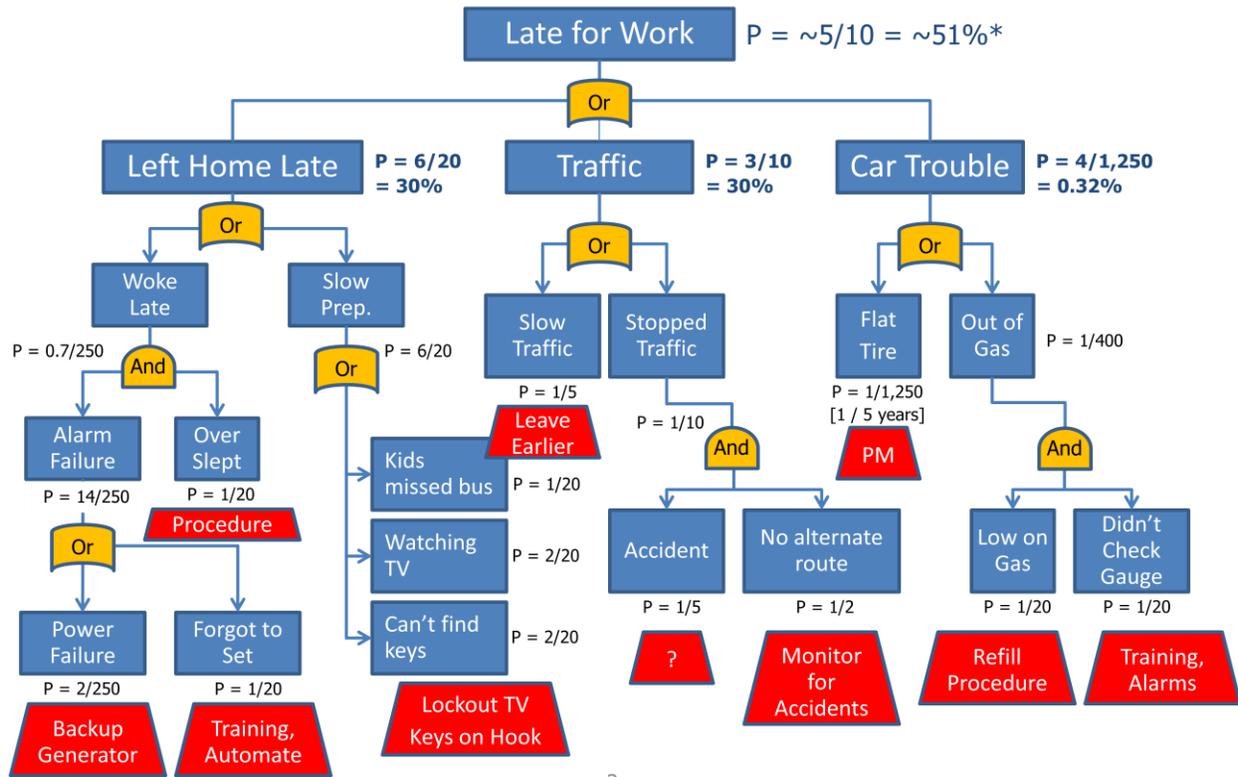
For example, consider a device and the risk of infection. There may be multiple causes that could lead to a patient getting an infection from a medical device (e.g., manufacturing contamination, poor package seal, inadequate sterilization, package damage, poor handling, etc.). If each of these routes to infection are considered individually (typical of an FMEA), the individual probabilities may be low enough that each individual risk is considered to be acceptable. However, if the overall probability of infection is considered (i.e., the top-level fault), it may not be acceptable. You can imagine a failure mode with 10 different (independent) causes. If each cause has a 1/1,000 chance of occurring, they may each be acceptable, but when considered together, the 1/100 chance of occurrence may not be.

The objective is to keep the top-level fault from occurring. You don’t want to be in a situation where you decide that mitigations are not needed because you’ve only considered the probability of a bunch of low level causes that appear to be acceptable. The focus needs to be on overall safety.

How do I Pick Mitigations?

Going back to our example, there are a lot of actions we could take to mitigate the risk of showing up late to work. Figure 4 identifies a variety of mitigations that could be implemented. Are they all needed? That’s unlikely. Some mitigations would be redundant and others would involve complex fixes to problems that rarely occur. For example, the backup generator for the alarm clock would be a complex fix to a relatively low-probability event. And since “Car Trouble” is estimated to cause our doctor to be late only 0.32 percent of the time, any mitigations in that area would have a negligible impact on the overall probability of occurrence.

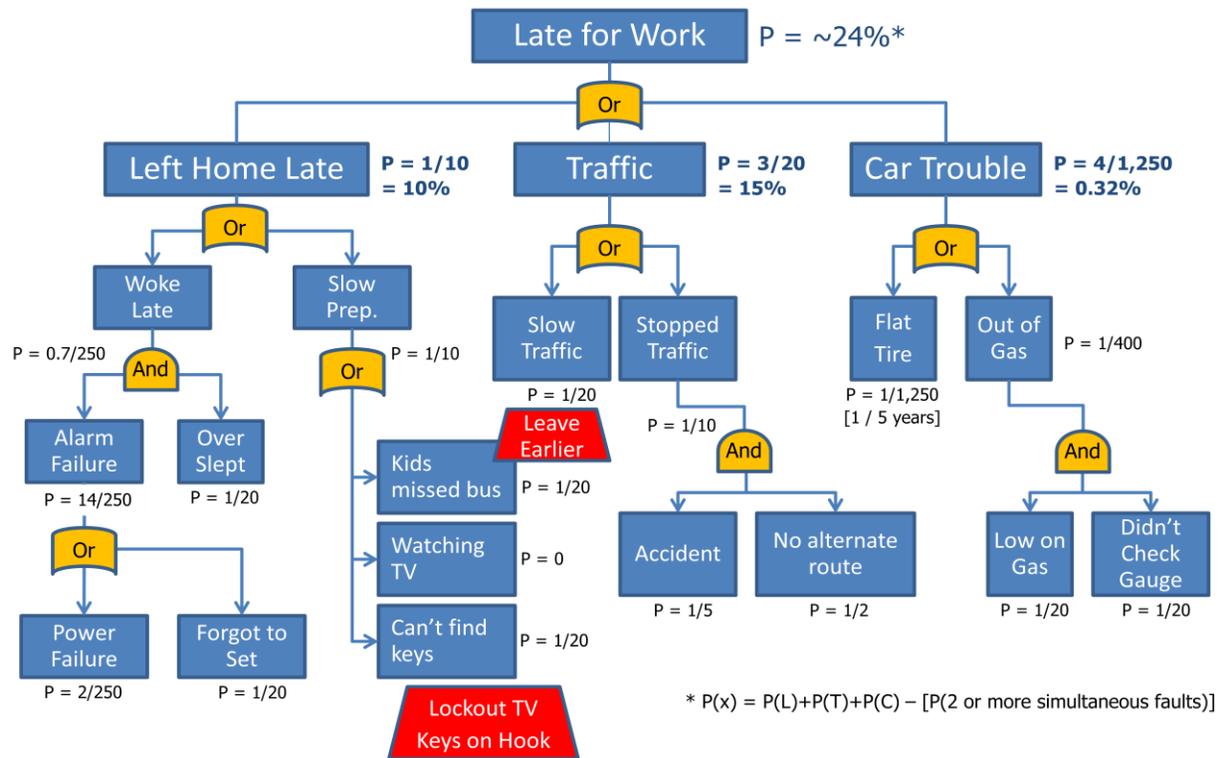
Figure 4: "Late for Work" FTA, With Mitigations



3

Looking at our options, establishing a procedure where the doctor leaves home earlier each day, keeps the car keys on a hook near the door, and locks out the TV so that it can't be turned on in the morning seem to be the most practical risk reduction actions. We estimate that leaving home earlier will make being late due to slow traffic four times less likely to occur, and keeping the keys on the hook will reduce the probability of that cause occurring by about half. Locking out the TV will totally eliminate that cause from delaying our commuter. As shown in Figure 5, these three mitigations reduce our overall probability of being late from about 51% to about 24%, which according to our risk acceptability table is acceptable.

Figure 5: “Late for Work” FTA, With Mitigations and Revised Probabilities



Is getting down to a 24% chance of occurrence good enough? That’s debatable. There are a few other causes that have a significant impact on the overall likelihood of occurrence. For example if there are some practical methods to ensure that the kids don’t miss the bus (or someone else can get them to school if they do), that might be worth considering. It’s the responsibility of the risk analysis team, and ultimately their management, to determine what risks are acceptable when “weighed against the benefits to the patient and are compatible with a high level of protection of health and safety.”¹

Again, when transferring information from the FTA to an FMEA format, only the primary causes (e.g., Left Home Late, Traffic, and Car Trouble) need to be listed in separate rows. You can then list the planned mitigations (if any) associated with those causes so that the risk reduction benefit of the mitigations can be clearly captured – see Figure 6. Ultimately, references will need to be added to a Verification column to provide evidence that the mitigation did, in fact, achieve the desired objective.

¹ Medical Device Directive (93/42/EEC: 2007-47-EC) Annex I, which is referenced in the Z annexes of EN ISO 14971:2012.

Figure 6: Sample FMEA, Un-Mitigated and Mitigated Risks

Failure Mode	Effect of Failure	S	Cause	P(O)	U-M Risk	Recommended Actions	M P(O)	M-Risk
1. Late for Work	Delay in Treatment (2)	2	Overall	4	Un	See below	2	Acc
-	-	-	Left home late	3	Acc	Lock out TV SOP: Keys on hook	2	Acc
-	-	-	Traffic	3	Acc	SOP: Leave earlier	2	Acc
-	-	-	Car Trouble	1	Acc	No action required	1	Acc

S = Severity
P(O) = Probability of Occurrence of harm
M = Mitigated
UM = Unmitigated
Un = Unacceptable
Acc = Acceptable

Next Steps

So far in our series, we have emphasized the need to recognize that risk management is not simply a set of forms to satisfy regulators, but rather it serves as a critical element in your efforts to ensure the safety of your medical devices throughout their lifecycles. We then introduced an approach to help prioritize your risk analysis efforts and recommended the use of Fault Tree Analysis (FTA) to gain a more complete understanding of safety risks. Now that we've identified how the FTA results can be fed back into your FMEA format, in the next article we'll begin to dig into the challenges of using the FMEA process to guide decisions that will improve device safety.