Table of Contents

Failure Mode and Effect Analysis

Failure Mode and Effect Analysis (FMEA) is a very common structured analysis method used to assure product reliability and safety. It is used to identify how a product can fail (its failure modes), the causes of those failures, and the effects of the failures on system/product performance.

Overview

FMEA is commonly used after a designed product is sold and in use, and uses available data about actual failures to identify and prioritize problems in the product's design.

However, FMEA can and should also be used early in the product development process to help catch and remedy design flaws as early as possible.

In many ways, FMEA is a more structured way to implement the why why why method of finding root causes of undesired situations (i.e. failures).

FMEA can be used for various other kinds of design analyses, including:

- system safety analyses;
- production planning;
- test planning & validation;
- repair level analyses;
- logistics support planning;
- maintenance planning;
- etc.

A *failure mode* is a way in which a system or component might fail. Some failure modes include: yielding, ductile rupture, fatigue, wear, impact, etc. There are many modes that result from interaction with other systems or users, e.g. entering the wrong data to a program, executing tasks in the wrong order, etc. Some typical generic modes of failure include:

- premature operation of a component
- failure of a component to operate at the prescribed time/condition
- failure of a component during operation
- failure of a component to stop operating at a prescribed time/condition

There are two ways in which FMEA can be applied:

- **Top-down, functional approach:** This approach is used in early design, before parts have been identified. The goal here is to look for logic errors in the expected function and operation of a product. One identifies a failure mode for the product as a whole, then traces its causes "down" into subsystems or subfunctions.
- **Bottom-up, structural approach:** This approach is used when specific parts or at least major assemblies have been designed. The goal here is to look for physical errors in the detailed design/manufacture of parts. One identifies a failure mode, and then follows its effects "up" to the

product as a whole in order to predict how the product will respond to the failure.

The bottom-up approach is used more often – typically because short lead-times do not allow the time to do the top-down approach during the design process itself.

The main interest here is in the top-down approach, because from an engineering standpoint, it is more likely to generate more reliable designs over entire development programs.

NOTES:

- A FMEA is only as good as the diligence of the engineers carrying it out. That is, FMEA depends on being able to identify all the modes of failure. Overlooking even one mode can, in principle, completely invalidate the FMEA. So FMEA is not a silver-bullet solution, but just a guide that will improve (but not perfect) your design.
- Human factors (i.e. "human error") are not considered in a FMEA. The focus of FMEA is on making sure the product works as it is supposed to. It is a different matter to make sure the product can be used correctly.

Quantifying FMEA data

Depending on how much information is available about a product, there are three general ways to "measure" failures and their effects.

Failures are generally measured in terms of their *criticality*, which is typically the sum of a failure's *severity* and its *probability*. Details will vary from one implementation of FMEA to another.

- **Probabilistic data:** If the product exists, and malfunctions, and there is data about the actual failures, then probabilities can be generated to establish both the probability of occurrence of a failure and the severity of the failure's effects.
- **Qualitative Probability and Severity indices:** If data on actual failures is missing, but the product has already been designed (or is nearly so), then one can use a qualitative but discrete scale to measure the probability and severity of a failure, then add them in some way. For example, one might use a 3-point scale where 0 = unlikely and not severe, 1 = somewhat likely and moderately severe, and 2 = likely and severe.
- **Qualitative Criticality indices:** If the design is still in the early stages, there is not even enough information available for assessing the probability and severity separately. In this case, one can assign a qualitative criticality measure as a single value.

Sometimes, a third element, *detection*, is also added. Detection can be a probabilistic or qualitative measure of the likelihood that the failure mode will be actually detected before the failure occurs.

- See Also: MIL-STD-882B Hazard Risk Assessment Matrix

The FMEA method

Determine FMEA scope

One typically has either not enough information or not enough time/money to conduct a complete FMEA. It is important to set a goal of the level of detail to which the FMEA is to be carried out.

Also, FMEA should be intended to determine the effects of failure modes on specific factors, such as safety, mission outcomes, or repair costs.

Develop a product architecture

Failures occur due to activities by the product or its users/environment. Activities involve interactions between product components. At the very least, then, a preliminary systems design must have been carried out.

Typically, systems are represented in some kind of block diagram indicating the major functional components of the system and their interactions. Such schematics are often called *product architectures*.

Developing a product architecture is a key element of Systems design.

Identify failure modes

For each system component (not necessarily parts), identify possible failure modes, including how (operationally) the failure might happen.

For example, one failure mode is corrosion, which might cause a metal pipe under a kitchen sink to develop a leak. The *how* of this failure mode might be: *water and foreign materials will act chemically on the metal over time*.

Determine root causes

This is where the why why why method can come in again.

The *root cause* of a failure is the most basic reason for a failure that can be reasonably determined. For example, the root cause of the leaky pipe mentioned above might be a lack of appropriate coating on the inside surface of the pipe.

Determine effects

Given a failure mode and its cause, what _effects_ will the failure have on the "containing" system? In the

case of the leaky pipe, some effects include:

- damage could result to contents of under-sink cabinets
- if water escapes from the cabinet and gets on a floor, someone could slip and fall
- if the leak is/becomes large enough, flooding could occur leading to water damage to many other parts of a house

Quantify the failure and its effects

Classify the severity of the failure effects. One often used scale (from MIL-STD-882B[1] is:

1. negligible (less than minor injury, illness, or system damage)
2. marginal (minor injury, occupational illness, or system damage)
3. critical (severe injury, occupational illness, or system damage)
4. catastrophic (death or system loss)

Classify the probability of the failure mode. One often used scale is:

1. extremely remote (unlikely to occur over any reasonable timeframe)
2. remote (will probably not occur at some time)
3. reasonably probable (will probably occur eventually)
4. probable (likely to occur in a short time)

If detection is also being considered, an analogous 4-point scale can be used to determine qualitative values for it.

Typically, the values for severity and probability (and detection) are just added together. The higher the sum, the greater the risk arising from that particular failure mode.

Tabulate the results

The tabulated form makes it easier to look for the greatest risks and allocate the most resources to dealing with them. FMEA tables are augmented with extra data explaining why particular choices of values were made.

Here are two simpler examples of FMEA tables, based on [Pug91]. The weights were calculated using pairwise comparison[2]. The rankings were arrived at by summing individual rankings of severity and probability on the 4-point scale noted above. (Detection was not considered.)

Here is a sample FMEA for the _parts_ of a lead pencil.

Part	Weight	Failure Modes				Total	%
		Breaks	Falls Apart	Smudges	Wears Out		
Lead	40%	8 (3.2)		4 (1.6)	8 (3.2)	8	48
Wood	40%	8 (3.2)	8 (3.2)			6.4	39

Part	Weight	Failure Modes				Total	%
		Breaks	Falls Apart	Smudges	Wears Out		
Eraser	5%	2 (0.1)	2 (0.1)	8 (0.4)	8 (0.4)	1	6
Eraser Holder	15%		8 (1.2)			1.2	7
Total						**16.6**	**100**

Here is a sample FMEA for the _functions_ of a paperclip.

Function	Weight	Failure Modes					Total	%
		Release paper	Wire snaps	Snags	Corrodes	Catches clothing		
Hold papers	50%	8 (4)		8 (4)	2 (1)	4 (2)	11	71
Reusability	20%	4 (0.8)	2 (0.4)	4 (0.8)	2 (0.4)		2.4	16
Toothpick	10%		1 (0.1)			3 (0.3)	0.4	3
Stress relief	20%		8 (1.6)				1.6	10
Total							**15.4**	**100**

Address each failure mode

Now that one can estimate what can go wrong, one can look at trying to fix the problems before they actually occur. Addressing each failure mode can be looked at as a design task in itself.

Generally, there are two strategies to treat failure modes: _failsafe_ (FS), and _fail operational, fail safe_ (FOFS). In the first case, failure of a component will cause the system to shut down in a controlled (safe) way. In the second case, the system remains (possibly only partially) operational after the first component failure, and shuts down safely after the second failure. Both strategies can be used in the same general product. For example, in a multi-engine airplane, failure of one engine causes the engine to shut down in failsafe mode, while the aircraft itself can continue to fly (FOFS).

Some typical ways that failure modes are addressed are:

- Redundancy: two or more identical elements working in parallel, such that system performance remains acceptable if one (or more) of the elements fail.
- Compensatory: one or more backup devices are in place (i.e. serial rather than parallel arrangement) in the event that a primary devices fails.
- Preventative Maintenance: critical elements are more carefully inspected and maintained more often to reduce the likelihood of failure.
- Design it right: if FMEA is done early enough in the design process, the product can be redesigned to avoid failure modes at minimal expense.

Shortcomings of FMEA

- If designers do not recognize a particular failure mode, then it cannot be addressed.
- Multiple-failure interactions are typically not treated due to the extreme complexity of such problems.
- Risks from the proper operation of a product are not assessed by FMEA.
- Human factors are typically not considered.

REFERENCES

[Pug91]. S. Pugh. 1991. **Total design: integrated methods for successful product engineering**. Addison-Wesley, England.

analysis, tool, method, behaviour

[1]

MIL-STD-882B has been revised several times. MIL-STD-882D was approved in Feb 2000. There's a draft of a rev E floating on the Web, dated 2005, but it doesn't seem to have been approved yet. Corrections to this are welcome. The point is: insofar as FMEA is concerned, not much has changed.

[2]

Bet you didn't see that coming!

From:
https://deseng.ryerson.ca/dokuwiki/ - **DesignWIKI**

Permanent link:
https://deseng.ryerson.ca/dokuwiki/design:failure_mode_and_effect_analysis

Last update: **2020.03.12 13:30**