Laboratory 1

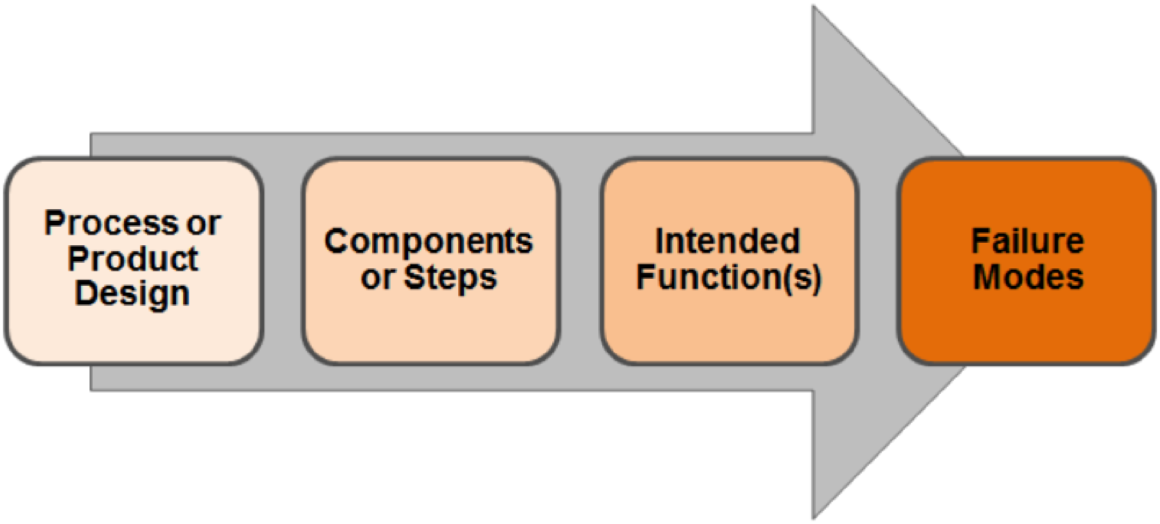
Failure mode and effects analysis (**FMEA**)—also "**failure modes**", plural, in many publications – was one of the first *highly structured, systematic* techniques for failure analysis. It was developed by reliability engineers in the late 1950s to study problems that might arise from malfunctions of military systems. A FMEA is often the first step of a system reliability study. It involves reviewing as many components, assemblies, and subsystems as possible to identify failure modes, and their causes and effects. For each component, the failure modes and their resulting effects on the rest of the system are recorded in a specific FMEA worksheet. There are numerous variations of such worksheets. A FMEA can be a qualitative analysis, but may be put on a quantitative basis when mathematical failure rate models are combined with a statistical failure mode ratio database [1].

An FMEA is a study to recognize the potential modes of failure, identify the effects of those failures and conduct an analysis to determine which failure modes have the highest risks relative to each other [4].

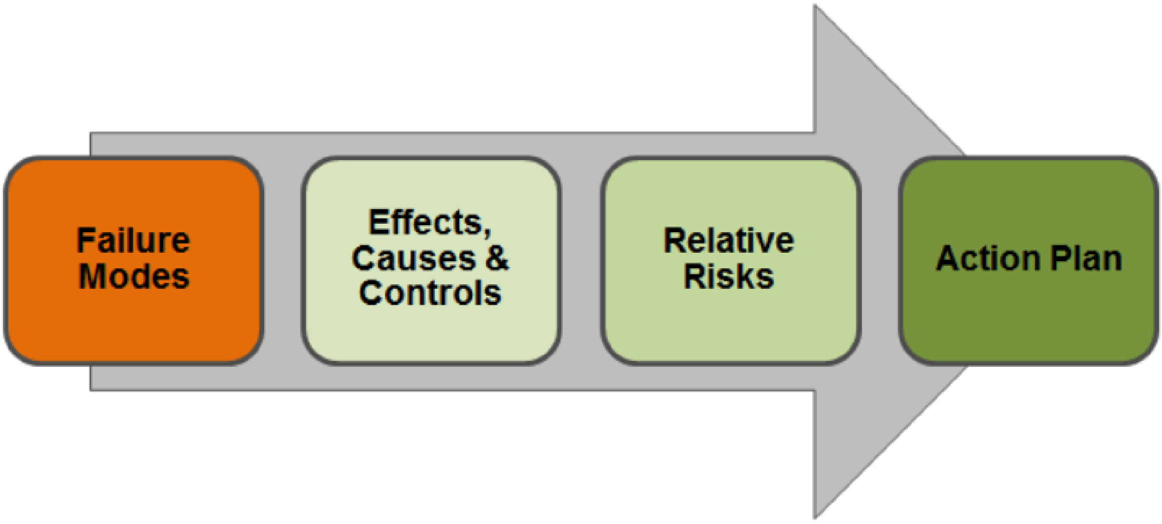
Simply put, an FMEA is a tool that allows us to identify the relative risks designed into the process or product; trigger action to reduce those with the highest potential risk; and track the results of the action plan in terms of risk reduction [4].

An FMEA will rate the magnitude of one risk relative to another. This provides a mechanism to prioritize risks. Focused action plans are developed and executed for the high risks while those failure modes with low potential risks are deemed acceptable.

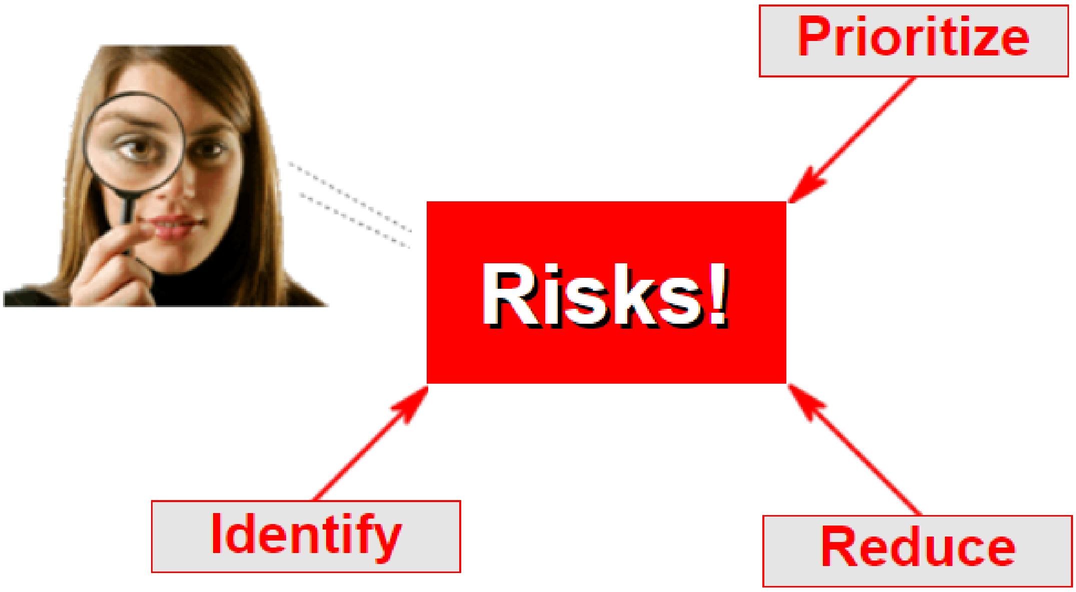
Let's take a look at how an FMEA works. To conduct an FMEA we will focus on either a process or product design. To begin the FMEA, break the process or product down into components or steps. Then for each component, identify their associated functions.



Next, we will identify the corresponding effect, cause, and controls of each potential failure mode. Then, we will rank the relative risk of the failure modes. Finally, we'll develop an action plan to reduce the risk.

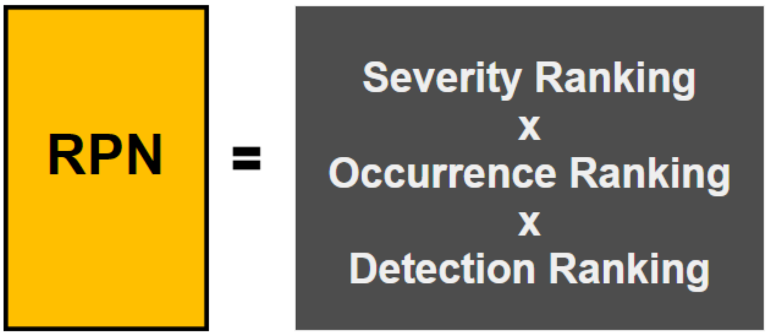


An FMEA is a tool that helps us focus on and understand potential process or product risks. During the course of an FMEA study, we will identify potential risks, prioritize them in ranked order, and then develop an action plan to reduce the risks associated with the product or process under study [4].

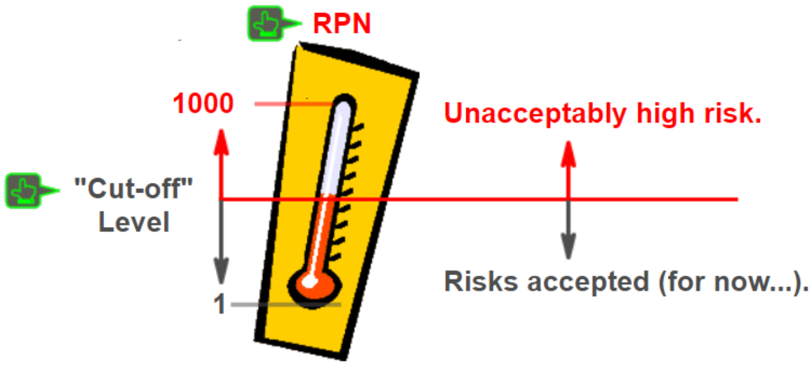


The FMEA process will lead us through a systematic approach, getting us to dig into the details of the product or process under study to identify potential risks. The step-by-step process will enable us to prioritize potential risks using a relative ranking scale [4].

With FMEAs, risk is a function of three factors. First, the severity of the effect of a failure; second, the frequency of the occurrence of the failure or cause of the failure; and third, the ability to detect the failure, effect of failure, or cause of failure before or after it has occurred. Your team will evaluate each failure mode and effect in terms of these three factors and the result will be a Risk Priority Number, or RPN. We'll use the RPN to rank the relative priority of the risks associated with the product or process.

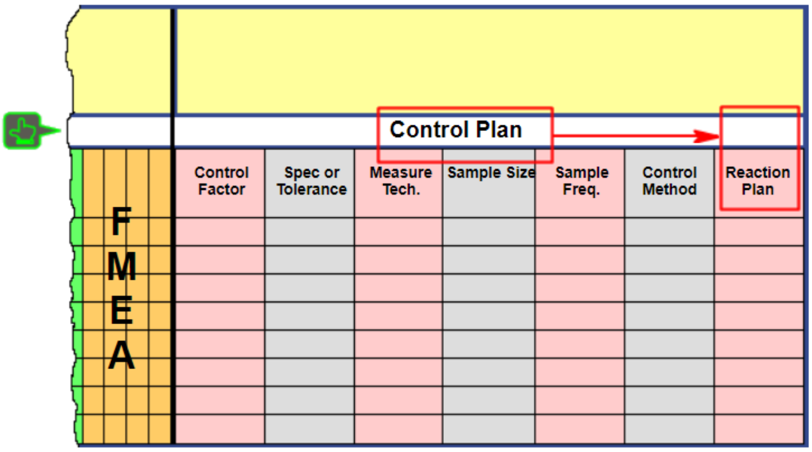


Since the risks are ranked on a relative scale, the higher the RPN, the higher the relative level of risks. The lowest possible RPN value is 1, the highest is 1,000. Your company may set a maximum allowable RPN. Any failure mode and effect with an RPN above the maximum RPN is considered to be an unacceptable risk; an action plan to reduce the risk level is required.



Most action plans developed to reduce risk are simple action plans that define who will do what by when. The RPN can be reduced by lowering the ranking for any one or any combination of the three factors that make up the RPN calculation: the severity ranking, the occurrence ranking, and the detection ranking.

FMEAs are the basis for developing Control Plans. Control Plans involve monitoring and measuring critical product or process characteristics and end up with a Reaction Plan to respond to any potential failures identified. This assures we have a well thought out plan not only to proactively work to prevent failures but to react to a failure if one does occur.



Even though we'll develop a Control Plan that includes a plan to react to a failure, the focus of FMEAs is on preventing failures before they occur, not reacting to them after an event [4].

A few different types of FMEA analyses exist, such as:

- Functional
- Design
- Process

Sometimes FMEA is extended to FMECA (failure mode, effects, and criticality analysis) to indicate that criticality analysis is performed too [1].

FMEA is an inductive reasoning (forward logic) single point of failure analysis and is a core task in reliability engineering, safety engineering and quality engineering.

A successful FMEA activity helps identify potential failure modes based on experience with similar products and processes—or based on common physics of failure logic. It is widely used in development and manufacturing industries in various phases of the product life cycle. *Effects analysis* refers to studying the consequences of those failures on different system levels.

Functional analyses are needed as an input to determine correct failure modes, at all system levels, both for functional FMEA or Piece-Part (hardware) FMEA. An FMEA is used to structure Mitigation for Risk reduction based on either failure (mode) effect severity reduction or based on lowering the probability of failure or both. The FMEA is in principle a full inductive (forward logic) analysis, however the failure probability can only be estimated or reduced by understanding the *failure mechanism*. Hence, FMEA may include information on causes of failure (deductive analysis) to reduce the possibility of occurrence by eliminating identified *(root) causes* [1].

The FME(C)A is a design tool used to systematically analyse postulated component failures and identify the resultant effects on system operations. The analysis is sometimes characterized as consisting of two sub-analyses, the first being the failure modes and effects analysis (FMEA), and the second, the criticality analysis (CA). Successful development of an FMEA requires that the analyst include all significant failure modes for each contributing element or part in the system. FMEAs can be performed at the system, subsystem, assembly, subassembly or part level. The FMECA should be a living document during development of a hardware design. It should be scheduled and completed concurrently with the design. If completed in a timely manner, the FMECA can help guide design decisions. The usefulness of the FMECA as a design tool and in the decision-making process is dependent on the effectiveness and timeliness with which design problems are identified. Timeliness is probably the most important consideration. In the extreme case, the FMECA would be of little value to the design decision process if the analysis is performed after the hardware is built. While the FMECA identifies all part failure modes, its primary benefit is the early identification of all critical and catastrophic subsystem or system failure modes so they can be eliminated or minimized through design modification at the earliest point in the development effort; therefore, the FMECA should be performed at the system level as soon as preliminary design information is available and extended to the lower levels as the detail design progresses [1].

Ground rules

The ground rules of each FMEA include a set of project selected procedures; the assumptions on which the analysis is based; the hardware that has been included and excluded from the analysis and the rationale for the exclusions. The ground rules also describe the indenture level of the analysis, the basic hardware status, and the criteria for system and mission success. Every effort should be made to define all ground rules before the FMEA begins; however, the ground rules may be expanded and clarified as the analysis proceeds. A typical set of ground rules (assumptions) follows [1]:

1. Only one failure mode exists at a time.
2. All inputs (including software commands) to the item being analysed are present and at nominal values.
3. All consumables are present in sufficient quantities.
4. Nominal power is available

Benefits

Major benefits derived from a properly implemented FMECA effort are as follows:

1. It provides a documented method for selecting a design with a high probability of successful operation and safety.
2. A documented uniform method of assessing potential failure mechanisms, failure modes and their impact on system operation, resulting in a list of failure modes ranked according to the seriousness of their system impact and likelihood of occurrence.
3. Early identification of single failure points (SFPS) and system interface problems, which may be critical to mission success and/or safety. They also provide a method of verifying that switching between redundant elements is not jeopardized by postulated single failures.
4. An effective method for evaluating the effect of proposed changes to the design and/or operational procedures on mission success and safety.
5. A basis for in-flight troubleshooting procedures and for locating performance monitoring and fault-detection devices.
6. Criteria for early planning of tests.

From the above list, early identifications of SFPS, input to the troubleshooting procedure and locating of performance monitoring / fault detection devices are probably the most important benefits of the FMECA. In addition, the FMECA procedures are straightforward and allow orderly evaluation of the design.

Basic Items

The following covers some basic FMEA terminology.

Failure

The loss of a function under stated conditions.

Failure mode

The specific manner or way by which a failure occurs in terms of failure of the item (being a part or (sub) system) *function* under investigation; it may generally describe the way the failure occurs. It shall at least clearly describe a (end) failure state of the item (or function in case of a Functional FMEA) under consideration. It is the result of the failure mechanism (cause of the failure mode). *For example; a fully fractured axle, a deformed axle or a fully open or fully closed electrical contact are each a separate failure mode of a DFMEA, they would not be failure modes of a PFMEA. Here you examine your process, so process step x - insert drill bit, the failure mode would be insert wrong drill bit, the effect of this is too big a hole or too small a hole.*

Failure cause and/or mechanism

Defects in requirements, design, process, quality control, handling or part applications, which are the underlying cause or sequence of causes that initiate a process (mechanism) that leads to a failure mode over a certain time. A failure mode may have more causes. *For example; "fatigue or corrosion of a structural beam" or "fretting corrosion in an electrical contact" is a failure mechanism and in* *itself (likely) not a failure mode. The related failure mode (end state) is a "full fracture of structural beam" or "an open electrical contact". The initial cause might have been "Improper application of corrosion protection layer (paint)" and /or "(abnormal) vibration input from another (possibly failed) system".*

Failure effect

Immediate consequences of a failure on operation, function or functionality, or status of some item.

Indenture levels (bill of material or functional breakdown)

An identifier for system level and thereby item complexity. Complexity increases as levels are closer to one.

Local effect

The failure effect as it applies to the item under analysis.

Next higher-level effect

The failure effect as it applies at the next higher indenture level.

End effect

The failure effect at the highest indenture level or total system.

Detection

The means of detection of the failure mode by maintainer, operator or built in detection system, including estimated dormancy period (if applicable)

Probability

The likelihood of the failure occurring.

Risk Priority Number (RPN)

Severity (of the event) * Probability (of the event occurring) * Detection (Probability that the event would not be detected before the user was aware of it)

Severity

The consequences of a failure mode. Severity considers the worst potential consequence of a failure, determined by the degree of injury, property damage, system damage and/or time lost to repair the failure.

Remarks / mitigation / actions

Additional info, including the proposed mitigation or actions used to lower a risk or justify a risk level or scenario.