How to Assess Risk Using FMEA

FMEA, or Failure Mode and Effects Analysis, is a widely adopted approach for failure analysis and risk assessment. While each step of the FMEA process is crucial for a successful analysis, the risk assessment element is key to zeroing in on the most risk sensitive areas that must be addressed in order to meet your quality and safety objectives. How do you assess risk using your FMEA data? This paper will provide details on proven strategies for risk assessment in failure analyses.

RELYENCE CORPORATION

Table of Contents

FMEA: Failure Mode & Effects Analysis

FMEA, or Failure Mode and Effects Analysis, is a proven and widely adopted approach for failure analysis and risk assessment. Originating in the 1940s for use in the U.S. military, FMEA is now one of the most commonly used techniques in engineering for failure analysis of products and processes. FMEA is an organized, step-by-step process for comprehensively evaluating a system or process to identify potential failure modes and eliminate or mitigate those deemed most critical.

The FMEA process begins by identifying all possible failure modes of a product or process. The second step is to determine the possible causes and resulting effects of those potential failures. You then assess the risk level associated with each of the failure modes based on a set of established criteria. Finally, you find ways to detect, mitigate, or prevent failures in order to bring your product or process into alignment with your overall quality and risk goals.

Our New to FMEA article is a helpful introductory overview of FMEA concepts.

FMEA Risk Assessment Strategy

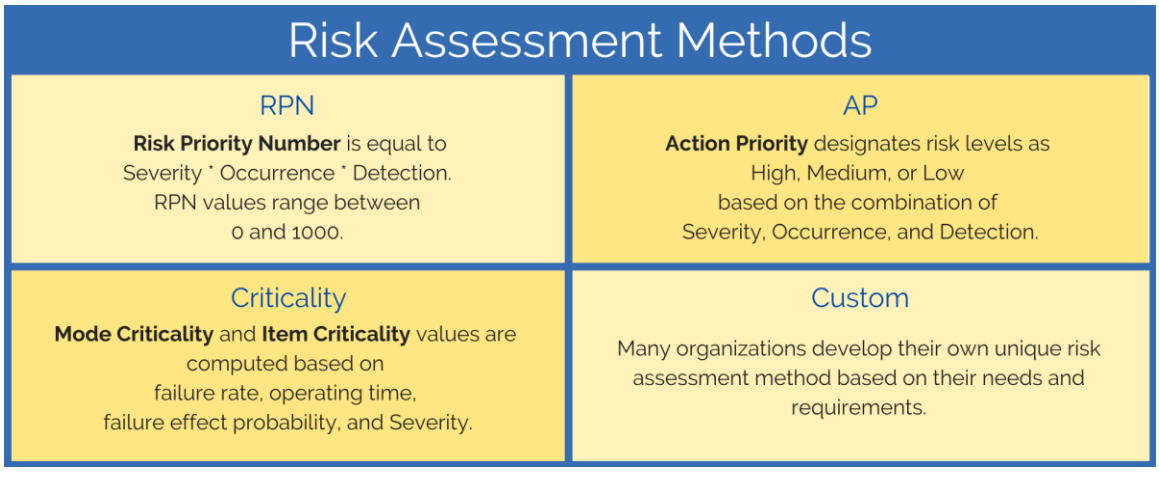
While each step of the FMEA process is crucial for a successful analysis, the risk assessment strategy you employ is vital in determining your action plan for product or process improvement. Essentially, ineffective risk assessment leads to an ineffective approach to risk reduction.

By utilizing a sound risk assessment strategy, you can easily determine the key areas to focus on for improvement. This ensures your team's efforts will be focused on those failures that are most critical. By targeting the key areas of concern for risk mitigation tasks, you can be confident you will meet your overall reliability and safety objectives.

There are various ways to assess the risk of the failures identified during the FMEA process. Three of the most commonly used approaches for risk assessment are:

1. RPN, or Risk Priority Number, defined in standards such as AIAG and SAE J1739
2. AP, or Action Priority, as defined in the FMEA Handbook from AIAG & VDA
3. Criticality as defined in MIL-STD-1629

To best suit their needs, organizations will choose to use one of the methods as defined in the handbooks, modify one of the methods, or create their own unique risk assessment method. By understanding the principles behind these assessment methodologies, you can decide which is the best approach for your organization.



Using RPN for Risk Assessment

RPN (Risk Priority Number) is a widely adopted method for risk assessment, and is used often in Design FMEAs (DFMEAs), Process FMEAs (PFMEAs), and other FMEA types. It has widespread use due to its longevity, ease of understanding, and effectiveness.

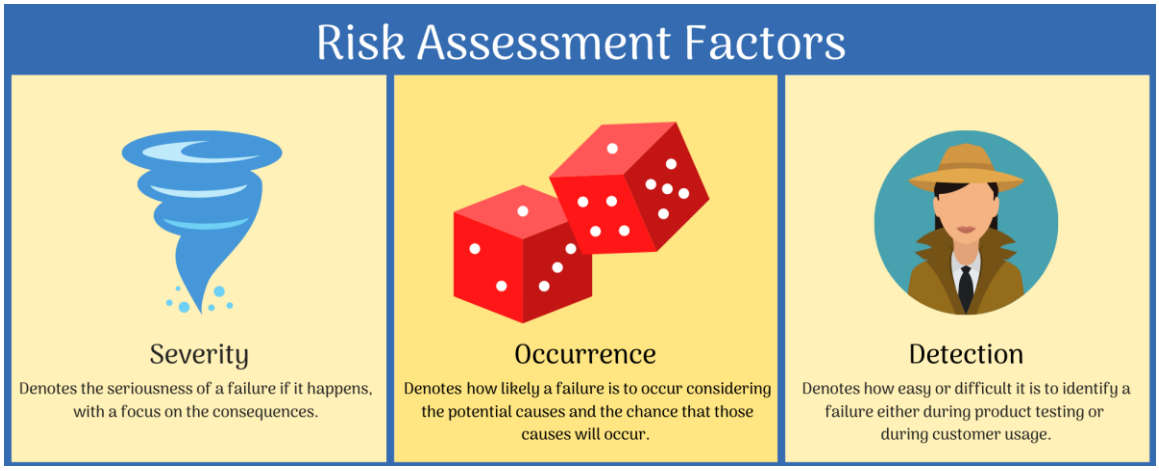
The first AIAG FMEA standard was published in 1993, so standards for FMEA practice have been in place for quite some time. The long historical roots of the AIAG standard is one of the reasons RPN is often employed for risk assessment in FMEAs. In addition, it is easily understood and implemented.

RPN provides a numerical result, and therefore, offers an intuitive approach to risk assessment: the higher the RPN value, the higher the risk. This makes it easier for companies to develop processes for handling risk. For example, an organization may institute a rule that no RPNs can be above a certain level prior to product release. In this manner, RPNs provide an easy way to assess risk and help in developing your risk mitigation plan.

RPN is determined based on three factors:

- Severity: Denotes the seriousness of the problem if it happens, with a focus on the consequences. The higher the number, the greater the severity.
- Occurrence: Denotes how likely the issue is to occur. To determine the rate of occurrence, you'll want to look at all the potential causes of a failure and the chance that those causes will occur. The higher the number, the greater the probability of occurrence.
- Detection: Denotes how easy or difficult it is to identify the problem. A higher rating means an issue is less likely to be detected either by engineers during the test phases of product development or by customers after product release. Therefore, the higher the number, the less likely the failure is detected.

RPN is calculated as Severity * Occurrence * Detection. Using a 1 to 10 scale for each factor results in RPN values ranging from 1 to 1000.



There are commonly used Severity, Occurrence, and Detection scales provided in FMEA standards. The rating scales found in AIAG and SAE standards are shown below. Though the wording is applicable to the automotive industry, you can easily see how it can be modified for use in other sectors.

The Severity rating scale:

Severity	Description
10	Potential failure mode affects safe vehicle operation and/or involves noncompliance with government regulation without warning.
9	Potential failure mode affects safe vehicle operation and/or involves noncompliance with government regulation with warning.
8	Loss of primary function (vehicle inoperable, does not affect safe vehicle operation).
7	Degradation of primary function (vehicle operable, but at reduced level of performance).
6	Loss of secondary function (vehicle operable, but comfort / convenience functions inoperable).
5	Degradation of secondary function (vehicle operable, but comfort / convenience functions at reduced level of performance).
4	Appearance or Audible Noise, vehicle operable, item does not conform and noticed by most customers (> 75%).
3	Appearance or Audible Noise, vehicle operable, item does not conform and noticed by many customers (50%).
2	Appearance or Audible Noise, vehicle operable, item does not conform and noticed by discriminating customers (< 25%).
1	No discernible effect.

The Occurrence rating scale:

Occurrence	Description
10	New technology/new design with no history.
9	Failure is inevitable with new design, new application, or change in duty cycle/operating conditions.
8	Failure is likely with new design, new application, or change in duty cycle/operating conditions.
7	Failure is uncertain with new design, new application, or change in duty cycle/operating conditions.
6	Frequent failures associated with similar designs or in design simulation and testing.
5	Occasional failures associated with similar designs or in design simulation and testing.
4	Isolated failures associated with similar design or in design simulation and testing.
3	Only isolated failures associated with almost identical design or in design simulation and testing.
2	No observed failures associated with almost identical design or in design simulation and testing.
1	Failure is eliminated through preventive control.

The Detection rating scale:

Detection	Description
10	No current design control; Cannot detect or is not analyzed.
9	Design analysis/detection controls have a weak detection capability; Virtual Analysis (e.g., CAE, FEA, etc.) is not correlated to expected actual operating conditions.
8	Product verification/validation after design freeze and prior to launch with pass/fail testing (Subsystem or system testing with acceptance criteria such as ride and handling, shipping evaluation, etc.).
7	Product verification/validation after design freeze and prior to launch with test to failure testing (Subsystem or system testing until failure occurs, testing of system interactions, etc.).
6	Product verification/validation after design freeze and prior to launch with degradation testing (Subsystem or system testing after durability test, e.g., function check).
5	Product validation (reliability testing, development or validation tests) prior to design freeze using pass/fail testing (e.g., acceptance criteria for performance, function checks, etc.).
4	Product validation (reliability testing, development or validation tests) prior to design freeze using test to failure (e.g., until leaks, yields, cracks, etc.).
3	Product validation (reliability testing, development or validation tests) prior to design freeze using degradation testing (e.g., data trends, before/after values, etc.).
2	Design analysis/detection controls have a strong detection capability. Virtual analysis (e.g., CAE, FEA, etc.) is highly correlated with actual or expected operating conditions prior to design freeze.
1	Failure cause or failure mode cannot occur because it is fully prevented through design solutions (e.g., proven design standard, best practice or common material, etc.).

As mentioned, organizations often adapt the rating scales to fit their requirements. For example, they may choose to define different scales for Severity, Occurrence, and Detection that use something other than 1 to 10 values. Or, they may decide to use less than 10 levels for a more concise list.

In addition, it is not uncommon for organizations to modify the RPN calculation itself. For example, perhaps you only want to focus on Severity and Occurrence. In that situation, you can define your RPN as Severity * Occurrence that results in values between 1 and 100 if using the 10 level Severity and Occurrence scales.

Essentially, RPN provides a solid starting point for thinking about how you best want to assess risk for your product or process.

Example Using RPN

The best way to understand how RPN is used is through an example. For our sample scenario, we'll consider a FMEA performed by a manufacturer of car batteries.

In this case, we'll zone in on one particular failure mode: the battery goes dead. For this failure mode, there are several causes and effects. For this example, one obvious effect is that the car does not start. One of the causes is that the driver failed to turn the headlights off.

We determine the RPN by analyzing the component factors:

1. Severity. Using the 1-10 scale, we determine the severity level is a 5. It is not a catastrophic failure, but one that is an annoyance, and clearly impacts customer satisfaction.

2. Occurrence. Using the 1-10 scale, we determine the occurrence level is a 7 due to the fact that if the headlights are left on there is a high likelihood this failure will occur.

3. Detection. In this case, there is no method of detection, so our Detection value is a 10, indicative of no detection.

The resulting RPN = Severity * Occurrence * Detection = 5 * 7 * 10 = 350.

Is an RPN of 350 high? It may be if you have a requirement that specifies that all RPNs must be less than 350. Or, it may be subjective based on your own situation. For example, you may decide any RPNs above 300 need to be investigated and that

RPNs above 500 are critical. In either case, the acceptable RPN level indicates your tolerable risk level and the quality you want to achieve.

	Function	Failure Mode	Effect	Severity	Cause	Occurrence	Detection	RPN
1	Provides convenient flying, aerial surveillance and video recording functionality and experience	Low battery life	Possible collision	7	Degraded battery	5	3	105
2					Cathode wear out	8	6	336
3		Battery leaking	Legal and safety issue	10	Manufacturing and packaging defects	2	2	40
4		Structural imbalance	Collision	10	Structural failure	7	8	560
5			Unable to fly straight	5	High winds and gusts	3	6	180
6					Motor malfunction	2	6	120
7	Provides the thrust and motion to the flight	Motor malfunction	Possible collision	7	Motor mechanical failure	2	6	84
8					Wear	6	8	336
9		Error in motor controller	Possible collision	7	High voltage	3	3	63

Example FMEA Worksheet using RPN

Using the Risk Matrix

Oftentimes, a risk matrix is employed in order to view overall system risk. A risk matrix provides a helpful visual overview of the RPNs across your FMEA.

Most commonly, the risk matrix is a graph of Severity vs Occurrence values in a grid. Within each element in the grid, the number of failure modes in that category is designated. Using the example risk matrix shown below, there are 8 failures with a severity of 8 and occurrence of 7, and 5 failures with a severity of 2 and an occurrence of 4.

Example FMEA Risk Matrix

The risk matrix color codes risk levels, typically with green, yellow, and red areas. In this case, the failures in the green range are low (acceptable) risk, so no action is required. Failures in the yellow range are medium level risk, and you may want to see if there are actions that could be taken to minimize those. However, failures in the red range are high and represent unacceptable risks that must be addressed through actions plans. In the example above, there are a number of failures that fall into the high risk (red) range. For example, the top box in the upper right shows 7 failures with a Severity of 10 and an Occurrence of 10. Risk matrices such as this provide a clear indication of where your risk reduction efforts need to be focused.

The green/yellow/red levels are subjective based on your particular situation. Additionally, you can customize the risk matrix itself. For example, you may want to graph Severity vs Detection. However you configure the risk matrix, it offers the advantage of concretely highlighting where your recommended action plans should be concentrated.

Using AP for Risk Assessment

Another method of risk assessment is Action Priority, or AP. AP was introduced in the AIAG & VDA FMEA Handbook. AP uses the same Severity, Occurrence, and Detection factors that RPN is based on. However, the AP ranking system gives more emphasis to Severity first, then Occurrence, and then Detection.

AP is not a value, but instead is a level ranking: High, Medium, or Low. In the AIAG & VDA standard, AP levels are defined as:

- H (Priority High): These items are the highest priority for review and action. You *must* either recommend an appropriate action to improve Prevention and/or Detection Controls for this item, or document why your current Controls are acceptable.

- M (Priority Medium): These items are medium priority for review and action. You *should* recommend an appropriate action to improve Prevention and/or Detection Controls for this item, or, optionally, document why your current Controls are acceptable.

- L (Priority Low): These items are low priority for review and action. You *could* recommend appropriate action to improve Prevention and/or Detection Controls.

The default table for AP as defined in the AIAG & VDA Handbook as:

Severity	Occurrence	Detection	AP
9-10	8-10	7-10	H
		5-6	H
		2-4	H
		1	H
	6-7	7-10	H
		5-6	H
		2-4	H
		1	H
	4-5	7-10	H
		5-6	H
		2-4	H
		1	M
	2-3	7-10	H
		5-6	M
		2-4	L
		1	L
	1	1-10	L
7-8	8-10	7-10	H
		5-6	H
		2-4	H
		1	H
	6-7	7-10	H
		5-6	H
		2-4	H
		1	M
	4-5	7-10	H
		5-6	M
		2-4	M
		1	M

	2-3	7-10	M
		5-6	M
		2-4	L
		1	L
	1	1-10	L
4-6	8-10	7-10	H
		5-6	H
		2-4	M
		1	M
	6-7	7-10	M
		5-6	M
		2-4	M
		1	L
	4-5	7-10	M
		5-6	L
		2-4	L
		1	L
	2-3	7-10	L
		5-6	L
		2-4	L
		1	L
	1	1-10	L
2-3	8-10	7-10	M
		5-6	M
		2-4	L
		1	L
	6-7	7-10	L
		5-6	L
		2-4	L
		1	L
	4-5	7-10	L

		5-6	L
		2-4	L
		1	L
	2-3	7-10	L
		5-6	L
		2-4	L
		1	L
	1	1-10	L
1	1-10	1-10	L

	Function	Failure Mode	Effect	Severity	Cause	Occurrence	Detection	AP
1	Provides convenient flying, aerial surveillance and video recording functionality and experience	Low battery life	Possible collision	7	Degraded battery	5	3	M
2					Cathode wear out	7	4	H
3		Battery leaking	Legal and safety issue	10	Manufacturing and packaging defects	2	2	L
4		Structural imbalance	Collision	10	Structural failure	4	8	H
5			Unable to fly straight	5	High winds and gusts	3	6	M
6					Motor malfunction	2	6	M
7	Provides the thrust and motion to the flight	Motor malfunction	Possible collision	7	Motor mechanical failure	2	6	M
8					Wear	5	4	M
9		Error in motor controller	Possible collision	7	High voltage	3	3	L

Example FMEA Worksheet using AP

Example Using AP

To demonstrate AP analysis, we'll use the same example we considered for RPN above: a manufacturer of car batteries.

The failure mode under analysis is that the battery goes dead. The effect is that the car does not start, and one of the causes is that the driver failed to turn the headlights off.

We determine the AP by analyzing the component factors. We use the same Severity, Occurrence, and Detection scales employed in our previous RPN analysis example. So, the Severity is a 5, the Occurrence is a 7, and the Detection is a 10.

According to the AP Table, our resulting AP in this example is Medium priority. In accordance with the AP definition, we should recommend action to

improve the Prevention and/or Detection Controls, or document why the current Controls are acceptable.

As with RPN, AP factors and results can be customized to better suit your needs. For example, you may want to modify the Severity, Occurrence, and/or Detection rating scales. Or, you may want to change the AP level settings.

Using Criticality for Risk Assessment

Criticality is a numerical approach to risk assessment typically used in FMECAs (Failure Mode, Effects, and Criticality Analysis) based on MIL-STD-1629. Mode Criticality values are computed based on failure rate, failure mode percentage, operating time and failure effect probability. Item Criticality values are based on Mode Criticality values per Severity level.

Criticality values are more detailed than RPN and AP and offer a uniquely metrics-based analysis of risk. The higher the criticality value, the higher the risk.

In FMECA, there are two criticality values: mode criticality and item criticality. Both are useful when analyzing risk levels.

Mode criticality is a numerical value determined for each failure mode. The equation for mode criticality is:

*Mode Criticality = Mode Failure Rate * Operating Time * Failure Effect Probability*

Where mode failure rate is computed by:

*Mode Failure Rate = Item Failure Rate * Failure Mode Percentage*

Essentially, mode failure rate is the percentage of the failure rate attributable to a given failure mode. Consider an example of an item with a failure rate of 50 FPMH (Failures per Million Hours) with two failure modes: one failure mode has a failure mode percentage of 80%, and the other is 20%. In this case, the mode failure rate of the first failure mode is 40 FPMH, and of the second is 10 FPMH.

The operating time is the time the item is operational. In some situations, such as phased systems, not all components are operating at all times.

The failure effect probability is a value between 0 and 1 that indicates the probability that the effect of the given failure mode will occur. If there is only a

single effect, then the failure effect probability is 1. Our car battery example is such an example: if the car battery goes dead the effect is that the car does not start. The failure effect probability of "car does not start" is 1. However, if a failure mode has more than one possible effect, then the failure effect probabilities should sum up to 1. For example, if I crash my drone when landing it, there are three possible effects: it is damaged beyond repair, in need of minor repair, or survives unscathed. The likelihood of each of these scenarios is not equal. Though I'd hope for the totally unscathed result, that's the least likely. In this example, I may assign the failure effect probabilities as 0.2 (damaged beyond repair), 0.7 (need of minor repair), and 0.1 (unscathed).

Item criticality is computed based on mode criticality values:

Item Criticality = Sum of the Failure Mode Criticalities with the same Severity Classification

Essentially, for each item, there is a set of criticality values. The number of criticality values is based on the number of levels used when determining the Severity rating. For example, the most commonly used Severity Classification is a 4-level scale defined in MIL-STD-1629:

I. Catastrophic (Category I): A failure which may cause death or weapon system loss (i.e. aircraft, tank, missile, ship, etc.).

II. Critical (Category II): A failure which may cause severe injury, major property damage, or major system damage which will result in mission loss.

III. Marginal (Category III): A failure which may cause minor injury, minor property damage, or minor system damage which will result in delay or loss of availability or mission degradation.

IV. Negligible (Category IV): A failure not serious enough to cause injury, property damage or system damage, but which will result in unscheduled maintenance or repair.

In this case, for each item in the FMECA, there will be 4 criticality values. For example, to determine the item criticality for the Catastrophic classification, mode criticality values of all the failure modes for this item that are designated as Catastrophic are added together.

	Function	Part Failure Rate	Failure Mode	Failure Mode Percentage	Failure Mode Failure Rate	Failure Effect Probability	Severity Class	Failure Mode Criticality	Item Criticality
1	Power Store	6.800091	Open	40.00	2.720036	0.200000	II. Critical	0.136002	0.476006
2		6.800091	Short	20.00	1.360018	0.100000	I. Catastrophic	0.034000	0.034000
3		6.800091	Mechanical Failure	40.00	2.720036	0.500000	II. Critical	0.340005	0.476006

Example FMECA Worksheet with Criticality Values

Using the Criticality Matrix

Similar to the way a risk matrix is used for analyses employing RPN values, a FMECA criticality matrix can be used for analysis purposes.

The FMECA criticality matrix is created based on the Severity Classification and Probability of Occurrence. In FMECAs, the Probability of Occurrence is determined based on failure mode probabilities. Failure mode probability is computed by:

Failure mode probability = $1 - e^{(-\lambda t)}$

where

λ = mode failure rate

t = time: the amount of the mission phase time of the failure mode

Using these values, the Probability of Occurrence is designated as one of these five levels per MIL-STD-1629A:

- Frequent (Level A): A high probability of occurrence, defined as a single failure mode probability greater than 0.20 of the overall probability of failure during the item operating time.
- Reasonably probable (Level B): A moderate probability of occurrence, defined as a single failure mode probability which is more than 0.10 but less than 0.20 of the overall probability of failure during the item operating time.

- Occasional (Level C): An occasional probability of occurrence, defined as a single failure mode probability which is more than 0.01 but less than 0.10 of the overall probability of failure during the item operating time.

- Remote (Level D): An unlikely probability of occurrence, defined as a single failure mode probability which is more than 0.001 but less than 0.01 of the overall probability of failure during the item operating time.

- Extremely unlikely (Level E): A failure whose probability of occurrence is essentially zero during the operating time interval, defined as a single failure mode probability less than 0.001 of the overall probability of failure during the item operating time.

The FMECA criticality matrix graphs Severity Classification vs. Probability of Occurrence. Again, the number of failure modes in each category is designated in the boxes on the graph. The green/yellow/red color coding is utilized to designate failures of low, medium, and high risk. Those in the red range are the most critical items to address.

Example Criticality Risk Matrix

While the criticality analysis using FMECAs is much more complex, it offers the unique advantage of being comprehensive, quantifiable, and robust. It is a much more precise risk assessment technique in contrast to the more qualitative approaches of RPN and AP.

Example Using Criticality

Returning to our car battery manufacturer used in our previous examples, let's determine criticality values.

Again, the failure mode under analysis is that the battery goes dead. The effect is that the car does not start, and one of the causes is that the driver failed to turn the headlights off.

For criticality analysis, we need additional information: the failure rate of the item and the operating time. We'll say we've determined the failure rate of the item using a Reliability Prediction analysis as 57.5 FPMH. We determined that this failure mode percentage is 75%.

For the time, we need to determine the operating time for this particular failure mode. For this example, we are going to look at the probability of failure over a year. We'll make the assumption that the car is driven about 2 hours/day and the lights are on for nighttime driving about 1/3 of the time. Therefore:

Operating Time = 2 hours/day * 365 days/year * 1/3 = 243.33 hours

We also need to identify the failure effect probability. In this case, the probability of the car not starting is high due to the lights being left on, so we'll say it is 0.8.

Our Mode Failure Rate = Item Failure Rate * Failure Mode Percentage =

57.5 * 75% = 43.125 FPMH

Our Mode Criticality = Mode Failure Rate * Operating Time * Failure Effect Probability =

43.125 * 243.33 * 0.8 = 8394.885

In FMECAs Mode Criticality values can widely vary. They all depend on the factors and failure rates of the system being analyzed. To use it effectively, you must review

your entire system, looking at the range of values, ranking them in value, and then determining how those values represent the risk levels of your particular situation.

In this example, using the Severity Classification list from MIL-STD-1629, this failure would be Marginal. In the computation of Item Criticality, this failure mode's Mode Criticality would be included in the Marginal level value.

To compute the Failure Mode Probability in order to assess Probability of Occurrence:

Failure mode probability = $1 - e^{(-\lambda t)} = 1 - e^{(-43.125 \text{ failures}/1000000 \text{ hours} * 243.33 \text{ hours})} = 0.0104$

So, for Probability of Occurrence, this example would fall into the Occasional level. Therefore, with the Severity as Marginal and the Probability of Occurrence as Occasional, finding the point of intersection on the Criticality Matrix, this mode would fall into the Medium (yellow) range using our example risk matrix color coded levels.

You can see the FMECA Criticality analysis is more complex than RPN or AP strategies for risk assessment. However, one of the benefits of FMECA Criticality analysis is that it is highly detailed and precise. FMECAs are often employed due to their comprehensive approach, which provides a thorough and highly effective failure analysis methodology.

Using a Custom Risk Assessment Strategy

Because the level of acceptable risk varies based on many factors, such as industry, product, complexity, compliance requirements, and more, companies frequently develop their own techniques to assess risk. These custom techniques may involve modifying the known methods, while others may entail developing a completely new methodology.

Some example ways risk methodologies could be customized:

- Change the Severity, Occurrence, and Detection scales from 1 – 10 to 1 – 5 for simpler list selection. The RPN values would then range from 1 – 125.

- Change RPN to exclude Detection. Perhaps detection is not an important element, and you prefer to concentrate on mitigation and elimination. In this case, RPN could be Severity * Occurrence, resulting in values from 1 – 100.

- Use only Severity. You decide this is the most important factor, and want to eliminate any highly severe failures, regardless of how often they occur or how easy they are to detect.

- Change the way RPN is calculated. You may want all items with a Severity over 8 to be addressed, so you set any items with Severity over 8 to have an RPN of 1000 knowing that this value will always fall into the "action required" category. You allow all other RPNs to be calculated normally.

- Change the AP table. You prefer a more equal balance to Severity and Occurrence, so you weight those items equally.

- Change the AP table to have more than 3 levels for a more refined breakdown.

- Develop your own "Risk Category" definition. Create a list of risk levels, describe what they are in reference to your organization, and add that column to your FMEA Worksheets.

These are just a few examples. You can see how risk assessment can be adapted to suit what is best for your specific needs. Whatever method you choose, the main objective is to rank the failure modes in your FMEA in order to prioritize the work necessary to lower risk to an acceptable level.

Reassessing Risk after Recommended Actions are Implemented

Lastly, this overview of assessing risk using FMEA would not be complete without a discussion about risk reassessment after recommended action plans have been completed.

As explained, the purpose of risk assessment is to identify those areas which are critical to address. Once the risk profile is evaluated, you investigate possible solutions for eliminating, mitigating, or detecting the high-risk items. Then, you select the preferred approach and develop an action plan. An action plan is a list of

the tasks required to implement the selected solution. Those tasks are then added to the FMEA Worksheet and task assignments are made. Often, due dates are assigned as well.

Once the action plan has been completed, it is vital to revisit the FMEA and perform a secondary risk assessment. On the FMEA Worksheet, you keep the original risk levels and add additional columns for the revised assessments. The revised values are a reassessment of Severity, Occurrence, and Detection levels considering the newly implemented recommended actions. The Revised RPN, Revised AP, Revised Criticality, or Revised Customized Risk Value is a new resulting value based on the revised factors.

For example, if you are using RPN, you end up with 2 sets of 4 columns for RPN analysis: the first set of 4 with Severity, Occurrence, Detection, RPN, and the second set of 4 with Revised Severity, Revised Occurrence, Revised Detection, and Revised RPN. If you have done your work properly, your system should be in compliance with your acceptable risk level based on the Revised RPN values.

Example Revised Risk Analysis

Using our example car battery, there are a couple of options we have in order to reduce the risk of the battery failing. We could add an alarm that would sound when the car was turned off and the headlights are left on. Or, we could automatically turn the headlights off some time after the car is turned off.

We decide the second option is less costly and more robust, so we assign a task to our software team to implement this as a software update.

Once our engineer completes the work, we can go back and determine our Revised RPN value.

Revised Severity = 5 (no change)

Revised Occurrence = 1 (because there is no way for the driver to leave headlights on)

Revised Detection = 10 (no change)

Therefore,

Revised RPN = 5 * 1 * 10 = 50

We've lowered the risk level for this failure from 350 to 50! Therefore, we determine that we've successfully addressed this failure and have lowered the RPN into an acceptable range.

Conclusion

The objective of FMEA is to help you achieve your reliability, quality, and safety goals. One of the most important ways FMEA aids in this effort is by offering a well-organized and useful approach for failure analysis. It is why FMEA remains one of the most commonly used tools in reliability engineering.

In order to quantify your product's or process' exposure to harmful risks using FMEA, your risk assessment strategy is key. How that risk assessment is done is variable, and various methodologies exist today that provide useful measures. Whether you choose to employ one of the standards-based techniques, modify one, or develop your own, the ability to quantify risk during your FMEA process is of utmost importance. Developing a well-grounded strategy for your organization enables you to maximize the effectiveness of your failure analyses.

Relyence FMEA offers support for the methods of risk assessment described here. Additionally, Relyence FMEA allows you to customize all aspects of the risk analysis, including modifying the Severity, Occurrence, and Detection lists, changing the RPN and AP calculations, and altering the color-coded range settings. Or you can also create a completely custom strategy if you prefer. If you would like more information, please feel free to sign up for a free trial, schedule a personal demo, or contact us for advice and guidance.