Job Support Tool: Failure Mode Effect Analysis (FMEA)

Hello All and welcome to the FMEA Job Support Tools Learning Assets. We at the College of Contract Management put together a set of Job Support Tools from our CMQ 260 – FMEA course to help you when you are working with your contractors in trying to understand how they developed FMEA and how to better read and understand what you are looking at. The following is a list of what this file contains. For more information please go to the CMQ 260 course material posted at the DAU.mil website. This material can be viewed in "browse" mode whether you have graduated the class or not and is available any time you wish to access it. Please feel free to ask any questions you may have to Roger Woods; roger.woods@dau.mil, 256-822- 9038.

You may click on any of the titles below to go directly to that particular job aid.

Job Support Tool 1 FMECA Probability of Occurrence

Job Support Tool 1 was developed to help you better understand what the Probably of Occurrence codes mean. Failure Mode Effects and Criticality Analysis (FMECA) probability of occurrence is determined using analysis, calculations, comparison to similar products/processes, and past documented failure modes. When part failure rate data is not available, the probability of occurrence of each failure is grouped into discrete levels that establish the ***qualitative*** failure probability level for each entry.

Job Support Tool 2: Severity Rating Criteria

This Job Support Tool is designed to help you understand what each severity level means.

Severity Rating Criteria are not defined in MIL-STD-1629A. However, criteria are defined in IEC 60812, automotive industry specifications and by NASA. This criteria uses a scale of 1-10 to rate how severe a failure is. If questions arise regarding the severity of a given failure effect, it may be helpful to refer to the product FMEA/CIL (Critical items list) for further insight or an estimate of the severity rating. These tables can be used as a reference to the severity rating criteria.

Job Support Tool 3: Risk Mitigation Techniques Advantages and Disadvantages

This Job Support Tool lists the risk mitigation techniques that can be used when trying to decide what to do with a certain risk. Of course, there are advantages and disadvantages to each technique's use. It is important that suppliers take into consideration what is the best way to address each risk. This chart provides a side by side view of the risk mitigation technique advantages and disadvantages.

Job Support Tool 4: Risk Mitigation Planning Checklist

If contractors have determine a risk they need to develop a risk mitigation plan. This checklist is designed to help you when reviewing that plan to ensure it is complete. There is also a wealth of information you can glean from this checklist that will help you in your surveillance planning. For instance, once a contractor had developed their risk mitigation plan you can use the plan to perform your surveillance to ensure the risk is being addressed properly thus, giving you the confidence you need when it comes time to accept product.

Job Support Tool 5: Risk Mitigation Strategy

During the course of developing the Risk Mitigation plan the contractor can determine what strategy they intend to use when addressing the risk. There are basically five strategic approaches they can use. They are: Risk Control, Risk Avoidance, Risk Assumption/Acceptance, Risk Transfer, and Risk Elimination. This Job Support Tool gives the definition of each of these strategies along with a couple examples of FMECA's where they have been used.

Job Support Tool 6: Four Step Approach

When developing a Process FMEA (PFMEA) there is a four step approach that should be used. The steps are: Plan, Perform, Implement, and Document. This Job Support Tool defines each of these steps in order for you to be prepared when performing PFMEA.

Job Support Tool 7: Map the Process

This Job Support Tool is designed as a visual reminder of the steps taken in the Process FMEA process.

Job Support Tool 8: Criticality Quantitative Example

The example provided in this Job Support Tool is to help you be able to calculate criticality based on knowing certain information. This will assist you in better understanding where the numbers come from when reviewing a contactors FMEA report.

Job Support Tool 1: FMECA Probability of Occurrence

Failure Mode Effects and Criticality Analysis (FMECA) probability of occurrence is determined using analysis, calculations, comparison to similar products/processes, and past documented failure modes. When part failure rate data is not available, the probability of occurrence of each failure is grouped into discrete levels that establish the ***qualitative*** failure probability level for each entry.

The four approaches that the analysis uses to determine the probability of occurrence of a failure (in order of preference) are:

- Past test or field data for similar equipment;
- Engineering analysis, failure mechanism modeling, and/or accelerated life testing
- Subject matter expertise based on known reliability levels for comparable equipment and technologies
- Reliability / failure data provided in federal, national and international handbooks/parts specifications

The failure mode probabilities of occurrence levels are:

Level	Probability of Occurrence	Description
A	Frequent	A high probability of occurrence during the item operating time interval. High probability may be defined as a single failure mode probability greater than 0.20 of the overall probability of failure during the item operating time interval.
B	Reasonably Probable	A moderate probability of occurrence during the item operating time interval. Probability may be defined as a single failure mode probability, which is more than 0.1 but less than 0.20 of the overall probability of failure during the item operating time interval.
C	Occasional	An occasional probability of occurrence during the item operating time interval. Occasional probability may be 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 interval.
D	Remote	An unlikely probability of occurrence during the item operating time interval. Remote probability may be 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 interval.

Level	Probability of Occurrence	Description
E	Extremely Unlikely	A failure whose probability of occurrence is essentially zero during the item operating time interval. Extremely unlikely may be defined as a single failure mode probability, which is less than 0.001 of the overall probability of failure during the item operating time interval.

[1]The overall probability of failure during the item/system operating time is generally found in the contract / Statement of Work (SOW).

Source: US Department of Defense, *MIL-STD-1629A: Procedures for Performing a Failure Mode Effects and Criticality Analysis.* November 1974, June 1977, November 1980. (Cancelled in August 4,

Job Support Tool 2: Severity Rating Criteria

Severity Rating Criteria are not defined in MIL-STD-1629A. However, criteria are defined in IEC 60812, automotive industry specifications and by NASA. This criteria uses a scale of 1-10 to rate how severe a failure is. If questions arise regarding the severity of a given failure effect, it may be helpful to refer to the product FMEA/CIL (Critical items list) for further insight or an estimate of the severity rating. This table can be used as a reference to the severity rating criteria.

Severity Rating Criteria	
Criteria	**Rating**
Very low severity rating Failure would have very little effect on further processing or product performance.	1
Low severity rating Failures have minor effect on further processing or product performance.	2 - 3
Moderate severity rating A failure, which causes customer concern or program impact, but will not cause a Criticality 1 failure of the end item or an equivalent process failure.	4 - 5 - 6
High severity rating Failure causes severity impact to component or process and may contribute to a Criticality 1 failure of the end item or an equivalent process failure.	7 - 8 - 9
Very high severity rating Failure contributes to a known or highly probable Criticality 1 failure of the end item of an equivalent process failure involving loss of life or a major loss of manufacturing facilities.	10

Source: *Analysis techniques for system reliability - Procedure for failure mode and effects analysis (FMEA),* IEC 60812 Ed. 2.0 (2006)

Process FMEA Severity Rating

Note: There are different variations of this rankings and ratings used in the industry. The tables presented are for illustrative for training purposes only.

Level	Severity of Effect	Rating
Extreme	May endanger machine or operator. Hazardous **without** warning	10
Extreme	May endanger machine or operator. Hazardous **with** warning	9
High	Major disruption to production line. Loss of primary function, 100% scrap. Possible jig lock and major loss of Takt* Time	8
High	Reduced primary function performance. Product requires repair or Major Variance. Noticeable loss of Takt Time	7
Moderate	Medium disruption of production. Possible scrap. Noticeable loss of Takt time. Loss of secondary function performance. Requires repair or Minor Variance	6
Moderate	Minor disruption to production. Product must be repaired. Reduced secondary function performance.	5
Moderate	Minor defect, product repaired or "Use-As-Is" disposition.	4
Low	Fit & Finish item. Minor defect, may be reprocessed on-line.	3
Low	Minor, Nonconformance, may be reprocessed on-line.	2
None	No effect.	1

*Takt time is the rate at which a finished product needs to be completed in order to meet customer demand

Return to Severity Number

Process FMEA Occurrence Ratings

Note: There are different variations of this rankings and ratings used in the industry. The tables presented are for illustrative for training purposes only.

Level	Likelihood of Occurrence	Failure Rate	Capability (Cpk)*	Rating
Very High	Failure is almost inevitable	1 in 2	<0.33	10
Very High	Failure is almost inevitable	1 in 3	>0.33	9
High	Process is not in statistical control. Similar processes have experienced problems.	1 in 8	>0.51	8
High	Process is not in statistical control. Similar processes have experienced problems.	1 in 20	>0.68	7
Moderate	Process is in statistical control but with isolated failures.	1 in 80	>0.83	6
Moderate	Previous processes have experienced occasional failures or out-of-control conditions.	1 in 400	>1.00	5
Moderate	Previous processes have experienced occasional failures or out-of-control conditions.	1 in 2000	>1.17	4
Low	Process is in statistical control.	1 in 15k	>1.33	3
Low	Process is in statistical control. Only isolated failures associated with almost identical processes.	1 in 150k	>1.50	2
Remote	Failure is unlikely. No known failures associated with almost identical processes.	1 in 1.5M	>1.67	1

*Process capability index is a statistical measure of process capability.

Return to Occurrence Number

Process FMEA Detection Ratings

Note: There are different variations of this rankings and ratings used in the industry. The tables presented are for illustrative for training purposes only.

Level	Likelihood that control will detect failure	Rating
Very Low	No known control(s) available to detect failure mode	10
Low	Controls have a remote chance of detecting the failure	9
Low	Controls have a remote chance of detecting the failure	8
Moderate	Controls may detect the existence of a failure	7
Moderate	Controls may detect the existence of a failure	6
Moderate	Controls may detect the existence of a failure	5
High	Controls have a good chance of detecting the existence of a failure	4
High	Controls have a good chance of detecting the existence of a failure	3
Very High	The process automatically detects failure	2
Very High	Controls will almost certainly detect the existence of a failure.	1

Job Support Tool 3: Risk Mitigation Technique Advantages and Disadvantages

Of course, there are advantages and disadvantages to each technique's use. It is important that suppliers take into consideration what is the best way to address each risk. This chart provides a side by side view of the risk mitigation technique advantages and disadvangates.

Risk Mitigation Technique	Advantages	Disadvantages
Risk Avoidance	Risk avoidance can be used in a cost-as-an-independent-variable (CAIV) tradeoff.	In order to discourage life cycle risk management versus risk avoidance, reducing requirements as a risk avoidance technique will be used only as a last resort. This should only be done with the participation and approval of the user's representative
Risk Transfer	For the risk transfer approach to be effective in government/contractor relationships, the risks transferred to the contractor must be those that the contractor has the capacity to control and manage. These are generally risks associated with technologies and processes used in the program - those for which the contractor can implement proactive solutions. The types of risks that are best managed by the Government include those related to the stability of and external influences on program requirements, funding, and schedule, for example.	Transfer of risk to another risk owner should only be performed if the other risk owner has the ability to handle the risk and the overall risk exposure is reduced.

Risk Mitigation Technique	Advantages	Disadvantages
Risk Control	Risk controls may reduce the impact or probability of identified risks. Risk controls monitor and manage risk in a manner that reduces the probability and/or impact of its occurrence or minimize the risk's effect on the program or weapon system.	Most Risk Control steps share two features: they require a commitment of program resources, and they may require additional time to accomplish them. Thus, the selection of risk-control actions will undoubtedly require some tradeoff between resources and the expected benefit of the actions. This option may add to the cost of a program; however, the selected approach should provide an optional risk among the candidate approaches of risk reduction, cost effectiveness, and schedule impact.
Risk Acceptance/ Assumption	Risk acceptance (also known as assumption) is acknowledging the existence of a particular risk situation and making a conscious decision to accept the associated level of risk without engaging in any special efforts to control it. However, a general cost and schedule reserve may be set aside to deal with any problems that may occur as a result of various risk acceptance decisions. This method recognizes that not all identified program risks warrant special handling. Risk acceptance is most suited for those situations that have been classified as low risk.	The fact that risks are assumed does not mean that they are ignored. In fact, every effort should be made to identify and understand them so that appropriate management action can be planned. Also, risks that are assumed should be monitored during development; this monitoring should be well planned from the beginning.

Job Support Tool 4: Risk Mitigation Planning Checklist

The type of mitigation should be determined and the details of the mitigation described for each root cause or risk.

This checklist may be helpful to determine if the suppliers risk mitigation plan addressed all of the necessary topics.

Are the following topics included in the Risk Mitigation Plan?	**Yes**	**No**	**Comments**
Descriptive title for the identified risk	☐	☐	
Date of the plan	☐	☐	
Point of contact responsible for controlling the identified root cause	☐	☐	
Brief description of the risk, that includes: • Summary of the performance • Schedule and resource impacts • Likelihood of occurrence • Consequence • Whether risk is in control of the program	☐	☐	
Reason the risk exists/root cause leading to the risk	☐	☐	
Mitigation options/possible alternatives to alleviate the risk	☐	☐	
Definition of events and activities intended to reduce the risk, success criteria for each plan event, and subsequent “risk level if successful” values	☐	☐	

Job Support Tool 4: Risk Mitigation Planning Checklist, Cont.

Are the following topics included in the Risk Mitigation Plan?	Yes	No	Comments
Brief risk status discussion	☐	☐	
Description of the fallback approach and expected decision date for considering implementation	☐	☐	
Management recommendation, that: • Allocates budget and/or time • Incorporates risk mitigation into estimate at completion or in other program plans	☐	☐	
Appropriate approval (IPT leader, higher-level Product Manager, Systems Engineer, Project Manager)	☐	☐	
Identified resource needs	☐	☐	

Job Support Tool 5: Risk Mitigation Strategy

NOTE: In accordance with the contract, a Risk Mitigation Plan is required for failure modes that can cause a Category I – Catastrophic Failure and Category II – Critical Failure which have a Probability of Occurrence of Frequent, Reasonable Probable or Occasional

Report Number: RMP 01

Date of this Plan: 12/10/2006

Risk Mitigation Point of Contact: Tom Roberts, 657-524-8799

Options for Mitigation

Risk Control – are controls used to manage the risk in a manner that reduces the likelihood of its occurrence and/or minimizes the risk's effects (impact) on the end item. ***Requires Risk Retention Rationale***.
Risk Avoid – include changes in the concept, requirements, specifications, and/or practices that reduce risk to an acceptable level.
Risk Accept – is an acknowledgement of the existence of a particular risk situation and a decision to accept the level of risk without trying to control it by any special measures. ***Requires Risk Retention Rationale***.
Risk Transfer – is a reallocation or transfer of the risk to some other entity.
Risk Elimination – completely eliminates the risk through redesign.

Job Support Tool 5: Risk Mitigation Plan, Example #1

Report Number: RMP 0225-01 **Date of this Plan:** 12/10/2006

Risk Mitigation Point of Contact: Tom Roberts, 657-524-8799

FMECA Failure Mode	FMECA Severity Class	FMECA Failure Effects	FMECA Failure Cause	FMECA Probability of Occurrence	WHY RISK EXISTS	POSSIBLE OPTIONS FOR MITIGATION	DECISION	EVENTS / ACTIVITIES TO REDUCE RISK
FL112 – No CID output	I - Catastrophic	CID does not illuminate/ inoperative	FL1121 - On/Off Switch internal contact stuck open	Frequent Probability of Occurrence	Technology prohibitive	Risk Control Risk Accept	Risk Control	Install a Failure Detection Circuit
			FL1122 - Bulb filament separated	Frequent Probability of Occurrence	Use of an incandescent lamp instead of a LED	Risk Control Risk Accept	Risk Control	Replace Filament Bulb with a more reliable Illumination LED Light. Install a Failure Detection Circuit
			FL1123 - Battery power below required operating voltage	Frequent Probability of Occurrence	Selection of a low reliability battery in the initial design to save cost	Risk Control Risk Accept	Risk Control	Replace current Lithium-ion Battery with a higher reliable Battery. Install a Failure Detection Circuit

Approvals			
Design Engineering	Tom Roberts	–signed--	12/10/06
Materials Engineering	Steve Conjob	–signed--	12/10/06
Program Manager	Fiona Gaubhaul	–signed--	12/10/06
	Print Name / Electronic Signature		**Date**

Job Support Tool 5: Risk Mitigation Plan, Example #2

Report Number: RMP 0225-02 **Date:** 12/10/2006

Descriptive Tile for Risk: FMECA FL111 – Failure Mode Constant CID Output **Severity Class:** Category I – Catastrophic

Risk Mitigation / Root Cause Point of Contact: Tom Roberts, 657-524-8799 **Is Risk in Control of the Program:** YES.

FMECA Failure Cause	FMECA Probability of Occurrence	Possible Options for Mitigation	Decision	Status	Target Date of Implementation	Events / Activities To Reduce Risk
FL1111 – On/Off Switch internal contact stuck closed	Probability of Occurrence	Risk Control Risk Accept	Risk Control	Design started 12/10/06	No fallback required. Design enhancement	A fault detection circuit will be included in the CID to warn user of this undesirable fault. The circuit will default to Red when the switch and/or associated circuitry are not properly functioning.
FL1112 – A1 CCA faulty output through the switch to the bulb	Occasional Probability of Occurrence	Risk Control Risk Accept	Risk Control	Design started 12/10/06	No fallback required. Design enhancement	The CCA provides a recharging circuit for the Lithium Ion Battery. A fault detection circuit will be included in the CID to warn the user of this undesirable fault. The circuit will default to Red when the CCA is not properly functioning.

Management Recommendation for Allocated Budget/Time: Budget impact for design of fault detection circuit is $1,050 for 1 design engineer. Cost of added components and wiring, per unit, is $25.50. Time to design is 10.0 hours. This design changes was anticipated and already included in the budget baseline.

Schedule / Resource Impact: None.

Changes in Risk Level if Successful (Values):

	ORIGINAL	REVISION
Severity (NO CHANGE)	Category 1 Catastrophic	Category 1 Catastrophic
Probability of Occurrence (NO CHANGE)	Part Failure Rate 11.25/per million hours	Part Failure Rate 11.25/per million hours
User Detection Method (CHANGE)	Human Detection	Fault Detection Circuit with Warning Lights

Approvals			
Design Engineering	Tom Roberts	–signed--	12/10/06
Materials Engineering	Steve Conjob	–signed--	12/10/06
Program Manager	Fiona Gaubhaul	–signed--	12/10/06
	Print Name / Electronic Signature		**Date**

Job Support Tool 6: Four Step Approach

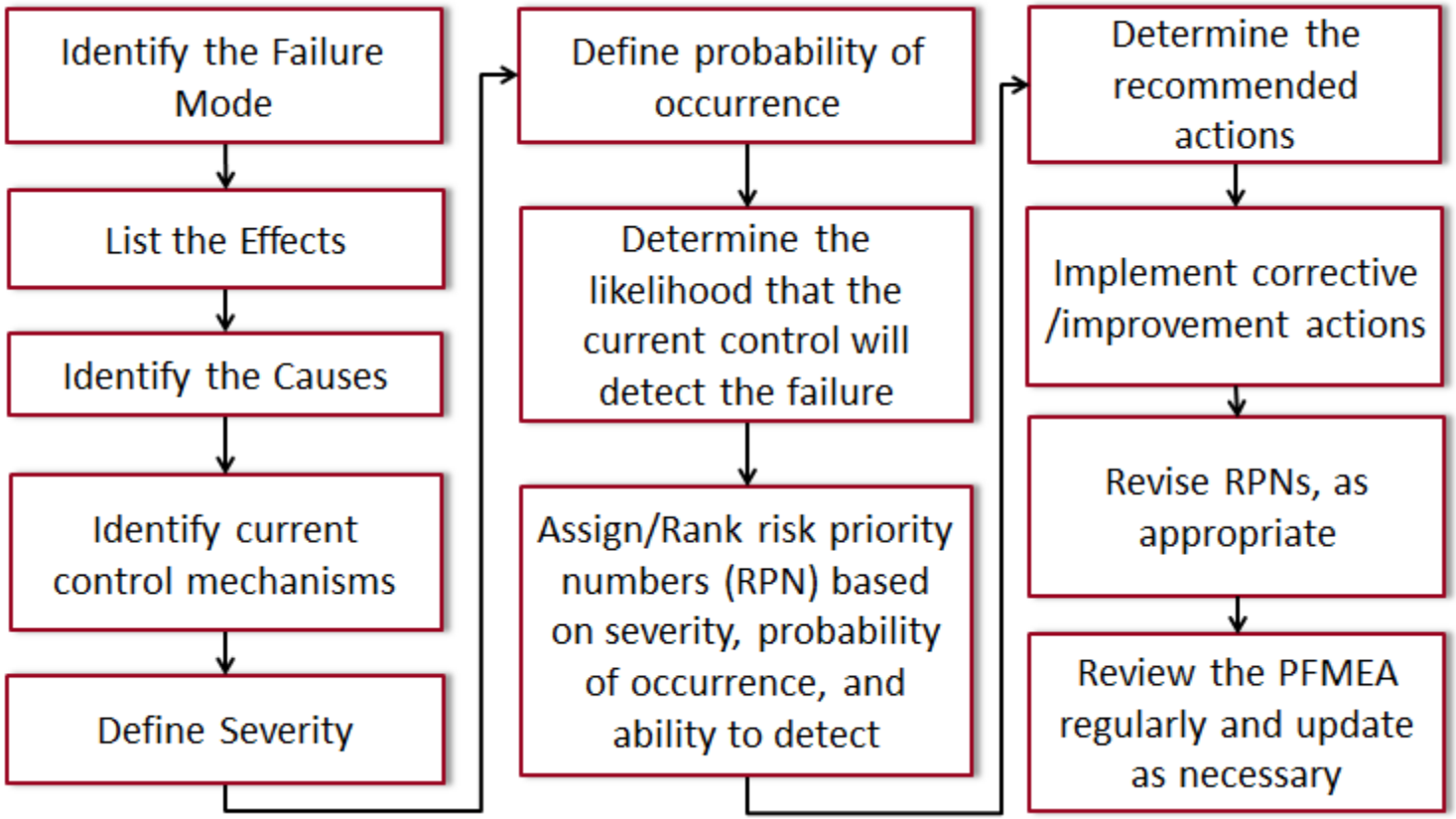
When developing a risk strategy is it recommended that a four step approach be used. The following defines each step

The four steps include: Step	Approach	Description	
1	Plan	The team leader: • Organizes the team • Defines the goals, methods, scope, responsibilities of each team member • Establishes a tentative schedule After reviewing engineering drawings, planning / procedures, work instructions and associated inspection criteria, the team leader develops a flow chart showing the ***major* steps**, functions or operations of the process to help team members understand the process.	

The four steps include: Step	Approach	Description	
2	Perform	For each process function (steps), the team: • Determines all credible failure modes • Discusses and records the failure effects, failure causes, and current controls for each potential failure mode. **Failure causes are viewed in terms of the five process elements / inputs of Manpower, Methods, Machines, Materials and Environment.** • Each potential failure cause must have its own entry so that it can be evaluated independently and have corrective action, if any, tracked. • Rates the severity, occurrence and detection for each failure cause o In the PFMEA, the detection method(s) is the method that would prevent the customer, both internal and external to the process, from receiving a nonconforming product or characteristic. o When rating the "occurrence" of this process step failing, customer feedback, internal audits and yield data should be used in the determination, if it exists. o The Risk Priority Number (RPN) is the product of severity, occurrence and detection ratings.	

The four steps include: Step	Approach	Description	
3	Implement	Corrective action to improve the process is the next step. Those failure causes with the high RPN ratings should be analyzed first. Some additional brain storming to develop effective and innovative ways to reduce failure is appropriate here. A high occurrence number indicates the causes should be eliminated or controlled. High detection numbers indicate a need for better or additional controls and a high severity number indicates product or process redesign may be needed. Proposed changes are then listed on the PFMEA form. At this point, although corrective actions may not be implemented, the team may decide to document the revised RPNs to show the effects of the proposed actions. Once implemented, as "Resulting Action Taken", new severity, occurrence and detection ratings and RPN rating are assigned. Corrective actions implemented should be checked for effectiveness.	
4	Document	Proposed changes for high / significant RPN ratings, which have not been completed, will be clearly identified on the PFMEA form as "Open Work", or similar language, along with the responsible organization and applicable name. In addition, all "Open Work" should be tracked to completion. Typically, if management approval to proceed with corrective actions is required, and an executive summary of the PFMEA results would be provided to management. Presenting the PFMEA results to work center management and releasing the final report	

Job Support Tool 7: Map the Process



Job Support Tool 8: Criticality Quantitative Example

Resistor R9 in the power supply of a launch system has a **failure rate of 0.04** failures per one million hours. Reference MIL-HDBK-217 (Section 9.6)

System power supply testing reveals the R9 resistor fails in an **open state 20%** of the time and the **performance is degraded 100%** of the time. The mission time is **one hour**.

1. Break down the information for the Criticality Analysis from the scenario above.

Criticality Analysis-Quantitative Approach	**FMECA Data**
λ_p = Part failure rate in every case per standard	0.04
α = Failure mode ratio for open state	0.20
β = Probability of occurrence for open and performance degradation	1.00
t = Mission duration in hours	1
C_m (open, performance degradation) Calculation: 0.20 * 1.00 * 0.04 * 1 =	0.008

2. Input the information into the appropriate FMECA Form field.

FMECA
Component Type: Resistor

Item	**Failure Rate (Lambda) per million hrs**	**Failure Mode**	**Failure Mode Ratio (Alpha)**	**Failure Effect**	**Severity**	**Failure Effect Probability (Beta)**	**Time (Hrs)**	**Cm x 10-6** $C_m = \beta\alpha\lambda_p t$
R9-0	0.04	Open	0.20	Performance Degradation	III	1.00	1	0.008