CHAPTER 11

Failure Mode and Effects Analysis

When an analyst begins to perform a risk analysis, he/she first must determine what exactly they are analyzing. For this chapter we must first determine what we consider a failure. Is a failure the total loss of a spacecraft, aircraft, ship, or chemical plant? Or is it the failure to ensure there are enough funds in an account before using a debit card? On 2 November 2006 the NASA Mars Global Surveyor last communicated with Earth. Up to that point the spacecraft that had been launched in 1996 had operated four times as long as the design life and sent back huge amounts of geographical data on the Red Planet. Therefore, the mission was a great success. However, on 2 November 2006 after the spacecraft was directed to perform a routine adjustment of its solar panels, it sent back that it had experienced a series of alarms. The spacecraft then indicated that it had stabilized. However, that was its final transmission. Next, the spacecraft reoriented to an angle that exposed one of two batteries carried on the spacecraft to direct sunlight. This caused the battery to overheat and ultimately led to the loss of both batteries. The communication antenna was not oriented correctly and kept the orbiter from telling controllers its status. The system's programmed safety response did not include making sure the spacecraft orientation was thermally safe, and it failed (1).

However, since it had already outperformed its original mission, had it truly failed? We all would like things we buy to live longer than we expect. The B-52 is an example of an aircraft that has far outlived its design life. In 1952 when the first B-52 flew, no one would have expected it to still be a major player in the second decade of the 2000s. So, as originally stated, we have to have a firm understanding of what is a failure before we begin an analysis.

Risk Assessment: Tools, Techniques, and Their Applications, Second Edition. Lee T. Ostrom and Cheryl A. Wilhelmsen.

Companion website: www.wiley.com/go/Ostrom/RiskAssessment_2e

11.1 INTRODUCTION

This section provides the basic instructions for performing a failure mode and effects analysis (FMEA) and a failure mode, effects, and criticality analysis (FMECA) for the purpose of analyzing procedures for risk. Also provided are examples of symbols and tables commonly used in the analysis process. An example of how these techniques are used for analyzing procedures is also provided.

11.1.1 Description

An FMEA is a detailed document that identifies ways in which a process or product can fail to meet critical requirements. It is a living document that lists all the possible causes of failure from which a list of items can be generated to determine types of controls or where changes in the procedures should be made to reduce or mitigate risk. The FMEA also allows procedure developers to prioritize and track procedure changes (2).

11.1.2 Why Is a Failure Mode and Effects Analysis Effective?

The process is effective because it provides a very systematic process for evaluating a system or a procedure, in this instance. It provides a means for identifying and documenting:

1. Potential areas of failure in process, system, component, or procedure.
2. Potential effects of the process, system, component, or procedure failing.
3. Potential failure causes.
4. Methods of reducing the probability of failure.
5. Methods of improving the means of detecting the causes of failure.
6. Risk ranking of failures, allowing risk informed decisions by those responsible.
7. A starting point from which the control plan can be created.

11.1.3 Types of Failure Mode and Effects Analyses

1. Procedure: Documents and addresses failure points and modes in procedures.
2. Process: Documents and addresses failure modes associated with the manufacturing and assembly process.
3. Software: Documents and addresses failure modes associated with software functions.
4. Design: Documents and addresses failure modes of products and components long before they are manufactured and should always be completed well in advance of prototype build.

5. System: Documents and addresses failure modes for system and subsystem level functions early in the product concept stage.
6. Project: Documents and addresses failures that could happen during a major program.
7. This document focuses on using the FMEA process for analyzing procedures.

11.1.4 Failure Mode and Effects Analysis Process

An FMEA is somewhat more detailed than a PHA and is conducted more on a step-by-step basis. Table 11.1 shows an example of an FMEA table. Note that a great deal of what is contained in a PHA is also contained in an FMEA. Therefore, this section will focus on the process of performing an FMEA.

The following constitutes the steps of an FMEA. These steps will be illustrated by the use of an example.

The first step is to create a flow diagram of the procedure. This is a relatively simple process in which a table or block diagram is constructed that shows the steps in the procedure. Table 11.2 shows the simple steps of starting a manual lawn mower. Note that this is a reasonable analysis and not an exhaustive analysis.

Table 11.3 shows the potential failure modes for each of the steps.

Table 11.4 shows the effect of the potential failures.

Table 11.5 lists the potential causes of the failures.

The basic process is complete once these four steps are completed. However, the next step in the FMEA process is very important for the procedure development process. This is providing a column listing the control measures for each of the potential failure causes. This step ensures that control measures are present and/or are adequate for each cause. It is very important to ensure that causes are not dismissed until there is an adequate control measure in place. Table 11.6 shows a listing of the control measures for each cause.

An additional technique used in FMEAs is to add the dimension of probability and criticality. This is known as an FMECA. An FMECA is an especially important technique for the assessment of risks in procedures because it can aid in:

1. The prioritization of steps/sections of procedures that need to be changed or the process changed to reduce risk.
2. Pointing out where warnings, cautions, or notes need to be added in procedures.
3. Pointing out where special precautions need to be taken or specialized teams/individuals need to perform tasks.

The criticality is mainly a qualitative measure of how critical the failure to the process really is. It is usually based on subject matter experts' opinion but can also be based on probability of occurrence and/or on the consequence or effect.

TABLE 11.1
Example FMEA Table

Item	Potential failure mode	Cause of failure	Possible effects	Probability	Criticality	Prevention
Step in procedure, part, or component	How it can fail: • Failures can be: ∘ Pump not working ∘ Stuck valve ∘ No money in a checking account ∘ Broken wire ∘ Software error ∘ System down ∘ Reactor melting down	What caused the failure: Broken part Electrical failure Human error Explosion Bug in software	Outcome of the failures: Nothing System crash Explosion Fire Accident Environmental release	How possible is it: Can use numeric values: 0.1, 0.01, or 1E-5 Can use a qualitative measure: negligible, low probability, high probability	How bad are the results: Can use dollar value: $10., $1 000., or $1 000 000 Can use a qualitative measure: nil, minimal problems, major problems	What can be done to prevent either failures or results of the failures?

TABLE 11.2
Process Steps For Starting a Lawn Mower

FMEA, starting a lawn mower Process steps
Check gas and oil
Fill as necessary
Set controls
Initiate starter

TABLE 11.3
Failure Modes Associated With Process Steps

FMEA, starting a lawn mower	
Process steps	Potential failure modes
Check gas and oil	Unable to remove gas cap
	Unable to remove oil plug
	Unable to determine depth of oil
	Oil or gas spill
Fill as necessary	No oil available
	Gas station closed
	No gas container
	Overfill gas
	Overfill oil
	Water in gas or oil
Set controls	Controls broken
	No instruction available
	Controls out of adjustment
Initiate starter	Starter malfunction
	Cord broken
	Engine flooded
	Ignition system malfunction

For the purposes of an FMECA, rough calculations can be developed using:

- Historical data
- A Delphi-like technique (3)
- Accident data
- Subject matter expert(s)
- Best estimate

Table 11.7 presents a way to calculate criticality based on probability.

TABLE 11.4
Effect of Potential Failures

FMEA, starting a lawn mower		
Process steps	Potential failure modes	Potential failure effects
Check gas and oil	Unable to remove gas cap	Delay in process or personal injury
	Unable to remove oil plug	Delay in process
	Unable to determine depth of oil	Delay in process or the potential to overfill oil level
	Oil or gas spill	Environmental damage or potential for fire
Fill as necessary	No oil available	Delay in process
	Gas station closed	Delay in process
	No gas container	Delay in process
	Overfill gas	Potential for a fire or environmental damage
	Overfill oil	Environmental damage
	Water in gas or oil	Delay in process or engine damage
Set controls	Controls broken	Delay in process
	No instruction available	Delay in process
	Controls out of adjustment	Delay in process or engine damage
Initiate starter	Starter malfunction	Delay in process and/or repairs necessary
	Cord broken	Delay in process and/or repairs necessary
	Engine flooded	Delay in process
	Ignition system malfunction	Delay in process and/or repairs necessary

Note that the probability numbers in Table 11.5 provide an indication of the level of criticality and not an absolute failure probability.

Organizations have also developed risk matrices that can also be used to indicate criticality. Table 11.8 shows such a matrix. Note that these matrices provide a way to combine probability of occurrence with severity of consequence. Also note that these matrices are subjective in nature but do provide a way to systematically assess risk.

The following example (Table 11.9) shows all the elements of an FMECA developed for assessing the steps in the lawn mower-starting example. Note that probability can also be included. The first step in this process is to determine what does "criticality" mean in this context. Is it how bad might the consequences be or how critical the step is in the operation of the system? For this process we will make the assumption that criticality means how bad might the consequences be if we don't perform the step correctly.

11.2 SUMMARY

FMEA and FMECA are very effective tools. They can be applied to a broad range of applications and industries and are effective in elucidating the vulnerabilities of a system and its subsystems. Like PHA, FMEA and FMECA are applied early in the

TABLE 11.5
Failure Mode And Effects Analysis With Potential Causes Of Failures Listed

FMEA, Starting a Lawnmower			
Process steps	Potential failure modes	Potential failure effects	Potential causes of failures
Check gas and oil	Unable to remove gas cap	Delay in process or personal injury	Cap rusted or broken
	Unable to remove oil plug	Delay in process	Operator error or plug cross threaded
	Unable to determine depth of oil	Delay in process or the potential to overfill oil level	Operator error or poor lighting
	Oil or gas spill	Environmental damage or potential for fire	Operator error
Fill as necessary	No oil available	Delay in process	Lack of planning
	Gas station closed	Delay in process	Lack of planning
	No gas container	Delay in process	Lack of planning
	Overfill gas	Potential for a fire or environmental damage	Lack of adequate equipment or operator error
	Overfill oil	Environmental damage	Lack of adequate equipment or operator error
	Water in gas or oil	Delay in process or engine damage	Poor practices
Set controls	Controls broken	Delay in process	Was not proper used on prior occasion
	No instruction available	Delay in process	Instructions not properly stored on prior occasion
	Controls out of adjustment	Delay in process or engine damage	Controls not properly maintained
Initiate starter	Starter malfunction	Delay in process and/or repairs necessary	Inadequate inspection or periodic maintenance
	Cord broken	Delay in process and/or repairs necessary	Inadequate inspection or periodic maintenance
	Engine flooded	Delay in process	Improper use of controls
	Ignition system malfunction	Delay in process and/or repairs necessary	Inadequate inspection or periodic maintenance

TABLE 11.6
Complete Table

FMEA, starting a lawn mower				
Process steps	Potential failure modes	Potential failure effects	Potential causes of failures	Control measure
Check gas and oil	Unable to remove gas cap	Delay in process or personal injury	Cap rusted or broken	Cap maintenance program
	Unable to remove oil plug	Delay in process	Operator error or plug cross threaded	Operator training
	Unable to determine depth of oil	Delay in process or the potential to overfill oil level	Operator error or poor lighting	Operator training and provide additional lighting
	Oil or gas spill	Environmental damage or potential for fire	Operator error	Operator training
Fill as necessary	No oil available	Delay in process	Lack of planning	Ensure adequate oil is available
	Gas station closed	Delay in process	Lack of planning	Ensure fuel supply is available
	No gas container	Delay in process	Lack of planning	Provide equipment to minimize spill potential
	Overfill gas	Potential for a fire or environmental damage	Lack of adequate equipment or operator error	Provide equipment to minimize spill potential
	Overfill oil	Environmental damage	Lack of adequate equipment or operator error	Ensure fuel and oil containers are not exposed to sources of water
	Water in gas or oil	Delay in process or engine damage	Poor practices	
Set controls	Controls broken	Delay in process	Inspection and periodic maintenance	Institute inspection and periodic maintenance program
	Lack of labeling on the controls	Delay in process	Instructions not properly stored on prior occasion	Ensure controls are adequately labeled
	Controls out of adjustment	Delay in process or engine damage	Controls not properly maintained	Institute inspection and periodic maintenance program
Initiate starter	Starter malfunction	Delay in process and/or repairs necessary	Inadequate inspection or periodic maintenance	
	Cord broken	Delay in process and/or repairs necessary	Inadequate inspection or periodic maintenance	
	Engine flooded	Delay in process	Improper use of controls	
	Ignition system malfunction	Delay in process and/or repairs necessary	Inadequate inspection or periodic maintenance	

TABLE 11.7
Criticality Based on Probability

FMECA criticality		
Criticality	Relative probability rates	Probability rates
Very high: Failure is almost inevitable	1 in 3 to 1 in 2	0.33 to >0.50
High: Generally associated with processes similar to previous processes that have failed	1 in 20 to 1 in 8	0.05 to 0.125
Moderate: Generally associated with processes that have experienced occasional failures	1 in 2 000 to 1 in 80	0.005 to 0.0125
Low: Isolated failures associated with similar processes	1 in 15 000	0.000 067
Very low: Only isolated failures associated with almost identical processes	1 in 150 000	0.000 006 7
Remote: Failure unlikely. No failure ever associated with an almost identical processes	1 in 1 500 000	0.000 000 67

TABLE 11.8
Example Risk Matrix

Risk matrix					
Consequence	Probability of failure				
No effect	Very low probability <1 in 1 000 000	Low probability 1 in 1 000 000 to 1 in 100 000	Moderate probability 1 in 100 000 to 1 in 10 000	High probability 1 in 10 000 to 1 in 100	Very high probability >1 in 100
Minor consequence (repair costs less than $100 or down time <1 h)	Low risk	Low risk	Low risk	Minor risk	Minor risk
Moderate consequence (repair costs from $100 to 10 000 or down time from 1 to 24 h)	Low risk	Low risk	Minor risk	Moderate risk	High risk
High consequence (repair costs from $10 000 to 100 000 or down time from 24 to 120 h or minor environmental spill or minor personal injury	Low risk	Minor risk	Moderate risk	High risk	Very high risk
Severe consequence (repair costs >100 000 or down time >120 h or major environmental spill or severe injury or fatality)	Minor risk	Moderate risk	High risk	Very high risk	Severe risk

TABLE 11.9
Criticality Analysis

FMECA, starting a lawn mower					
Process steps	Potential failure modes	Potential failure effects	Potential causes of failures	Control measure	Criticality of step
Check gas and oil	Unable to remove gas cap Unable to remove oil plug Unable to determine depth of oil Oil or gas spill	Delay in process or personal injury Delay in process Delay in process or the potential to overfill oil level Environmental damage or potential for fire	Cap rusted or broken Operator error or plug cross threaded Operator error or poor lighting Operator error	Cap maintenance program Operator training Operator training and provide additional lighting Operator training	Low criticality
Fill as necessary	No oil available Gas station closed No gas container Overfill gas Overfill oil Water in gas or oil	Delay in process Delay in process Delay in process Potential for a fire or environmental damage Environmental damage Delay in process or engine damage	Lack of planning Lack of planning Lack of planning Lack of adequate equipment or operator error Lack of adequate equipment or operator error Poor practices	Ensure adequate oil is available Ensure fuel supply is available Provide equipment to minimize spill potential Provide equipment to minimize spill potential Ensure fuel and oil containers are not exposed to sources of water	High criticality if filling process is done incorrectly

TABLE 11.9
(*Continued*)

FMECA, starting a lawn mower					
Process steps	Potential failure modes	Potential failure effects	Potential causes of failures	Control measure	Criticality of step
Set controls	Controls broken Lack of labeling on the controls Controls out of adjustment	Delay in process Delay in process Delay in process or engine damage	Inspection and periodic maintenance Instructions not properly stored on prior occasion Controls not properly maintained	Institute inspection and periodic maintenance program Ensure controls are adequately labeled Institute inspection and periodic maintenance program	Low criticality
Initiate starter	Starter malfunction Cord broken Engine flooded Ignition system malfunction	Delay in process and/or repairs necessary Delay in process and/or repairs necessary Delay in process Delay in process and/or repairs necessary	Inadequate inspection or periodic maintenance Inadequate inspection or periodic maintenance Improper use of controls Inadequate inspection or periodic maintenance		Low criticality

The highly critical step in this process concerns adding oil or fuel. In these cases, then, warnings/cautions should be included in the procedure, or the system should be modified to include controls to prevent adding fuel to a hot engine.

design life of a system and used to ensure the system has no unidentified failure points. As with the Mars Global Surveyor, we have to determine up front what is a failure and what is success.

Self-Check Questions

1. Perform an FMEA on a small appliance.

2. In some cases an FMEA might be as detailed of a risk assessment that is needed. Why or why not?

3. Perform an FMEA on your house, apartment, or dorm room. Discuss what you found.

4. Perform an FMEA on your car, SUV, pickup, or public transportation system. Discuss what you found.

5. Do you think an FMEA should be performed on social media platform? Discuss what such an analysis might reveal.

REFERENCES

1. NASA (2007). Report Reveals Likely Causes of Mars Spacecraft Loss|NASA. http://www.nasa.gov/mission_pages/mgs/mgs (accessed August 2018).
2. Department of Defense (2012). *Standard Practice System Safety, Mil std 882E*. US Military.
3. Gertman, D. and Blackman, H.S. (1994). *Human Reliability and Safety Analysis Handbook*. New York: Wiley.