Presentation Notes
Paper
Bio
Return to Main Menu

PRESENTATION

T5

Thursday, November 4, 1999
10:30 AM

IDENTIFYING CRITICAL REQUIREMENTS USING FMEA

Edith Maverick-Folger
LifeScan Inc.

INTERNATIONAL CONFERENCE ON
SOFTWARE TESTING, ANALYSIS & REVIEW
NOVEMBER 1-5, 1999
SAN JOSE, CA

Identifying Critical Requirements Using FMEA*

*Failure Mode and Effects Analysis

Edith Maverick-Folger
LifeScan Inc.

A Quote . . .

An FMEA can reduce or eliminate the chance of implementing a corrective change which could create an even larger concern.

– Chrysler Corporation
– Ford Motor Company
– General Motors Corporation

Incident: The Lithium Battery

- Process Function: Station software turns on meter for the first time and initiates manufacturing mode.
- Potential Failure Mode: Meter smokes.
- Potential Cause of Failure: Polarity of Lithium battery reversed.
- Potential Effect of Failure: Destroy an otherwise good meter.

Lithium Battery Continued . . .

- Current Process Controls: Functional requirement to do lithium battery test before turning on meter.
- Severity: 8 (destroy product, no repair).
- Occurrence: 6 (1:80).
- Detectability: 1 (almost certain).
- RPN (Risk Priority Number): 48.

Application to Software

- Problems are only cheap and easily fixed early in the development process.
- FMEA reduces the risk of error at the requirements stage.
- I recommend you customize the FMEA process for your business to mitigate hazards and disconnects ASAP.

The Columns Explained

- Sequence Number (optional--for tracing)
- Process Function
- Potential Failure Mode
- Potential Effects of Failure
- Severity Number
- Class Number (optional)
- Potential Cause(s) of Failure

The Columns Continued

- Occurrence Number
- Current Process Controls
- Detection Number
- Risk Priority Number = Severity x Occurrence x Detectability
- Recommended Actions
- Responsibility & Target Completion Date

The Columns Continued

- Action Results Columns
  - Actions Taken
  - Severity Number
  - Occurrence Number
  - Detection Number
  - Risk Priority Number = Severity x Occurrence x Detectability

The FMEA Meeting

- Another Quote: . . . *the responsible engineer is expected to directly and actively involve representatives from all affected areas*.
- The group constructs the FMEA.
  - The process can be started with a draft or an FMEA of a similar product.
  - The meeting location should be close to reference materials.

The FMEA Meeting Continued

- Usually meetings take a number of half or full day sessions.
  - there needs to be a moderator and recorder.
  - Plan hourly breaks.
  - Make sure technology doesn't make the meeting slower.
- Fill out Function, Failure Mode and Cause columns, completely, first.

The FMEA Meeting Continued

- Fill out Severity, Occurrence and Detection columns one at a time.
  - The idea is to get a ranking.
  - Don’t get hung up on the absolute value of the number.
  - If you use a spreadsheet, the RPN can be calculated automatically.

FMEA--A Demonstration! The Triangle Requirement

- Audience divides into four groups:
  - Software Engineers
  - V&V / QE
  - Sales
  - Marketing / Packaging.

Summary

- Customize FMEA for your business.
- Mitigate hazards and disconnects in the requirements phase.
- Your customers are counting on you.

Identifying Critical Requirements Using FMEA – Edith Maverick-Folger

> *Up front time spent in doing a comprehensive FMEA well, when product / process changes can be most easily and inexpensively implemented, will alleviate late change crises. An FMEA can reduce or eliminate the change of implementing a corrective change which could create an even larger concern. Properly applied, it is an interactive process which is never ending.*[1]
> --Potential Failure Mode and Effects Analysis (FMEA) Reference Manual.

The authors of this quote are Chrysler Corporation, Ford Motor Company, and General Motors Corporation. These automobile companies first issued this pamphlet in 1993, as part of their quality methods standardization process QS-9000. The first formal application of the FMEA process was in the aerospace industry in the mid-1960's.

Engineers in other specialties have adopted the FMEA to analyze all sorts of manufacturing processes and products. The FMEA process allows a development team to identify potential product related process failure modes and assess the effects these failures might have.

The execution of a software program is comparable to a manufacturing process. Software takes input, manipulates it, and delivers a result, just as a process on a manufacturing line would. The FMEA process explores this sequence of events, finds potential failure modes, their causes and effects, and, where necessary, prompts the correct people to take actions to prevent failures. The process also attempts to produce an overall ranking of hazards by prompting the team members to rank a problem for severity, occurrence and detectability.

First, let us get through some verbiage. Just like test people maintain that there is a difference between validation and verification, failure analysis claims exact definitions for harm, hazard and risk.

Definitions in Failure Mode Effects Analysis:	
Harm:	Physical injury or damage to health or property.
Hazard:	A potential source of harm.
Risk:	The probability rate of occurrence of a hazard causing harm and the degree or severity of the harm.

An Example FMEA Table

Page 2 has the example of an FMEA table, populated with some items from this triangle identification problem.

The Triangle Problem:
Develop a program that, given a computer punch card with three numbers on it, tells me what sort of triangle they describe—equilateral, isosceles or scalene.

Page 3 is a blank FMEA page for your use.

Example FMEA Table—Triangle problem

SEQ #	Process Function or Description	Potential Failure Mode	Potential Effects of Failure	Severity	Potential Cause of Failure	Occurrence	Current Process Controls	Delectable	RPN	Recommended Action(s)	Responsible Area and/or Completion Date	Resulting Actions Taken	Severity	Occurrence	Delectability	RPN
10	Get input from computer punch card	Does not decode card correctly	Program fails to deliver an answer Program delivers the wrong answer	4 10	Use ASCII, or another proprietary character set, instead of EBCDIC	6 6	Program filters out all non-numeral input Program will use BCS for card input, a subset of EBCDIC and other punch card codes	1 10	24 600	Test card decoding						
20		Non numeric input gets interpreted as numeric input	Program fails to deliver an answer Program delivers the wrong answer	4 10	Operator mistakenly puts in characters other than numerals	6 6	Program filters out all non-numeral input Program uses BCS for card input	1 10	24 600	Test program non-numeric input handling						
30	Translate string into numeric values	There are less than three numbers translated from card input.	Program fails to deliver an answer	4	Operator did not put delimiters between each number	6	Instructions for usage include directions to leave spaces between numeric values	1	24	Test program on different numbers of numeric values						

Example FMEA Table

SEQ #	Process Function or Description	Potential Failure Mode	Potential Effects of Failure	Severity	Potential Cause of Failure	Occurrence	Current Process Controls	Delectable	RPN	Recommended Action(s)	Responsible Area and/or Completion Date	Resulting Actions Taken	Severity	Occurrence	Delectability	RPN

Description of the FMEA Table Columns

The FMEA table is at the center of this effort. Each row is a step in the process, and its columns are defined as follows:

1. SEQ#: The sequence number. You may want to increment by 10 for squeezing in unforeseen steps.

2. Process Function or Description:
   - Get input from computer punch card.

3. Potential Failure Mode:
   - Does not decode card correctly.

4. Effects of failure, there are two identified in this case:
   - Program fails to deliver an answer
   - Program delivers the wrong answer

5. Severity is ranked on a scale from 1 to 10. There are two effects to rank. The first one ranks a 4 and the second ranks a 10.

6. Potential Cause of Failure:
   - Use ASCII, or another proprietary character set, instead of EBCDIC

7. Occurrence ranked on a scale from 1 to 10. Typos happen--this a 6.

8. Current Process controls: Example
   - Program filters out all non-numeral input
   - Program will use BCS for card input, a subset of EBCDIC and other punch card codes

9. Delectable ranked on a scale from 1 to 10. The less detectable the failure is, the worse it is. Program failing to deliver an answer gets a 1. However, program delivering the wrong answer, gets a 10.

10. RPN: Multiply Sev. Occ. and Det.: We get 24 for the first effect and 600 for the second effect.

11. Recommended Actions: If no action is warranted, this column entry may be blank. For this example we have:
    - Test card decoding

12. Responsible Area and/or Completion Date: The engineers needed to implement the recommended actions.

12. Resulting Action(s) Taken: Documenting what (if any) fix was implemented.

13,14,15,16. Resulting Sev. Occ., Det. and RPN: Updated numbers with the fix in place.

An optional Class column can appear after the Severity column. If the FMEA is to keep track of layers of functionality, then it might benefit from the addition of this column. Alternatively, you might want to do a separate FMEA for that functionality.

For this table column description, I picked an example that does have a specific order. Many times in software there is no predetermined order of execution. The order of events depends upon user input,

random number generators, or the previous stopping point. Assign an order. The collaborative process of the FMEA meeting needs to consider all the events. Perhaps a latent order of events will be uncovered.

Structure of an FMEA Meeting

FMEA meetings are usually half a day to a day long, and, for any project of size, it takes a series of these to finish identifying all of the steps of a process. A meeting series may start out with an FMEA table from a similar piece of software, or someone may come up with a rough draft to get things started. But the charter of these meetings is to generate the FMEA.

The primary focus of the early meeting(s) should be:

- Description,
- Failure Mode,
- Causes of Failure,
- Current Process Controls
- ***not*** *on the numbers*.

The severity, occurrence and detectable numbers are for ranking priority, not for assigning an absolute measure. Do not get hung up on them. Dissuade the other team members from obsessing on them. As long as the more important issues have larger numbers than the less important ones, the process is working.

Once the Description, Failure Mode, Causes of Failure, and Current Process Controls columns are filled out, completely, for the whole project, then go back and fill in the numbers, one column at a time, so the ranking will be consistent for all issues. Multiplication can take place off-line or automatically if using a spreadsheet.

The Potential Effects of Failure column can be filled in at the same time as the Severity column. Fill in the Recommended Actions column after priorities have been set. You may choose to do nothing about low priority items.

The Resulting Actions columns are filled in at a follow-up meeting after corrective actions have been taken.

Criteria Charts

All companies will have different takes on what these rankings indicate. They need to be customized for your application.

Severity Criteria

10	Hazardous-without warning
9	Hazardous-with warning
8	Very High
7	High
6	Moderate
5	Low
4	Very Low
3	Minor
2	Very Minor
1	None

Occurrence Criteria

10	1 in 2
9	1 in 3
8	1 in 8
7	1 in 20
6	1 in 80
5	1 in 400
4	1 in 2000
3	1 in 15,000
2	1 in 150,000
1	1 in 1,500,000

Detection Criteria

10	Almost Impossible
9	Very Remote
8	Remote
7	Very Low
6	Low
5	Moderate
4	Moderately High
3	High
2	Very High
1	Almost Certain

Hints on Running FMEA Meetings

FMEA meetings need to be collaborative, but they are not brainstorming sessions.

FMEA meetings are held over a series of weeks, with a portion of time each week dedicated to the process. Some issues will arise that will need input from people not in the room, or participants may need other information from their offices to continue.

In my experience, the project manager or responsible engineer often gets both the moderator and recorder jobs. This really slows the meeting down. Delegate. The meetings are long enough as they are.

The moderator must remind participants to take breaks every hour, and ergo stretches more often, as the day wears on.

Here are some suggestions for the recorder who wants to use a computer hooked to a projector to get the editing done in real time:

- Make sure the extension cord is comfortably long enough to get from the wall to your computer.
- Use a real keyboard and a real mouse or roller ball.
- Get the keyboard at the right ergonomic height.
- Use a spreadsheet, and hide the columns not being worked on.
- Get a bright projector, and pick a font that displays well.
- Learn the keyboard shortcut keys.

Conclusion

Generating an FMEA for your project will drive out uncertainty, and flush out those requirements that were assumed to be common knowledge. Often the mitigation to a hazard will be software testing. Providing the traceability from the hazard to the test will document that your software is under control.

EDITH MAVERICK-FOLGER

Edith Maverick-Folger is a software engineer with LifeScan Inc. She has 10 years' experience in medical biotech development, QA, and validation under FDA cGMP's and ISO 9000 guidelines. At LifeScan, she tests software for the automated test and assembly stations on blood glucose meter manufacturing lines. As a V&V professional, her overriding goal is to bring a focus on quality, from requirements to test, for system development.

To build in quality, an organization needs to find problems early in the development cycle. This minimizes the time and cost of a project. Biotechnology's diverse engineering teams share their different quality assurance methods to achieve this goal; consequently, at LifeScan, Edith was introduced to Failure Mode and Effects Analyses (FMEAs).

Edith has a B.A. in computer science. She added QA laboratory work, electronics, and manufacturing statistics skills through work experience and further education.