DEVELOPMENT AND APPLICATION OF SFMEA MODEL TO SOFTWARE TESTING ENVIRONMENT

Dr. R. Dillibabu¹, Sangeetha. A², L. Sudha³

¹Department of Industrial Engineering, Anna University, Chennai- 600025, India
²Department of Industrial Engineering, Anna University, Chennai- 600025, India
³Department of Management studies, Anna University, Chennai-600025, India

ABSTRACT

In software industry, the concept of quality has become a significant aspect and is expressed and defined in many different ways. Quality assurance, and in particular software testing and verification, are areas that yet have much to offer to the industry. This paper emphasizes the importance of a quality process and also discusses about the ways in which it could be achieved through offline software quality techniques in particular SFMEA Model.

Software FMEA determines the software failure modes that are likely to cause top level failure events. Software FMEAs are useful when designing and testing the error handling part of the software process. It has to be found that there is significant improvement in quality in terms of reduced RPN values.

A detailed literature was collected for the SFMEA model. The application of these SFMEA model for the software development is very much limited. Only few papers were highlighted the application of these model in software industry. The objectives can be achieved by developing the SFMEA model for the software development of three banking projects. The construction of the SFMEA model was compiled for the software development. The causes and effects for the failures were analyzed and validated using the SFMEA model.

1.0 INTRODUCTION

In software industry, the concept of quality has become a significant aspect with respect to customer satisfaction. This project mainly focuses on the offline quality assurance of software products and capturing the customer satisfaction.
1.1 Offline Quality Assurances

Offline Quality Assurance deals with the measures to select and choose controllable product and process parameters in such a way that the deviation between the product or process output and the standard will be minimized. These techniques include QFD, FMEA, Design of Experiments, Taguchi Methods, etc.

1.1.1 Software Quality Assurance

When we examine an item based on its measurable characteristics, two kinds of quality may be encountered: Quality of design and Quality of conformance. In software development, quality of design encompasses requirements, specifications and the design of the system. Quality of conformance is an issue focused primarily on implementation.

Software quality is defined as “Conformance to explicitly stated functional and performance requirements, explicitly documented development standards, and implicit characteristics that are expected of all professionally developed software”.

Software quality definition serves to emphasize three important points:

- Software requirements are the foundation from which quality is measured. Lack of conformance to requirements is lack of quality.
- Specified standards define a set of development criteria that guide the manner in which software is engineered. If the criteria are not followed, lack of quality will almost surely result.
- There is a set of implicit requirements that often goes unmentioned. If software conforms to its explicit requirements but fails to meet implicit requirements, software quality is suspect.

Software quality assurance is an umbrella activity that is applied throughout the software process. It is considered to be one of the important planning and management concepts in developing and improving the products at any stage of manufacture. It is important to control the defects at any stages of development phases, hence it is necessary to adopt the preventive technique to reduce the errors and improve the quality in all the phases. The important techniques used to reduce the defects is Software Failure Mode and Effects Analysis (SFMEA).

1.1.1.1 Failure Mode And Effect Analysis (FMEA)

Failure Mode and Effects Analysis (FMEA) was one of the first systematic techniques for failure analysis. It was developed by reliability engineers in the 1950s to study problems that might arise from malfunctions of military systems. A FMEA is often the first step of a system reliability study. It involves reviewing as many components, assemblies, and subsystems as possible to identify failure modes, and their causes and effects. For each component, the failure modes and their resulting effects on the rest of the system are recorded in a specific FMEA worksheet. There are numerous variations of such worksheets. A FMEA is mainly a qualitative analysis.

FMEA is a systematic way to recognize and evaluate the potential failures of a product or process. It provides a formal mental discipline for eliminating or reducing the risks of product failure. It also serves as a living document, providing a method of organizing and tracking concerns and changes through product development.
FMEA is an interactive process of continuous improvement that involves team effort. Functional areas involved include design, materials, manufacturing, assembly, packaging, shipping, service, recycling, and quality. It is a procedure by which each potential failure mode in a system is analyzed to determine the results or effects thereof on the system and to classify each potential failure mode according to its severity.

Why Use Failure Modes Effects Analysis

The FMEA process captures and documents what is known about:

- How the product or process may fail to meet the customer's expectations (The failure modes),
- The consequences of failure, within the extended supply chain or in use. (The effects of failure)
- The potential causes of failure, including errors and omissions in the specification, design or production process that could generate, or allow, the failure to occur
- The controls or countermeasures introduced to prevent failure, by eliminating the causes, or to detect the error condition and alert you potential failure so that the effects can be mitigated or avoided.

There are many types of FMEA, but the most widely used are probably the following:

- System FMEA, which is used for global systems;
- Design or Product FMEA, which is used for components or subsystems;
- Process FMEA, which is used for manufacturing and assembly processes;
- Service FMEA, which is used for services; and
- Software FMEA, which is used for software.

Despite the existence of many types of FMEA today, the basic structure and process for executing them remains the same. Any FMEA process must include the following steps, information details of which are documented in the FMEA Table:

- Assembly of the team;
- Understanding of the Product or Process to be subjected to FMEA;
- Breaking down of the product or process into its components or steps (components and steps are also known as items);
- Identification and assessment of the following for every item listed: function(s), potential failure mode(s), failure mode effect(s), failure mode cause(s), and controls for detecting or preventing the failure mode(s);
- Evaluation of the risks associated with the failures modes and prioritizing them according to importance;
- Implementation of corrective actions to minimize the occurrence of the more significant failure modes;
- Reassessment of the product or process by another cycle of FMEA after the actions have been completed; and
- Regular updating of the FMEA Table.
The most critical information on the FMEA Table is the Risk Priority Number (RPN), which is the numerical rating given to the level of risk associated with a failure mode, and therefore denotes the urgency of addressing that failure mode.

The RPN is actually the product of three (3) factors, namely, the severity of the effect of the failure mode (SEV), the probability of the occurrence of the cause of the failure mode (OCC), and the effectiveness of the controls for detecting and preventing the failure mode (DET). Thus, RPN = SEV x OCC x DET. The SEV, OCC, and DET are also documented in the FMEA Table.

The FMEA Table is a living document, constantly changing from the time of its first release when the product or process is still being designed until its archiving after the product or process has been obsolete.

Critical times or events that require an update to the FMEA Table include the following:

- When a new product or process is being designed or introduced;
- When a critical change in the operating conditions of the product or process occurs;
- When the product or process itself undergoes a change;
- When a new regulation that affects the product or process is instituted;
- When customer complaints about the product or process are received; and
- When an error in the FMEA Table is discovered or new information that affects its contents comes to light.

1.1.4.2 Ground Rules And Benefits Of FMEA

A. Ground Rules of FMEA

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

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

B. Benefits of FMEA

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

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

A basis for in-flight troubleshooting procedures and for locating performance monitoring and fault-detection devices.

Criteria for early planning of tests.

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

1.1.4.3 Detection, Risk Priority Number, Severity and Remarks

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

B. Risk Priority Number (RPN)
Cost (of the event) * Probability (of the event occurring) * Detection (Probability that the event would be detected before the user was aware of it)

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

D. Remarks / Mitigation / Actions
Additional info, including the proposed mitigation or actions used to lower a risk or justify a risk level or scenario.

1.1.5 Software Failure Mode And Effect Analysis (SFMEA)
The application of FMEA to software was first proposed in 1979. Since that time, the software FMEA has been refined and applied successfully at functional, interface and detailed levels. Some of the approaches taken to SFMEA; however, are flawed. Software FMEA has also been useful in conjunction with requirements analysis.

The failure modes of software are generally unknown. The software modules do not fail, they only display incorrect behavior. SFMEA has to find out the appropriate starting point for the analysis, set up a list of relevant failure modes and understand what makes those failure modes possible and what their consequences are. The failure modes in SFMEA should be seen in a wide perspective reflecting the failure modes of incorrect behavior of the software.

This is achieved by introducing controls including:-
Prevention Controls to eliminate or reduce the causes of failure, and
Detection Controls to give warning of a fault or error condition

The level of risk associated with particular failure modes is determined by considering:-
The effects the failure will have when it occurs (Severity), and
The chance that the causes of failure will be present (Occurrence), and
The ability to detect when the error condition is present (Detection) so that the consequences of the failure are reduced or avoided.
2.0 LITERATURE REVIEW

The detailed literatures were collected for the SQFD Model. Based on the literatures studied or reviewed, the problem statement has been identified.

Ozarin, N, Siracusa, M (2003) points out that Software FMEA is a means to determine whether any single failure in computer software can cause catastrophic system effects, and additionally identifies other possible consequences of unexpected software behavior. The procedure described here was developed and used to analyze mission- and safety-critical software systems. The procedure includes using a structured approach to understanding the subject software, developing rules and tools for doing the analysis as a group effort with minimal data entry and human error, and generating a final report. Software FMEA is a kind of implementation analysis that is an intrinsically tedious process but database tools make the process reasonably painless, highly accurate, and very thorough. The main focus here is on development and use of these database tools.

Dong Nguyen (2001) has written that this paper presents a systematic problem solving approach, which is based on the failure modes and effects analysis (FMEA), to system software reliability. This approach was created for software reliability analysis and testing in the multimedia digital distribution system (MDDS) at Thomson-CSF Sextant In-Flight Systems to improve the software reliability for the ISDN Communication Control Unit (CCU) subsystem of the MDDS, and then globally applied to the software reliability analysis MDDS and improvement for the whole MDDS. It has been proven to be an effective and efficient approach to system software reliability.

There is a gap in the application of FMEA model to software development process. These applications will ensure that the software development process will give 100% deliverables.

3.0 PROBLEM STATEMENT

In order to meet the software quality assurance in all phases in software development process and customer satisfaction, it is better to use SQA model like SFMEA model in software testing environment. The objective of the project is

- To apply SFMEA model in software testing environment.
- To validate the implementation of SFMEA model.

4.0 IMPLEMENTATION OF SOFTWARE FMEA MODEL

This model has been implemented in a leading software company for software development process. The objective of this study is to bring out the zero-defect or defect free testing in the testing phase. The various failure modes of application 1 and application 2 are identified. From the occurrence, severity and detection of the failures, the risk priority number is calculated. The corrective actions are recommended to reduce the effects of the failures. After the action taken, again the risk priority number is calculated from the occurrence, severity and detection of the failures. The bar chart can be drawn for risk priority number values and the difference can easily be understood.
### Table 1: Occurrence Rating Values

<table>
<thead>
<tr>
<th>Occurrence Rating</th>
<th>Probability of failure</th>
<th>Rating</th>
<th>Criteria</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Very Frequently</td>
<td>10</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Frequently</td>
<td>8</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Sometimes</td>
<td>4</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Rare</td>
<td>1</td>
</tr>
</tbody>
</table>

### Table 2: Severity Rating Values

<table>
<thead>
<tr>
<th>Severity Rating</th>
<th>Effect</th>
<th>Rating</th>
<th>Criteria</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Very High</td>
<td>10</td>
<td>Rework is greater than 8ph</td>
</tr>
<tr>
<td></td>
<td>High</td>
<td>7</td>
<td>Rework is greater than 4ph &amp; &lt; 8ph</td>
</tr>
<tr>
<td></td>
<td>Moderate</td>
<td>5</td>
<td>Rework is greater than 2ph &amp; &lt; 4ph</td>
</tr>
<tr>
<td></td>
<td>Low</td>
<td>3</td>
<td>Rework is greater than 1ph &amp; &lt;2ph</td>
</tr>
<tr>
<td></td>
<td>Very Low</td>
<td>1</td>
<td>Rework is less than 1ph</td>
</tr>
</tbody>
</table>

### Table 3: Detection Rating Values

<table>
<thead>
<tr>
<th>Detection Rating</th>
<th>Detection</th>
<th>Rating</th>
<th>Criteria</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Difficult</td>
<td>10</td>
<td>No defined methods for identifying the process error &amp; only the o/p product analysis lead to detection</td>
</tr>
<tr>
<td></td>
<td>Moderate</td>
<td>5</td>
<td>Can be identified in the exit phase of the process or subsequent process entry check</td>
</tr>
<tr>
<td></td>
<td>Easy</td>
<td>1</td>
<td>process has built in checks for identifying sub process failure</td>
</tr>
</tbody>
</table>
4.1 SFMEA FOR APPLICATION1

The modes of failures for application1 are mentioned below.

- inadequate skills/knowledge about the process
- inadequate time
- requirement change
- inappropriate skilled resources for DEV
- testing & review objective is not clear
- inappropriate skilled resources for testing & review
- not reused the existing rules
- invalid data
- testing objective is not clear
- inappropriate skilled resources for testing
- inappropriate skilled resources for review
- inadequate time
- improper details about code review

For the above modes of failures, the effects and causes of failures and the current controls are noted in the table. The current status will be captured through occurrence, severity, detection of the failures. The risk priority number is calculated as the product of occurrence, severity, detection of the failures. The revised status can be captured after the implementing the recommended corrective actions.

Table 4: SFMEA for Application1

<table>
<thead>
<tr>
<th>SFMEA No: A1</th>
<th>SFMEA COMMITTEE: Project Team</th>
</tr>
</thead>
<tbody>
<tr>
<td>SHEET No. 1</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Item</th>
<th>Failure/Process</th>
<th>Sub Process</th>
<th>Mode of Failure</th>
<th>Effect of Failure</th>
<th>Cause of Failure</th>
<th>Current Controls</th>
<th>Current Status</th>
<th>Recommended Corrective Actions</th>
<th>Action By</th>
<th>Action Taken</th>
<th>Revised Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Coding</td>
<td>Planning</td>
<td>Inadequate skills/ knowledge about the process</td>
<td>Unable to access the application</td>
<td>Request has not been raised to get access</td>
<td>This should be added in implementation</td>
<td>4</td>
<td>4</td>
<td>1</td>
<td>Assigning JSPC to get access</td>
<td>Project Manager (PM)</td>
<td>Knowledge Transfer about process</td>
</tr>
<tr>
<td>Coding</td>
<td>Planning</td>
<td>Inadequate time</td>
<td>Delivery not in time</td>
<td>Request Estimated hours</td>
<td>Estimation should be done by skilled resources</td>
<td>4</td>
<td>4</td>
<td>5</td>
<td>1</td>
<td>10</td>
<td>9</td>
</tr>
<tr>
<td>Coding</td>
<td>Development</td>
<td>Not reused the existing data</td>
<td>File size is huge to store</td>
<td>Increase in the count of files</td>
<td>Code Review should be done to check the logic and rules handled</td>
<td>4</td>
<td>4</td>
<td>5</td>
<td>1</td>
<td>10</td>
<td>10</td>
</tr>
<tr>
<td>Coding</td>
<td>Testing</td>
<td>Invalid data</td>
<td>Defects raised</td>
<td>Improper data handled with testing</td>
<td>Proper Unit Test Scripts should be provided</td>
<td>4</td>
<td>4</td>
<td>5</td>
<td>1</td>
<td>10</td>
<td>10</td>
</tr>
<tr>
<td>Coding</td>
<td>Review</td>
<td>Inappropriate skilled resources for Review</td>
<td>Defects raised</td>
<td>Projected un necessary codes</td>
<td>Should give this details about the code to be reviewed</td>
<td>4</td>
<td>4</td>
<td>5</td>
<td>1</td>
<td>10</td>
<td>10</td>
</tr>
</tbody>
</table>
4.2 SFMEA FOR APPLICATION2
The modes of failures for application1 are mentioned below.
- Inadequate skills/ knowledge about the process
- Inadequate time
- Requirement Change
- Inappropriate skilled resources for DEV
- Testing & Review objective is not clear
- Inappropriate skilled resources for Testing & Review
- Not reused the existing rules
- Invalid data
- Testing objective is not clear
- Inappropriate skilled resources for Testing
- Inappropriate skilled resources for Review
- Inadequate time
- Improper details about code review

For the above modes of failures, the effects and causes of failures and the current controls are noted in the table. The current status will be captured through occurrence, severity, detection of the failures. The risk priority number is calculated as the product of occurrence, severity, detection of the failures. The revised status can be captured after the implementing the recommended corrective actions.
Table 5: SFMEA for Application2

SFMEA No: A2
SFMEA COMMITTEE: Project Team
SHEET No. 1

4.3 SFMEA FOR APPLICATION3
The modes of failures for application1 are mentioned below.
- Inadequate skills/knowledge about the process
- Inadequate time
- Requirement Change
- Inappropriate skilled resources for DEV
- Testing & Review objective is not clear
- Inappropriate skilled resources for Testing & Review
- Not reused the existing rules
- Invalid data
- Testing objective is not clear
- Inappropriate skilled resources for Testing
- Inappropriate skilled resources for Review
- Inadequate time
- Improper details about code review

For the above modes of failures, the effects and causes of failures and the current controls are noted in the table. The current status will be captured through occurrence, severity, detection of the failures. The risk priority number is calculated as the product of occurrence, severity, detection of the failures. The revised status can be captured after the implementing the recommended corrective actions.
Fig. 2: Bar Chart of RPN values for Application2

Table 6: SFMEA for Application3

<table>
<thead>
<tr>
<th>Process</th>
<th>SFMEA No: A3</th>
<th>SFMEA COMMITTEE: Project Team</th>
</tr>
</thead>
<tbody>
<tr>
<td>SHEET No. 1</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Functional/Process</th>
<th>Sub Process</th>
<th>Mode of Failure</th>
<th>Effect of Failure</th>
<th>Cause of Failure</th>
<th>Current Controls</th>
<th>Current Status</th>
<th>Recommended Corrective Actions</th>
<th>Activity</th>
<th>Action Taken</th>
<th>Revisited Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Coding</td>
<td>Planning</td>
<td>Inadequate skill/ knowledge about the process</td>
<td>Unable to access the application</td>
<td>Request has not been</td>
<td>4</td>
<td>5</td>
<td></td>
<td>Assigning QC to access</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>Coding</td>
<td>Planning</td>
<td>Inadequate time</td>
<td>Delivery not in time</td>
<td>Incorrect Estimated hours</td>
<td>4</td>
<td>10</td>
<td>5</td>
<td>Project Owner needs to review the estimation based on requirements given</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>Coding</td>
<td>Development</td>
<td>Not issued the testing plan</td>
<td>Rate is too high to</td>
<td>Increase in the cost of labor</td>
<td>4</td>
<td>5</td>
<td>1</td>
<td></td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>Coding</td>
<td>Testing</td>
<td>Inadequate data</td>
<td>Defects raised</td>
<td>Data not available until testing</td>
<td>4</td>
<td>10</td>
<td>5</td>
<td></td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>Coding</td>
<td>Review</td>
<td>Inadequate data</td>
<td>Defects raised</td>
<td>Data is not available</td>
<td>4</td>
<td>5</td>
<td>1</td>
<td></td>
<td>1</td>
<td>2</td>
</tr>
</tbody>
</table>

5.0 CONCLUSIONS

It is found that there is a significant improvement in quality in terms of reduced RPN values. The RPN measures also indicate on which failure one has to concentrate to maximize the benefit. The results can be used further for continuing SFMEA process until the defect reaches to a satisfactory level.
ACKNOWLEDGEMENT

I am extremely thankful to my project guide Dr. R. Dillibabu, Department of Industrial Engineering for imitating keen interest and giving valuable guidance at every stage of this project.

I would also like to thank my parents, friends and well-wishers who encourage me to complete this project successfully.

REFERENCES