IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 1, January 2016

An innovated method using Failure mode and effects analysis for improving quality of the software

Dr.V.Sangeetha., M.Sc., Mphil[1], P.Saravanan[2]

Asst. Professor, Department of Computer Science, PRUCAS, Dharmapuri, Tamilnadu[1]

Asst. Professor, Department of Computer Science, Govt. Arts and Science College, Dharmapuri, Tamilnadu[2]

Abstract: Failure mode and effects analysis (FMEA) is a structured prospective risk assessment method that is widely used event logs. FMEA involves a multidisciplinary team mapping out a high-risk process of care, identifying the failures that can occur, and then characterizing each of these in terms of probability of occurrence, severity of effects and detect ability, to give a risk priority number used to identify failures most in need of attention. One might assume that such a widely used tool would have an established evidence base. This paper considers whether or not this is the case, examining the evidence for the reliability and validity of its outputs, the mathematical principles behind the calculation of a risk priority number, and variation in how it is used in practice. In this paper we described a model of FMEA and its failure and also explain various types of tools used in this method.

Keywords: Single failure points (SFPS), Failure mode and effects analysis (FMEA).

1. INTRODUCTION

1.1. Failure model:

Failure mode and effects analysis (FMEA)—also "failure modes," plural, in many publications—was one of the first systematic techniques for failure analysis. It was developed by reliability engineers in the late 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 can be a qualitative analysis, but may be put on a quantitative basis when mathematical failure rate models are combined with a statistical failure mode ratio database.[10]

A few different types of FMEA analyses exist, such as

- ✓ Functional
- ✓ Design, and
- ✓ Process FMEA.

FMEA is an inductive reasoning (forward logic) single point of failure analysis and is a core task in reliability engineering, safety engineering and quality engineering. Quality engineering is specially concerned with the "Process" type of FMEA.

A successful FMEA activity helps to identify potential failure modes based on experience with similar products and processes - or based on common physics of failure logic. It is widely used in development and manufacturing industries in various phases of the product life cycle. Effects analysis refers to studying the consequences of those failures on different system levels.

Functional analyses are needed as an input to determine correct failure modes, at all system levels, both for functional FMEA or Piece-Part (hardware) FMEA. A FMEA is used to structure Mitigation for Risk reduction based on either failure effect severity reduction or based on lowering the probability of failure or both. The FMEA is in principle a full inductive analysis, however the failure probability can only be estimated or reduced by understanding the failure mechanism. Ideally this probability shall be lowered to "impossible to occur" by eliminating the (root) causes. It is therefore important to include in the FMEA an appropriate depth of information on the causes of failure (deductive analysis).

The FMEA is a design tool used to systematically analyze postulated component failures and identify the resultant effects on system operations. The analysis is sometimes characterized as consisting of two sub-analyses, the first being the failure modes and effects analysis (FMEA), and the second, the criticality analysis . Successful development of an FMEA requires that the analyst include all significant failure modes for each contributing element or part in the system.

FMEAs can be performed at the system, subsystem, assembly, subassembly or part level. The FMECA should be a living document during development of a hardware design. It should be scheduled and completed concurrently with the design. If completed in a timely manner, the FMECA can help guide design decisions. The usefulness of the FMECA as a design tool and in the decision-making process is dependent on the effectiveness and timeliness with which design problems are identified. Timeliness is probably the most important consideration. In the extreme case, the FMECA would be of little value to the design decision process if the analysis is performed after the

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 1, January 2016

hardware is built. While the FMECA identifies all part failure modes, its primary benefit is the early identification of all critical and catastrophic subsystem or system failure modes so they can be eliminated or minimized through design modification at the earliest point in the development effort; therefore, the FMECA should be performed at the system level as soon as preliminary design information is available and extended to the lower levels as the detail design progresses.

1.2. Functional analysis

The analysis may be performed at the functional level until the design has matured sufficiently to identify specific hardware that will perform the functions; then the analysis should be extended to the hardware level. When performing the hardware level FMECA, interfacing hardware is considered to be operating within specification. In addition, each part failure postulated is considered to be the only failure in the system. In addition to the FMEAs done on systems to evaluate the impact lower level failures have on system operation, several other FMEAs are done. Special attention is paid to interfaces between systems and in fact at all functional interfaces. The purpose of these FMEAs is to assure that irreversible physical and/or functional damage is not propagated across the interface as a result of failures in one of the interfacing units. These analyses are done to the piece part level for the circuits that directly interface with the other units. The FMEA can be accomplished without a CA, but a CA requires that the FMEA has previously identified system level critical failures. When both steps are done, the total process is called a FMECA.

1.3. Ground rules

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. The ground rules also describe the indenture level of the analysis, the basic hardware status, and the criteria for system and mission success. 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

1.4.Benefits

- ✓ 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.[11]
- ✓ 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.

1.5.FMEA

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 FMECA.[11]In addition, the FMECA procedures are straightforward and allow orderly evaluation of the design.

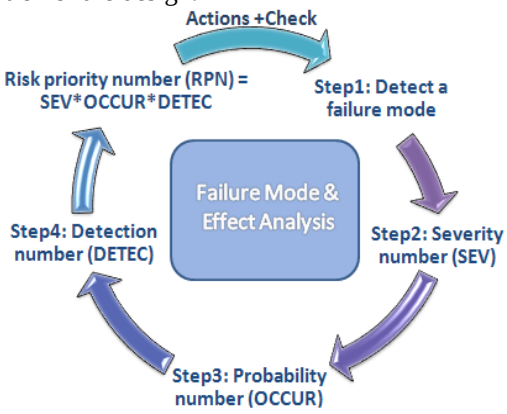

FIG:-1 FMEA Design

2.1 Failure mode

The specific manner or way by whic h a failure occurs in terms of failure of the item function under investigation; it may generally describe the way the failure occurs. It shall at least clearly describe a failure state of the item under consideration. It is the result of the failure mechanism cause of the failure mode.

2.2.Failure cause and/or mechanism

Defects in requirements, design, process, quality control, handling or part application, which are the underlying cause or sequence of causes that initiate a process that leads to a failure mode over a certain time. A failure mode may have more causes. "corrosion of a structural beam" or "fretting corrosion in an electrical contact" is a failure mechanism and in itself not a failure mode. The related failure mode is a "full fracture of structural beam" or "an open electrical contact". The initial cause might have been "Improper application of corrosion protection layer.

2.3.Failure effect

Immediate consequences of a failure on operation, function or functionality, or status of some item. An identifier for system level and thereby item complexity. Complexity increases as levels are closer to one. The

failure effect as it applies to the item under analysis. The failure effect as it applies at the next higher indenture level. The failure effect at the highest indenture level or total system. The means of detection of the failure mode by maintainer, operator or built in detection system, including estimated dormancy period.

Risk Priority Number (RPN) Severity (of the event)

* Probability (of the event occurring)
* Detection (Probability that the event would not be detected before the user was aware of it).[2]

2.4.Probability

It is necessary to look at the cause of a failure mode and the likelihood of occurrence. This can be done by analysis, calculations / FEM, looking at similar items or processes and the failure modes that have been documented for them in the past. A failure cause is looked upon as a design weakness. All the potential causes for a failure mode should be identified and documented. This should be in technical terms. Examples of causes are: Human errors in handling, Manufacturing induced faults, Fatigue, Creep, Abrasive wear, erroneous algorithms, excessive voltage or improper operating conditions or use (depending on the used ground rules). A failure mode is given a Probability Ranking.

Determine the Severity for the worst-case scenario adverse end effect (state). It is convenient to write these effects down in terms of what the user might see or experience in terms of functional failures. Examples of these end effects are: full loss of function x, degraded performance, functions in reversed mode, too late functioning, erratic functioning, etc. Each end effect is given a Severity number based on cost and/or loss of life or quality of life. These numbers prioritize the failure modes (together with probability and detectability). Below a typical classification is given.[12] Other classifications are possible. See also hazard analysis.

The means or method by which a failure is detected, isolated by operator and/or maintainer and the time it may take. This is important for maintainability control and it is especially important for multiple failure scenarios. This may involve dormant failure modes. It should be made clear how the failure mode or cause can be discovered by an operator under normal system operation or if it can be discovered by the maintenance crew by some diagnostic action or automatic built in system test. A dormancy and/or latency period may be entered.

2.5.Detection

The means or method by which a failure is detected, isolated by operator and/or maintainer and the time it may take. This is important for maintainability control (Availability of the system) and it is especially important for multiple failure scenarios. This may involve dormant failure modes (e.g. No direct system effect, while a redundant system / item automatic takes over or when the failure only is problematic during specific mission or system states) or latent failures (e.g. deterioration failure mechanisms, like a metal growing crack, but not a critical length). It should be made clear how the failure mode or cause can be discovered by an operator under normal system operation or if it can be discovered by the maintenance crew by some diagnostic action or automatic built in system test. A dormancy and/or latency period may be entered.

2.6.Indication

If the undetected failure allows the system to remain in a safe working state, a second failure situation should be explored to determine whether or not an indication will be evident to all operators and what corrective action they may or should take. Indications to the operator should be described as follows: Normal. An indication that is evident to an operator when the system or equipment is operating normally. Abnormal. An indication that is evident to an operator when the system has malfunctioned or failed. Incorrect. An e rroneous indication to an operator due to the malfunction or failure of an indicator .

3.LIMITATIONS

While FMEA identifies important hazards in a system, its results may not be comprehensive and the approach has limitations. In the healthcare context, FMEA and other risk assessment methods, including SWIFT (Structured What If Technique) and retrospective approaches, have been found to have limited validity when used in isolation. Challenges around scoping and organisational boundaries appear to be a major factor in this lack of validity. [3]

If used as a top-down tool, FMEA may only identify major failure modes in a system. Fault tree analysis (FTA) is better suited for "top-down" analysis. When used as a "bottom-up" tool FMEA can augment or complement FTA and identify many more causes and failure modes resulting in top-level symptoms. It is not able to discover complex failure modes involving multiple failures within a subsystem, or to report expected failure intervals of particular failure modes up to the upper level subsystem or system.

Additionally, the multiplication of the severity, occurrence and detection rankings may result in rank reversals, where a less serious failure mode receives a higher RPN than a more serious failure mode. The reason for this is that the rankings are ordinal scale numbers, and multiplication is not defined for ordinal numbers.

3.1.Types Functional

Functional design solutions are provided functions can be evaluated on potential functional failure effects. General Mitigations can be proposed to limit consequence of functional failures or limit the probability of occurrence in this early development. It is based on a functional breakdown of a system. This type may also be used for Software evaluation.

3.2.Concept Design / Hardware:

Analysis of systems or subsystems in the early design concept stages to analysis the failure mechanisms and lower level functional failures, specially to different concept solutions in more detail.

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 1, January 2016

3.3.Detailed Design / Hardware:

Analysis of products prior to production. These are the most detailed FMEAs and used to identify any possible hardware failure mode up to the lowest part level. It should be based on hardware breakdown . Any Failure effect Severity, failure Prevention (Mitigation), Failure Detection and Diagnostics may be fully analysed in this FMEA. Process analysis of manufacturing and assembly processes. Both quality and reliability may be affected from process faults. The input for this FMEA is amongst others a work process / task Breakdown .

3.4.Failure Mode, Effects and Criticality Analysis

Not being able to identify your design flaws, failures in manufacturing or processes could result in costly repairs, warranty costs, production delays, catastrophic failures, and even loss of life.Organizations perform Root Cause Analysis to identify and eliminate severe malfunction and potential failures from products and production processes.[11] An inductive approach or procedure often serves as a design aid to identify and prevent catastrophic failures. The need to determine the effect of system and equipment failure becomes more evident and urgent.FMECA (Failure Mode, Effects, and Criticality Analysis) analyzes potential failure within a system, identifies the potential hazards associated with these failures, and classifies them according to their severity. FMECA addresses reliability and quality problems associated with design, manufacturing, process, safety, and environment.

4.TYPES OF FMEA'S

There are several types of FMEAs, some are used much more often than others. FMEAs should always be done whenever failures would mean potential harm or injury to the user of the end item being designed.

The types of FMEA are:

- ✓ System - focuses on global system functions
- ✓ Design - focuses on components and subsystems
- ✓ Process - focuses on manufacturing and assembly processes
- Service - focuses on service functions
- Software - focuses on software functions

5.TOOLS SUPPORT FOR FEMA

Failure Modes and Effects Analysis (FMEA) is a systematic, proactive method for evaluating a process to identify where and how it might fail and to assess the relative impact of different failures, in order to identify the parts of the process that are most in need of change.

FMEA includes review of the following:

- ✓ Steps in the process
- ✓ Failure modes (What could go wrong?)
- ✓ Failure causes (Why would the failure happen?)
- ✓ Failure effects (What would be the consequences of each failure?)

Teams use FMEA to evaluate processes for possible failures and to prevent them by correcting the processes proactively rather than reacting to adverse events after failures have occurred. This emphasis on prevention may reduce risk of harm to both patients and staff. FMEA is particularly useful in evaluating a new process prior to implementation and in assessing the impact of a proposed change to an existing process. potential failure modes and effects analysis; failure modes, effects and criticality analysis (FMECA).

Failure modes and effects analysis (FMEA) is a step-by-step approach for identifying all possible failures in a design, a manufacturing or assembly process, or a product or service.

“Failure modes” means the ways, or modes, in which something might fail. Failures are any errors or defects, especially ones that affect the customer, and can be potential or actual. “Effects analysis” refers to studying the consequences of those failures.

Failures are prioritized according to how serious their consequences are, how frequently they occur and how easily they can be detected. The purpose of the FMEA is to take actions to eliminate or reduce failures, starting with the highest-priority ones.[4]

Failure modes and effects analysis also documents current knowledge and actions about the risks of failures, for use in continuous improvement. FMEA is used during design to prevent failures. Later it’s used for control, before and during ongoing operation of the process. Ideally, FMEA begins during the earliest conceptual stages of design and continues throughout the life of the product or service. Begun in the 1940s by the U.S. military, FMEA was further developed by the aerospace and automotive industries. Several industries maintain formal FMEA standards. What follows is an overview and reference. Before undertaking an FMEA process, learn more about standards and specific methods in your organization and industry through other references and training.

When to Use FMEA When a process, product or service is being designed or redesigned, after quality function deployment.[9]

Periodically throughout the life of the process, product or service FMEA Procedure (Again, this is a general procedure. Specific details may vary with standards of your organization or industry.) Assemble a cross-functional team of people with diverse knowledge about the process, product or service and customer needs. Functions often included are: design, manufacturing, quality, testing, reliability, maintenance, purchasing (and suppliers), sales, marketing (and customers) and customer service.

Identify the scope of the FMEA. Is it for concept, system, design, process or service? What are the boundaries? How detailed should we be? Use flowcharts to identify the scope and to make sure every team member understands it in detail. (From here on, we’ll use the word “scope” to mean the system, design, process or service that is the subject of your FMEA.) Identify the functions of your scope. Ask, “What is the purpose of this system, design, process or service? What do our customers expect it to do?”

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 1, January 2016

Name it with a verb followed by a noun. Usually you will break the scope into separate subsystems, items, parts, assemblies or process steps and identify the function of each. For each function, identify all the ways failure could happen. These are potential failure modes. If necessary, go back and rewrite the function with more detail to be sure the failure modes show a loss of that function. For each failure mode, identify all the consequences on the system, related systems, process, related processes, product, service, customer or regulations.[10] These are potential effects of failure. Ask, "What does the customer experience because of this failure? [8]What happens when this failure occurs?"

Determine how serious each effect is. This is the severity rating, or S. Severity is usually rated on a scale from 1 to 10, where 1 is insignificant and 10 is catastrophic. If a failure mode has more than one effect, write on the FMEA table only the highest severity rating for that failure mode. For each failure mode, determine all the potential root causes. Use tools classified as

5.1.Cause Analysis Tool:

As well as the best knowledge and experience of the team. List all possible causes for each failure mode on the FMEA form. For each cause, determine the occurrence rating, or O. This rating estimates the probability of failure occurring for that reason during the lifetime of your scope. Occurrence is usually rated on a scale from 1 to 10, where 1 is extremely unlikely and 10 is inevitable. On the FMEA table, list the occurrence rating for each cause. For each cause, identify current process controls. These are tests, procedures or mechanisms that you now have in place to keep failures from reaching the customer. These controls might prevent the cause from happening, reduce the likelihood that it will happen or detect failure after the cause has already happened but before the customer is affected. For each control, determine the detection rating, or D. This rating estimates how well the controls can detect either the cause or its failure mode after they have happened but before the customer is affected. Detection is usually rated on a scale from 1 to 10, where 1 means the control is absolutely certain to detect the problem and 10 means the control is certain not to detect the problem (or no control exists).

On the FMEA table, list the detection rating for each cause. (Optional for most industries) Is this failure mode associated with a critical characteristic? (Critical characteristics are measurements or indicators that reflect safety or compliance with government regulations and need special controls.) If so, a column labeled Classification" receives a Y or N to show whether special controls are needed. Usually, critical characteristics have a severity of 9 or 10 and occurrence and detection ratings above[3].

Calculate the risk priority number, or RPN, which equals S × O × D. Also calculate Criticality by multiplying severity by occurrence, S × O. These numbers provide guidance for ranking potential failures in the order they should be addressed.

Identify recommended actions. These actions may be design or process changes to lower severity or occurrence. They may be additional controls to improve detection. Also note who is responsible for the actions and target completion dates. As actions are completed, note results and the date on the FMEA form. Also, note new S, O or D ratings and new RPNs.

6.CONCLUSION

Typically, failure modes and effects analysis (FMEA) is used in addressing the failures and mitigating interventions for hardware systems. It is unclear how FMEA could be used to analyze software systems.[9] This can be attributed to the difference in the way software and hardware fail and also since FMEA was developed to analyzing hardware failure. This paper has investigated the possibility of using FMEA in the failure analysis of software systems .[7] In both software and hardware systems, failure analysis should begin from the infancy stage of design through to completion. Therefore this paper demonstrated the use of FMEA in analyzing software system at the top level software architecture - use case diagram. The paper then establishes and proposes a failure analysis model for software architecture.

REFERENCES

[1] N. Storey, Safety-Critical Computer Systems, Addison Wesley Longman , London (1996)
[2] P. Haapanen, and A. Helminen, "Failure mode and Effects Analysis of Software-based AutomationSystems", (2011) July 3.
[3] N. Leveson, "A New Accident Model for Engineering Safer Systems", Safety Science (2004) Vol. 42, No. 4, pp. 237-270
[4] G. Cassanelli, G. Mura, F. Fantini, M. Vanzi, and B. Plano, "Failure Analysis-assisted FMEA", Microelectronics and Reliability, Vol. 46, Issues 9-11 (2006) pp. 1795-1799
[5] V. Ebrahimipour, K. Rezaie, and S. Shokravi, "An Ontology Approach to Support FMEA Studies", Expert Systems with Applications, Vol. 37, Issue 1 (2010) pp. 671-677
[6] R.S. Pressman, Software Engineering: A Practitioner's Approach, 5th Ed, McGraw-Hill Series in Computer Science, New York (2001)
[7] P. Sinha, "Architectural Design and Reliability Analysis of a Fail-Operational Brake-by-Wire System from ISO 26262 Perspectives", Reliability Engineering & System Safety, Vol. 96, Issue 10 (2011) pp. 1349-1359
[8] H.T. Dorissen, K. Dürkopp, "Mechatronics and Drive-by-Wire Systems Advanced Non-contacting Position Sensors", Control Engineering Practice, ol. 11, Issue 2 (2003) pp. 191-197
[9] C. Wilwert, N. Navet, Y.-Q. Song, and F. Simonot-Lion, "Design of automotive X-by-Wire systems," FL: CRC (2004)
[10] IDRA, ISO 26262 The merging Automotive Safety Standard [online], Available: (2011) October 21, SiliconIndia Website.
[11] N.G. Leveson, System Safety Engineering: Back to the Future, Aeronautics and Astronautics, Massachusetts Institute of Technology (2002)
[12] Antonio pecchia, Marcello cinque, Domenico cotroneo "Event log for the analysis of software failures a rule-based approach",June-2013.