A Unified Approach to Failure Mode, Effects and Criticality Analysis (FMECA)

Benjamin C. Wei; Manager, Nuclear Energy Standards; Washington DC

Key Words: Failure mode, Criticality analysis, FMECA

Abstract

The failure mode, effects, and criticality analysis (FMECA) is an essential function in design from concept through development. To be effective, the FMECA must be iterative to correspond with the nature of the design process itself. The information derived from a FMECA should have a major influence on the technical and economic viability of any major engineering projects by detailing where design changes or other corrective actions can lead to minimal downtime, the elimination of human hazards, and an improvement in system reliability and safety.

The purpose of a FMECA is to provide a systematic, critical examination of potential failure modes of plants and equipment and their causes, to assess the safety of various systems or components, to analyze the effect of each failure mode on system operation, and to identify corrective action, i.e., design modifications. For an effective FMECA, the reporting must be thorough and accurate and must show results that can be interpreted easily by the top management to assist them in decision making processes.

The usefulness of the FMECA as a design tool is dependent upon the effectiveness with which problem information is communicated for early design attention. FMECA should therefore be initiated as soon as preliminary design information is available at the higher system levels and extended to the lower levels as more information

becomes available on the items in question.

The FMECA is not only an essential task for reliability, it is also useful in maintainability, in maintenance plan analysis, and for failure detection and subsystem design.

This paper presents a unified approach in performing FMECA applicable to large plant design. This procedure will assist the project contractors in performing a FMECA, and will aid the Owner organization in evaluating FMECA results and corrective actions.

Introduction

FMECA is an analysis procedure which:

- Documents all probable failures in a system within specified ground rules.
- Determines by failure mode analysis the effect of each failure on system operation.
- Identifies single failure points.
- Ranks each failure in accordance to a severity classification of failure effect.

Prior to conducting a FMECA, ground rules applicable to the analysis should be defined. The following are examples of areas to be considered when defining ground rules for a FMECA:

1. Determine to which indenture level the FMECA will be conducted.

Introduction (cont'd)

2. Define the operational temperature range within which the equipment is expected to operate.
3. Define environmental conditions that will or will not be considered in the analysis: e.g., tornadoes, earthquakes, sand storms, etc.
4. State whether structural failures will be considered in the analysis.
5. Define what constitutes successful operation.
6. Define what constitutes a performance failure.
7. State whether redundant items are to be considered critical.
8. Indicate whether electrical cables and/or piping will be analyzed as part of the system with which they are most closely associated or whether they will be identified and evaluated as separate subsystems.

Figure 1 illustrates the logic for performing an FMECA.

FMECA Planning

The FMECA process shall be initiated as an integral part of early design process. Further, it should be updated to reflect design changes as FMECA is a major consideration at Design Review.

The following items shall be considered in FMECA planning:

- Worksheet formats
- Ground rules
- Analysis assumptions
- Identification of lowest indenture level
- Coding
- System description
- Failure definitions
- Identification of FMECA integration by contractor's reliability organization

Performing FMECA

The following delineates the steps to perform FMECA:

1. Determine the Functional Level Breakdown Structure (FLBS). - Identification of largest item, i.e., a plant and then its subdivisions into equipment, assemblies, subassemblies, and parts.
2. Use a consistent coding system that uniquely identify the item and reflect its association with items at higher and lower levels.
3. Construct Functional Block Diagrams (FBD). - Functional and reliability block diagrams illustrating operation, interrelationships, and interdependencies of functional entities.
4. Identify all potential item and interface failure modes, and define their effect on the mission to be performed.
5. Evaluate each failure mode in terms of the worst potential consequences as categorized by the Severity of Failure.
6. Establish criticality factor used to rank failure modes for corrective action. It is the product of Probability of Failure Occurrence and the Category of Severity of Failure.

7. Identify corrective design required to eliminate the failure or control the risk.

8. Identify effects of corrective actions.

9. Document analysis and summarize problems which could not be corrected by design.

Figure 2 illustrates a Functional Level Breakdown Structure for a coal gasification power generating plant. Figure 3 shows the Functional Block Diagram for system 2.0 of the coal gasification plant. Figure 4 gives an example of a worksheet for Failure Mode and Effects Analysis.

Performing FMECA (cont'd)

Severity Classification

Four categories of severity classifications are assigned to provide a qualitative measure of worst potential consequences resulting from design error or item failure.

1. Category I - Catastrophic
 - Loss of Life
 - Severe reduction of item's functional output
 - Higher indenture level item failure
 - Subcategory 1R - Redundant hardware failure
2. Category II - Critical
 - Personal injury
 - Severe reduction in functional output of item
 - Subcategory 2R - Redundant hardware failure that cannot be repaired by routine maintenance personnel
3. Category III - Minor
 - Minimal effect on item's functional output
 - Higher indenture level failure that can be repaired by maintenance personnel within a short period of time
4. Category IV - Insignificant
 - Negligible effect on item's functional output
 - Higher indenture level degradation that can be repaired by minor maintenance

Probability of Occurrence

The levels of probability of occurrence are defined as follows:

- Level A - Frequent. A high probability of occurrence during the item operating time interval. Defined as a single failure mode probability > 0.20 .

- Level B - Reasonably probable. A moderate probability of occurrence during the item operating time interval. Defined as a single failure mode probability > 0.10 but < 0.20 .
- Level C - Occasional. An occasional probability of occurrence during item operating time interval. Defined as single failure mode probability > 0.01 but < 0.10 .
- Level D - Remote. An unlikely probability of occurrence during item operating time interval. Defined as single failure mode probability $> .001$ but less than $< .01$.
- Level E - Extremely Unlikely. A failure whose probability of occurrence is essentially zero during item operating time interval. Defined as a single failure mode probability < 0.001 .

Figure 5 illustrates an example of the criticality matrix.

Criticality Number Calculation Method

Criticality analysis is the method used for quantifying and evaluating the probability of occurrence of item failure modes and resultant system failure effects. Criticality numbers are normally calculated for only those components and subsystems whose failures would result in significant adverse failure effects on systems' capability, safety, environment, cost, schedule, or other significant parameters.

The following equation can be used to calculate the criticality number (C_n) for one failure mode and effect for a single component:

Performing FMECA (cont'd.)

$$C_{\lambda} = K_A K_E \alpha \beta \lambda t \cdot 10^6$$

In which

K_A = operational factor adjusting the failure rate (λ) for the difference between operating stresses from item analysis vs. those from measurement.

K_E = environmental factor adjusting λ for the difference between the environmental stresses from analysis vs. those from measurement.

t = required or planned operating time period in hours or in number of operating cycles of the item

α = item failure mode ratio which is that portion of the items failure rate, λ , attributable to the specific failure mode being considered.

β = the probability that a specific failure effect will occur provided the particular failure mode being considered has occurred. Value for β will range from a maximum of 1.00 down to 0.10 or less.

λ = failure rate of the item expressed in failures per hour or failures per cycle. (Frequently expressed as failures per 10^6 hours).

FMECA Report

A FMECA report shall be written that identifies the level of analysis, summarizes the results, reports the data sources and techniques used in performing the analysis, and includes the system definition narrative, resultant analysis data and worksheets.

In the Summary Section, it should include: design evaluation summary of major problems, rationale for excluding items in FMEA analysis, and conclusions and recommended actions for elimination or reduction of failure risks.

A reliability critical item list shall also be included that provide information on:

- Item identification and FMEA cross-reference
- Description of design features minimizing occurrence of failure
- Description of tests verifying design features and tests planned during operations that would detect failure mode occurrence
- Description of planned inspections to ensure hardware being built to design requirements
- A statement relating to history of this particular design
- Description of the method(s) by which the occurrence of the failure mode is detected by the operator
- Rationale for not eliminating the related failure mode(s)
- Category 1, 1R and Category 2, 2R failure mode list
- Single failure points list, including criticality classification for each failure point

Performing FMECA (cont'd)

Application Criteria

In general, the application of FMECA shall consider system complexity, funding, and schedule on the level of detail and timing of the FMECA.

The level of detail applies to level of indenture at which failures are postulated. The choice of level of indenture is to be compatible with program cost, scheduler constraints, and system safety and reliability requirements. FMECA should not be performed below the level necessary to identify critical items.

The objective of FMECA is to support decision making process. If late, it has made no contribution and is untimely. Hence, time-phasing of FMECA effort is to be identified in FMECA plan to assure availability of analysis results to support project decision. FMECA serves to verify design integrity, quantify sources of undesirable failure modes, and document reliability risks. FMECA results can also be used for maintenance planning analysis, safety and hazards analyses, and for fault detection and isolation design.

Summary

The FMECA procedure presented has established the steps necessary to perform a Failure Mode, Effects and Criticality Analysis on any item at any level. Specifically, this procedure:

- Provides a technique for performing a thorough analysis that can identify engineering problem areas and failure modes at specific plant levels, and contribute to the validity of design review process.
- Provides formats for documenting plant/equipment operating characteristics so

that failure modes can readily be identified with a functional characteristic.

- Provides an analytical technique that can identify necessary corrective action, with which top management can make critical decisions. The end product shall be the reduction or elimination of plant and personnel hazards resulting in improvement of plant safety, as well as the improvement of efficiency and effectiveness, resulting in reduction of life-cycle costs.

References

1. MIL-STD-785, "Reliability Program for Systems and Equipment Development and Production."
2. MIL-STD-882, "System Safety Program Requirements."
3. MIL-STD-1629A, "Procedures for Performing a Failure Mode, Effects and Criticality Analysis."
4. MIL-HDBK-217, "Reliability Prediction of Electronic Equipment."
5. J. R. Lance, G. A. Mutone, and E. F. Bjoro, "Safety Analysis of an Advanced Energy System Facility," 1980 Proc. AR&MS.

Appendix

Definitions

1. Corrective action. A documented design, process, procedure, or materials change implemented and validated to correct the cause of failure or design deficiency.
2. Common Mode Failure (CMF)/Common Cause Failure (CCF) Analysis. A technique applied to identify a single cause that can result in multiple cause-dependent failures that negate the benefits of redundant or diverse components or systems.

Appendix (cont'd)

3. Compensating provision.

Actions that are available or can be taken by an operator to negate or mitigate the effect of a failure on a system.

4. Criticality. A relative measure of the consequences of a failure mode and its frequency of occurrences.

5. Criticality analysis (CA). A procedure by which each potential failure mode is ranked according to the combined influence of severity and probability of occurrence.

6. Severity. The consequences of a failure mode. Severity considers the worst potential consequence of a failure, determined by the degree of system damage, property damage, or injury that could ultimately occur.

7. Detection mechanism. The means or methods by which a failure can be discovered by an operator under normal system operation or can be discovered by the maintenance crew by some diagnostic action.

8. Environments. The conditions, circumstances, influences, stresses and combinations thereof, surrounding and affecting systems or equipment during storage, handling, transportation, testing, installation, and use in standby status and mission operation.

9. External Events. External events are events that occur external to a system and that may cause the failure of one or more systems (external events are sometimes also called major common cause initiating events). Typical examples of external events are fires, floods, earthquakes, extreme winds.

10. Failure cause. The physical or chemical processes, design defects, quality defects, part mis-application, or other processes which are the basic reason for failure or which initiate the physical process by which deterioration proceeds to failure.

11. Failure effect. The consequence(s) a failure mode has on the operation, function, or status of an item. Failure effects are classified as local effect, next higher level, and end effect.

12. Local effect. The consequence(s) a failure mode has on the operation, function, or status of the specific item being analyzed.

13. Next higher level effect. The consequence(s) a failure mode has on the operation, functions, or status of the items in the next higher indenture level above the indenture level under consideration.

14. End effect. The consequence(s) a failure mode has on the operation, function, or status of the highest indenture level.

15. Failure mode. The manner by which a failure is observed. Generally describes the way the failure occurs and its impact on equipment operation.

16. Failure mode and effects analysis (FMEA). 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.

17. FMECA-Maintainability information. A procedure by which each potential failure is analyzed to determine how the failure is detected and the actions to be taken to repair the failure.

18. Indenture levels. The item levels which identify or describe relative complexity of assembly or function. The levels progress from the more complex (system) to the simpler (part) divisions.

19. Initial indenture level. The level of the total, overall item which is the subject of the FMECA.

20. Other indenture levels. The succeeding indenture levels (second, third, fourth, etc.) which represent an orderly progression to the simpler division of the item.

Appendix (cont'd)

21. Interfaces. The systems, external to the system being analyzed and commonly called support systems, which provide a common boundary or service and are necessary for the system to perform its function in an undegraded mode. For example, systems that supply power, cooling, heating, air services, or input signals are typical support systems.

22. Redundancy. The existence of more than one means for accomplishing a given task, where all means must fail before there is an overall failure to the system.

23. Redundancy, active. That redundancy wherein all redundant items are operating simultaneously rather than being switched on when needed.

24. Redundancy, parallel. The existence of two systems working at the same time to accomplish the task, where either system can handle the job itself in case the other system fails.

25. Redundancy, standby. That redundancy wherein the alternative means of performing the function is inoperative until needed and is switched on upon failure of the primary means of performing the function.

26. Redundancy, diverse. That redundancy wherein the alternative means of performing the function are not dependent on the same support systems and who accomplish their function by different means (e.g., an ac motor-driven pump and a steam turbine driven pump independent of ac).

27. Single failure point. The failure of an item which would result in failure of the system and is not compensated for by redundancy or alternative operational procedure.

28. Undetectable failure. A postulated failure mode in the FMEA for which there is no failure detection method by which the operator is made aware of the failure.

Biographies

Benjamin C. Wei, Ph.D., PE
U. S. Department of Energy
NE-46, Washington, DC 20545 USA

Benjamin C. Wei is Manager, Nuclear Energy Standards, and is also associated with quality assurance and reliability of reactor plants in the Office of Nuclear Safety Self-Assessment. He has been with the Department of Energy since 1970, engaged in design, safety, and reliability, and R&D project management of advanced LMR reactor components. In 1967-1970, he was consulting engineer, Solid Mechanics Laboratory, General Electric co. He taught physics and advanced mechanics at the New Jersey Institute of Technology in 1961-1967. His Ph.D. is in Theoretical and Applied Mechanics from the University of Illinois.

He is a member of the ASME Code committee on elevated temperature design. He has published 25 technical papers in various engineering societies, and served as Associate Editor of ASME Journal of Pressure Vessel Technology for six years. He is a Registered Professional Engineer in New Jersey and New York.

FIGURE 1. LOGIC FOR PERFORMING AN FMECA

FIGURE 2. FUNCTIONAL LEVEL BREAKDOWN STRUCTURE

FIGURE 3. COAL GASIFICATION PLANT (SYSTEM 2.0)

PAGE _____ OF _____
REV. NO. _____ DATE _____

PROJECT/FACILITY _____
LEVEL _____
DRAWING NO. _____
LEVEL _____
DRAWING NO. _____
LEVEL _____
DRAWING NO. _____

PROBABILITY OF FAILURE
DESCRIPTION
1 - HIGH
2 - MODERATE
3 - LOW
4 - UNLIKELY

SEVERITY OF FAILURE
DESCRIPTION
1 - CATASTROPHIC
2 - CRITICAL
3 - MAJOR
4 - MINOR

COMPANY _____
FMEA ANALYST _____
DATE _____
REVIEWED BY _____

ITEM NO.	ITEM/NAME FUNCTION	S/N	OPERATING PARAMETER(S)	F/N	FAILURE MODE	PROB. OCC.	FAILURE SYMPTOMS/ REASONS	ITEM FAILURE EFFECT	SEVERITY	CRITICAL	END EFFECTS AND CRITICALITY					PROPOSED CORRECTIVE ACTIONS) AND/OR REMARKS	
											SUBSYSTEM	SYSTEM	CRIT.	INTERFACING SYSTEM	CRIT.		
12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29

FIGURE 4. FAILURE MODE AND EFFECTS ANALYSIS WORKSHEET

FIGURE 5. EXAMPLE OF CRITICALITY MATRIX