Subject:	Effective Date:	Initiated by:
Failure Modes and Effects Analysis	**April 20, 1999**	Head, Engineering and Technical Infrastructure
	Supersedes: TOP 22.019 dated 11/1/88	**Approved:** Director

Applicability

This procedure applies to all activities at C and D-Sites of the Laboratory where need for failure modes and effects analysis (FMEA) has been determined. The FMEA shall be performed for the required equipment or levels as defined in project requirements documents, work planning documents, or by management directive. The FMEA shall be documented as part of the projects' system design processes and may be included as part of a project's safety documentation (e.g., Safety Analysis Report, Safety Assessment Document, etc.).

Introduction

This procedure establishes the requirements for the preparation, review, and release of the FMEA. The depth of the analysis, and its documentation, will vary with the system or project under analysis. In situations where failure probability and severity must be determined, the FMEA should be expanded into a Failure Modes, Effects and Criticality Analysis (FMECA). FMECA is also useful in situations where many multiple failures are a concern. However, the analyst should be aware that a statistically significant reliability database is needed to make the probability estimates used in a FMECA. Guidance for performing a FMECA is available in both of the reference documents below.

Reference Documents

IEC Standard 812	Procedure for Failure Mode and Effects Analysis (FMEA)
MIL-STD-1629A	Procedures for Performing a Failure Mode, Effects and Criticality Analysis

Responsibility	Action
Responsible Line Manager	1. Assigns individual to perform FMEA (analyst) and another individual to review it (reviewer). The reviewer shall by qualified by having like or greater expertise and technical experience as the analyst.
Analyst	2 Describes system under analysis and either prepares system diagrams or uses existing documentation to depict all major components and their performance criteria. The level of assembly will vary with the level of the analysis.
	3. Performs FMEA using the guidance of Attachment 1.
	4. Documents results using the guidance of Attachment 2.
	5. Signs FMEA and provides it to the reviewer.

Reviewer	6. Reviews FMEA for technical content and signs if no significant problems are identified. Otherwise discusses the FMEA with the analyst.
Analyst	7. Files FMEA in the Operations Center.

Attachments:

1. Guidance on the Performance of a FMEA
2. Guidelines for Documenting an FMEA.
3. FMEA Documentation Example

Purpose

This attachment describes the standard steps involved in performing an FMEA.

Performing the FMEA

The basic steps for an FMEA are:

1) Define the system and its functional and operating requirements;

   1.1 Include primary and secondary functions, expected performance, system constraints, and explicit conditions that constitute a failure. The system definition should also define each mode of operation and its duration.

   1.2 Address any relevant environmental factors such as temperature, humidity, radiation, vibration, and pressure during operating and idle periods.

   1.3 Consider failures that could lead to noncompliance with applicable regulatory requirements. For example, a failure that could result in a release that exceeds environmental permit limits.

2) Develop functional block diagrams showing the relationships among the elements and any interdependencies. Separate diagrams may be required for each operational mode. As a minimum, the block diagram should contain:

   2.1 a breakdown of the system into major subsystems including functional relationships;

   2.2 appropriately and consistently labeled inputs and outputs and subsystem identification;

   2.3 any redundancies, alternative signal paths, and other engineering features that provide "failsafe" measures.

   Existing drawings developed for other purposes may be used for the FMEA if the above elements are adequately described.

3) Identify failure modes, their cause and effects.

   3.1 IEC 812 1985 provides a list of failure modes, reproduced here as Table I, to describe the failure of any system element.

   3.2 Identify the possible causes associated with each postulated failure mode. The list in Table I can be used to define both failure modes and failure causes. Thus, for example, a power supply may have a specific failure mode "loss of output" (29), and a failure cause "open (electrical)" (31).

   3.3 Identify, evaluate, and record the consequences of each assumed failure mode on system element operation, function, or status. Consider maintenance, personnel, and system objectives as well as any effect on the next higher system level.

4) Identify failure detection and isolation provisions and methods. Determine if other failure modes would give an identical indication and whether separate detection methods are needed.

5) Identify design and operating provisions that prevent or reduce the effect of the failure mode. These may include:

   5.1 redundant items that allow continued operation if one or more elements fail;

   5.2 alternative means of operation;

   5.3 monitoring or alarm devices;

   5.4 any other means permitting effective operation or limiting damage.

6) Identify specific combinations of multiple failures to be considered. The more multiple failures considered, the more complex the FMEA becomes. In many such cases it would be advantageous to perform a FMECA using the guidance of IEC Standard 812 or MIL-STD-1629A. Using the FMECA, the severity of failure effects are categorized, the probability is determined, and the number of redundant mitigating features needed to keep probability of failure acceptably low are better determined.

7) Revise or repeat, as appropriate, the FMEA as the design changes. Changes may be in direct response to the results of the previous FMEA or may be due to unrelated factors.

TABLE I Generic Failure Modes (IEC 812-1985)

1 Structural failure (rupture)	17 Restricted flow
2 Physical binding or jamming	18 False actuation
3 Vibration	19 Fails to stop
4 Fails to remain (in position)	20 Fails to start
5 Fails to open	21 Fails to switch
6 Fails to close	22 Premature operation
7 Fails open	l23 Delayed operation
8 Fails closed	24 Erroneous input (increased)
9 Internal leakage	25 Erroneous input (decreased)_
10 External leakage	26 Erroneous output (increased)
11 Fails out of tolerance (high)	27 Erroneous output (decreased)
12 Fails out of tolerance (low)	28 Loss of input
13 Inadvertent operation	29 Loss of output
14 Intermittent operation	30 Shorted (electrical)
15 Erratic operation	31 Open (electrical)
16 Erroneous indication	32 Leakage (electrical)
33 Other unique failure conditions as applicable to the system characteristics, requirements and operational constraints	

DOCUMENTING THE FMEA

The following information is required to be documented for an FMEA. The headings below presume use of the sample form shown on the next page: Complex systems may need more extensive descriptions preceding the tabular portion of the FMEA.

1) Heading
Identify the system, subsystem or assembly being addressed, the modes of operation, the analyst, and the date. Where appropriate, include or reference a description of the system.

2) Operating Mode
For which of the operating modes is the failure being evaluated?

3) Failure Mode & Cause
Address each failure mode and cause separately unless two or more failures have the same basic cause and produce the same effect on the remainder of the system.

4) System Effect
What would be the effect of the failure on the next higher level of assembly, and if applicable, the Project objectives if no mitigating action were taken. Quantitative descriptions of affected performance parameters as well as safety related conditions (fire, toxic smoke, radiation release, etc.) should be noted.

5) Fault Detection/Isolation
How will the failure be detected and when (e.g. during maintenance inspection, real time monitor, etc.)? Detection of related conditions, such as fire, smoke, leakage, etc., should also be indicated
How will the location of failure be determined and how will the specific component that has failed be indicated?

6) Compensating Provisions/Failure Recovery
List any provisions designed into the equipment or system or available externally to circumvent or alleviate the effects of the postulated failure mode. Also, indicate by what method, if any, the failure will be repaired. Particular note should be made of any remote repair expectations.

7) Remarks
Any clarifications, recommendations or justification notes should be here. Recommendations should include design changes or operation restrictions intended to avoid the failure.

Project: _____ **FAILURE MODES AND EFFECTS ANALYSIS** Page: ____ of ____

WBS Element: _____ Performed By: _____ Date: _____

Component: _____ Reviewed By: _____ Date: _____

Function: _____

Operating Mode	Failure Mode/Cause	System Effect	Fault Detection/ Isolation	Compensating Provisions	Remarks

Project: NSTX

FAILURE MODES AND EFFECTS ANALYSIS

WBS Element: 1.2 Vacuum Vessel & Support Structures Performed By: the engineer Date: date

Component: Support Structures Reviewed By: the reviewer Date: date

Function: The coil support structures provide mechanical support for the outer PF coils and outer TF coil legs, and provide dielectric breaks where required (PF5). The vacuum vessel legs support the vacuum vessel and provide dielectric breaks.

Operating Mode	Failure Mode/Cause	System Effect	Fault Detection/ Isolation	Compensating Provisions	Remarks
Bakeout	Physical binding or jamming Failure of sliding joint of umbrella structure	Excessive stress in umbrella and vacuum vessel, possible structural deformations, failure of welds, weakening of structure	Maintenance inspection, magnetic diagnostics	None-Shutdown and repair	This is a simple. passive component unlikely to fail. No known design alternatives identified.
Bakeout	Physical binding or jamming Failure of sliding joint of vacuum vessel leg support	Excessive stress in leg and structure, possible structural deformations, failure of welds, weakening of structure, possible dislocation of vacuum vessel, loss of vacuum integrity	Monitoring of displacement of vacuum vessel. Maintenance inspection,	None-Shutdown and repair	This is a simple. passive component unlikely to fail. At higher cost redundant joints could be developed.
CHI Operations	Structural failure Failure of dielectric joint(s) associated with outer PF coils supports or vacuum vessel leg supports	Fault on CHI power supply, arcing, burning, melting.	Maintenance inspection & test, magnetic diagnostics, power supply system ground and overcurrent fault detection.	None-Shutdown and repair	This is a simple. passive component unlikely to fail. At higher cost redundant joints could be developed.