

<b>PPPL</b>	<b>PRINCETON PLASMA PHYSICS LABORATORY</b>	<b>PROCEDURE</b>	<b>No. ENG-008 Rev 1 page 1 of 3</b>
<b>Subject:</b>  <b>Failure Modes and Effects Analysis</b>	<b>Effective Date:</b>  4/13/18	<b>Initiated by:</b>  Head, Engineering Department	
	<b>Supersedes:</b> R0, dated 4/20/1999	<b>Approved:</b>  Director	

**Management System (Primary):** 03.00 ENGINEERING (ENG)  
**Management System Owner:** Head, Engineering Department  
**Management Process:** 03.04 Engineering Programs and Processes  
**Process Owner:** Head, Engineering Department  
**Sub-Process:** 03.04.03 Engineering and Design Processes  
**Sub-Process Owner:** Head, Engineering Department  
**Subject Matter Expert** Head, Engineering Department; Chief Engineer

### Applicability

This procedure applies to all items and activities where need for failure modes and effects analysis (FMEA) has been determined in the Work Planning form, per ENG-032. In addition, any work involving more than 1 gram of lithium or any amount of finely divided lithium (such as powder) requires a FMEA to be developed ahead of implementation. The FMEA should be included as part of a High Hazard and Accelerator project's safety documentation (e.g., Safety Analysis Report, Safety Assessment Document, etc.) per procedure ESH-025.

### 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 from the external reference documents below.

### Reference Documents

IEC Standard 60812 Procedure for Failure Mode and Effects Analysis (FMEA), 2006  
 MIL-STD-1629A Procedures for Performing a Failure Mode, Effects and Criticality Analysis - retired  
 ENG-032 Work Planning Procedure  
 ESH-025 Operations Hazard Classification Criteria and Safety Certification System

**Responsibility****Action**

- |                      |  |
|----------------------|--|
| Responsible Engineer | 1. Assigns individual to perform FMEA (analyst) and another individual to review it (reviewer). The reviewer shall be 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.  |
| Responsible Engineer | 8. Provides FMEA in design review package and in relevant safety documentation as required.  |

**TRAINING (SECTION REQUIRED FOR ALL PROCEDURES)**

- |                                     |   |
|-------------------------------------|---|
| Head, Engineering                   | 1. Specifies the appropriate training methods and means (below) and obtains concurrence of the Management System Owner and the Management Process Owner.<br><br><b>A. Target Audience:</b> Responsible Engineers<br>Instructor: <u>Head, Engineering Department</u><br>Training Method:<br><u>X</u> Read only<br><br>Frequency:<br><u>X</u> Every time procedure is re-issued, including TCRs |
| Management System Owner or Designee | 2. Notifies the Human Resources Training Office of the training so that they will be aware of the training requirements and be able to provide assistance and guidance in the course development, implementation, tracking, and maintenance.  |

**Records Requirements Specific To This Procedure**

Records Custodians must assure records are maintained as follows:

Record Title	Record Custodian	Location	Retention Time
FMEA Document	Operations Center	Operations Center	See Record Schedule for specific Project Type <i>Reference Admin 17, Cartographic, Aerial Photography, Architectural &amp; Engineering Records (30.c)</i>

**Attachments:**

1. Guidelines for Performance of a FMEA
2. Guidelines for Documenting a FMEA.
3. FMEA Documentation Example

<b>PPPL</b>	<b>PRINCETON PLASMA PHYSICS LABORATORY</b>	<b>PROCEDURE</b>	<b>No. ENG-008 Rev 1 page 1 of 3</b>
<b>Guidelines for Performance of a FMEA</b>			<b>Attachment 1</b>

### 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 60812 (2006) states that the key to evaluation of system performance is the identification of critical system elements. The procedures for identifying failure modes, their causes and effects can be effectively enhanced by the preparation of a list of failure modes anticipated with respect to the following:
    - a) the use of the system;
    - b) the particular system element involved;
    - c) the mode of operation;
    - d) the pertinent operational specifications;
    - e) the time constraints;
    - f) the environmental stresses;
    - g) the operational stresses.
 An example list of general failure modes is given in Table 1. Note that this is an example, only. Different lists would be required for different types of systems.

<b>PPPL</b>	<b>PRINCETON PLASMA PHYSICS LABORATORY</b>	<b>PROCEDURE</b>	<b>No. ENG-008 Rev 1 page 2 of 3</b>
<b>Guidelines for Performance of a FMEA</b>			<b>Attachment 1</b>

- 3.2 The most likely causes for each potential failure mode should be identified and described. Since a failure mode can have more than one cause, the most likely potential independent causes for each failure mode need to be identified and described.

The identification and description of failure causes is not always necessary for all failure modes identified in the analysis. Identification and description of failure causes, as well as suggestions for their mitigation should be done on the basis of the failure effects and their severity. The more severe the effects of failure modes, the more accurately failure causes should be identified and described. Otherwise, the analyst may dedicate unnecessary effort on the identification of failure causes of such failure modes that have no or a very minor effect on system functionality.

Failure causes may be determined from analysis of field failures or failures in test units. When the design is new and without precedent, failure causes may be established by eliciting the opinion of experts.

When the causes of each failure mode are identified the recommended action will be evaluated based on their estimated probability of occurrence and the severity of their effect.

- 3.3 The consequences of each failure mode on system element operation, function, or status need to be identified, evaluated and recorded. Maintenance activities and system objectives should also be considered whenever pertinent. A failure effect may also influence the next level up and ultimately the highest level under analysis. Therefore, at each level, the effect of failures on the level above should be evaluated.
- 4) For each failure mode, determine the way in which the failure is detected and the means by which the user or maintainer is made aware of the failure. Failure detection may be implemented by an automatic feature of the design (built-in-test), establishment of a special checkout procedure before system operation or by inspection during maintenance activities. It may be implemented at start up of the system or continuously during operation or at prescribed intervals. In either case, failure detection and its annunciation should preclude a hazardous operating condition.

Failure modes other than the one being considered which give rise to an identical manifestation should be analyzed and listed. The need for separate detection of failure of redundant elements during operation should be considered.

For a design, FMEA detection considers how likely, when, and where a design deficiency will be identified (by review, by analysis, by simulation, by test, etc.). For a process, FMEA detection considers how likely and where in the process a deficiency can be identified and with which probability, e.g., by operator, by statistical process control, by quality check procedure or by later steps in the process.

Table 1 – Example of a set of general failure modes (IEC 60812)

1	Failure during operation
2	Failure to operate at prescribed time

<b>PPPL</b>	<b>PRINCETON PLASMA PHYSICS LABORATORY</b>	<b>PROCEDURE</b>	<b>No. ENG-008 Rev 1 page 3 of 3</b>
<b>Guidelines for Performance of a FMEA</b>			<b>Attachment 1</b>

3	Failure to cease operation at a prescribed time
4	Premature operation

- 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 60812 (or retired standard 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.

<b>PPPL</b>	<b>PRINCETON PLASMA PHYSICS LABORATORY</b>	<b>PROCEDURE</b>	<b>No. ENG-008 Rev 1 page 1 of 2</b>
<b>Guidelines for Documenting a FMEA</b>			<b>Attachment 2</b>

## 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.

**PPPL**PRINCETON PLASMA  
PHYSICS LABORATORY**PROCEDURE**No. ENG-008 Rev 1  
page 2 of 2**Guidelines for Documenting a FMEA****Attachment 2**

Project: \_\_\_\_\_

**FAILURE MODES AND EFFECTS ANALYSIS**

Page: \_\_\_\_\_ of \_\_\_\_\_

WBS Element: \_\_\_\_\_

Performed By: \_\_\_\_\_ Date: \_\_\_\_\_

Component: \_\_\_\_\_

Reviewed By: \_\_\_\_\_ Date: \_\_\_\_\_

Function: \_\_\_\_\_

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



Project: NSTX

**FAILURE MODES AND EFFECTS ANALYSIS**

Page: 1 of 8

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.