# PROCESS HAZARD ANALYSIS
# FAILURE MODE EFFECTS ANALYSIS (FMEA)

Failure Mode Effects Analyses (FMEAs) evaluate the ways equipment can fail or be improperly operated and the effects these failures can have. In an FMEA, each individual failure is considered as an independent occurrence with no relation to other failures in the system, except for the subsequent effects the original failure may produce. In short, FMEAs identify single failure modes that either directly result in or contribute significantly to an accident.

## Purpose:

FMEAs are conducted to improve the safety of equipment by:

1) Identifying single component, equipment and system failure modes.
2) Determining the potential effects on the equipment, system, or plant associated with each individual failure mode.
3) Generating recommendations for increasing reliability of the component, equipment and/or system.

## Deliverables:

1) Qualitative, systematic reference list of equipment, failure modes and effects.
2) Worst case estimate of consequences resulting from a single failure.
3) Documented analysis.
4) Recommendations for improving safety/reliability of appropriate components.

## Terms:

1) Failure Mode describes how equipment fails (open, closed, on, off, leaks, etc.)
2) Effect is determined by the system's response to equipment failure.

## Procedure:

**1) Defining the Scope:**

- Identify specific items for inclusion
- Determine the level of detail needed
- Identify the boundary conditions under which these items are analyzed
  - Identify equipment or system to be analyzed
  - Establish the physical system boundaries (i.e., connections with other processes, utilities, and/or support systems)
  - Establish the system's analytical boundaries: Initial operating condition of equipment, failure modes, operating consequences, causes, or existing safeguards which will or will not be analyzed
    (I.e., may exclude jet liner crashes or earthquakes as a failure mode. The initial operating condition may be a normally 'open' or 'closed valve.)

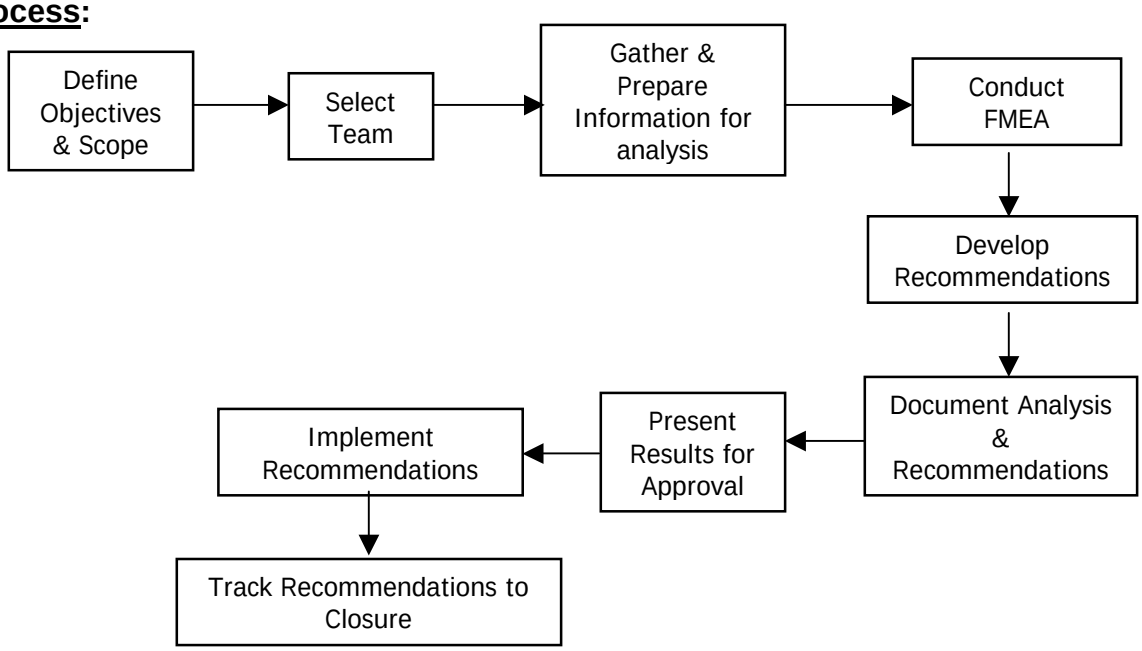
**2) Performing the Review:**

- Prepare for the review:
  - Select team
  - Identify facilitator and record keeper
  - Gather schematics and other information
- Use a deliberate, systematic manner to reduce the possibility of omissions and to enhance the completeness (I.e., consistent format for recording information and results which contribute to consistency and detail needed)
- Evaluate all identified failure modes for each component or system addressed in the FMEA before moving on to the next component.
- Typically, the FEMA format includes:
  - A unique equipment identifier that relates the equipment and components to a system drawing, process, or location. (I.e., component identification numbers from schematics)

- Equipment description including the equipment type, operating configuration, and other service characteristics that may influence the failure modes and their effects. (I.e., motor-operated valve, normally open, in a three-inch sulfuric acid line.)
- Failure modes are listed for each component, which are consistent with the equipment description. Consider all conceivable malfunctions that would alter the equipment's normal operating state.
- For each failure mode, describe both the immediate effects of a failure at the location and the anticipated effects of the failure on other components, equipment, and processes.
- For each identified failure mode, the analyst should describe any safety features or procedures that can reduce the likelihood of a specific failure occurring or mitigate the consequences of a failure.
- Recommended corrective actions for reducing the likelihood of effects associated with the specific failure mode are included in the FMEA.

3) **Document the results:**
   - Systematically and consistently tabulate the effects of equipment failure within a process or system.
   - Equipment identification provides a direct reference between the equipment and system process flow diagrams and schematics.

## Process:




## Example of FMEA Table Format:

| Item No. | Description | Failure Mode | Effect | Safeguards | Actions |
|---|---|---|---|---|---|
| Unique Number for component or equipment | Description/ name of component or equipment | How fails (i.e., fails open or fails closed) | Consequences Local System | Prevention/mitigation measures in place | Actions needed to eliminate, reduce, or mitigate risk of failure |

# Example FMEA

## System: Firewater Supply

| Item No. | Component Description | Failure Mode | Effects | Safeguards | Actions |
|---|---|---|---|---|---|
| 1 | Pump suction piping and screen | Plugged | No water supply to firewater pump | Redundant pump<br>Periodic testing | |
| | | Broken | Debris sucked into pump | Redundant pump<br>Periodic testing | Inspect pump suction strainer periodically |
| 2 | Firewater pump/driver | External rupture | Loss of firewater supply | Redundant pump | |
| | | Fails to start | Loss of firewater supply | Redundant pump<br>Periodic testing | |
| | | Fails off while running | Loss of firewater supply | Redundant pump<br>Periodic testing | |
| | | Operates with degraded head/flow performance | Loss of firewater supply | Redundant pump<br>Periodic testing | |
| 3 | Pump discharge pipe from check valve | External rupture | Loss of firewater supply | Redundant pump<br>Check valve in discharge line | |
| | | Plugged | Loss of firewater supply | Redundant pump<br>Periodic testing | |
| 4 | Air release valve (ARV-610/611) | Plugged or fails to operate | Air trapped in system, possible hydraulic hammer | Periodic testing | |
| | | Stuck open | Firewater leak | Periodic testing | |
| 5 | PCV-610B/611B | Plugged or fails to open | Damaged firewater pump | Redundant pump | Add PCV-610B/611B to periodic test schedule |
| | | Opens prematurely or fails to close | Diversion of firewater overboard | | Add PCV-610B/611B to periodic test schedule<br>Verify manual close mechanism on PCV-610B/611B |
| 6 | Check valve | Stuck open | Potential diversion of firewater backward through idle pump<br>Prevents starting of idle diesel or damages pump during start up | | Test discharge check valve during periodic firewater pump tests |
| 7 | Pipe from pump check valve to firewater header | External rupture | Loss of firewater supply | Redundant pump<br>Manual isolation valves | |
| | | Plugged | Loss of firewater supply | Redundant pump<br>Alternate water path | |
| 8 | Discharge strainer | Plugged | Loss of firewater supply | Redundant pump<br>Periodic testing | Verify strainer material is resistant to marine growth |
| | | Broken | Debris plugs firewater nozzles | Clean out settings on fire monitors and hoses | Inspect screen condition periodically |

| Item No. | Component Description | Failure Mode | Effects | Safeguards | Actions |
|---|---|---|---|---|---|
| 9 | Manual test valve | Prematurely opens<br>Left open after test | Diversion of firewater overboard | Redundant valve in discharge line<br>Low pressure switch (PSL-610B/611B) | Requires indepent check of valve position after tresting & periodically thereafter<br>Indicate pressure switch status in control room |
| | | Prematurely closes<br>Left closed during test | Blocked discharge from firewater pump, possibly damaging pump | Pressure control valve (PCV-610B/611B) | |
| 10 | Isolation valve for firewater loop | Prematurely closes<br>Left closed after test | Loss of firewater supply | | Requires independent check of valve position after testing and peridically thereafter |
| 11 | PSL-610B/611B | Spurious low signal | Starts firewater pump | | |
| | | Failure to signal | Firewater pump fails to start on pressure demand | Remote starting system<br>Manual starting system<br>Redundant pump & starting system | Add pressure switch testing to routine pump test |

## FMEA Electrical Example

| Item No. | Component Description | Failure Mode | Effects | Safeguards | Actions |
|---|---|---|---|---|---|
| 1 | Breaker (AB-1) | Inadvertently opens | Shutdown of A-100<br>Shutdown of FCCU | AB-10 opens on low voltage | ♦ Implement an automatic switchover to AB-8 without tripping AB-10<br>♦ Increase/improve preventive maintenance<br>♦ Include IR scanning in quarterly PMs<br>♦ Provide a mechanism to verify AB-4 loading while the FCCU is operating |
| | | Operator cycles breaker | Potential damage to A-100, A-200, A-300, PR-1, PR-2, PR-3, P-100A/B or P-200A/B<br>Potential shutdown of FCCU | ♦ Labels on breakers<br>♦ CB-7 is normally open<br>♦ All breakers open on faults<br>♦ Internal surge protection for A-100 | ♦ Implement out-of-phase permissives that prevent closing beakers between voltage sources<br>♦ Initiate additional operator training |
| | | Fails to Open | Potential damage to A-100<br>Potential shutdown of FCCU | ♦ Main bus breakers open on faults<br>♦ AB-6 opens on faults<br>♦ AB-10 opens on faults, high and low voltage, or high current (time delay)<br>♦ Internal surge protection for A-100 | |
| | | Loss of DC power supply | Loss of breaker control (breakers remain in current positions) | ♦ DC undervoltage alarm<br>♦ DC ground indicators | Verify that all DC equipment is inside only |