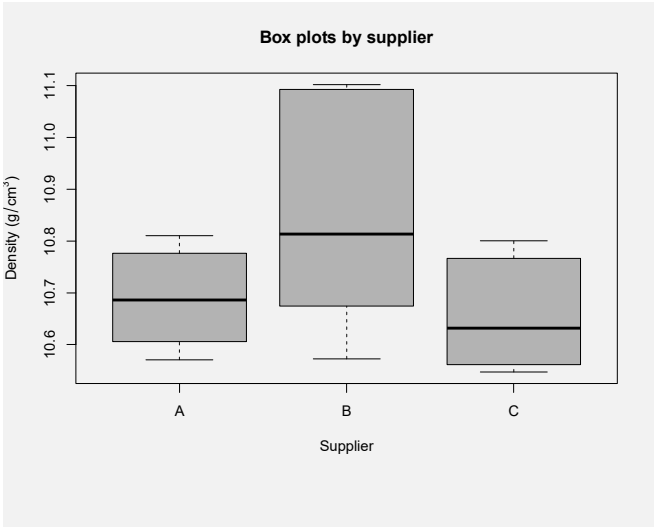
Box Plot

```
psupplier <- rep(c("A", "B", "C"), each = 8)
boxplot(pdensity ~ psupplier,
        col = "gray70",
        xlab = "Supplier",
        ylab = expression("Density ("*g/cm^3*")"),
        main = "Box plots by supplier")
```



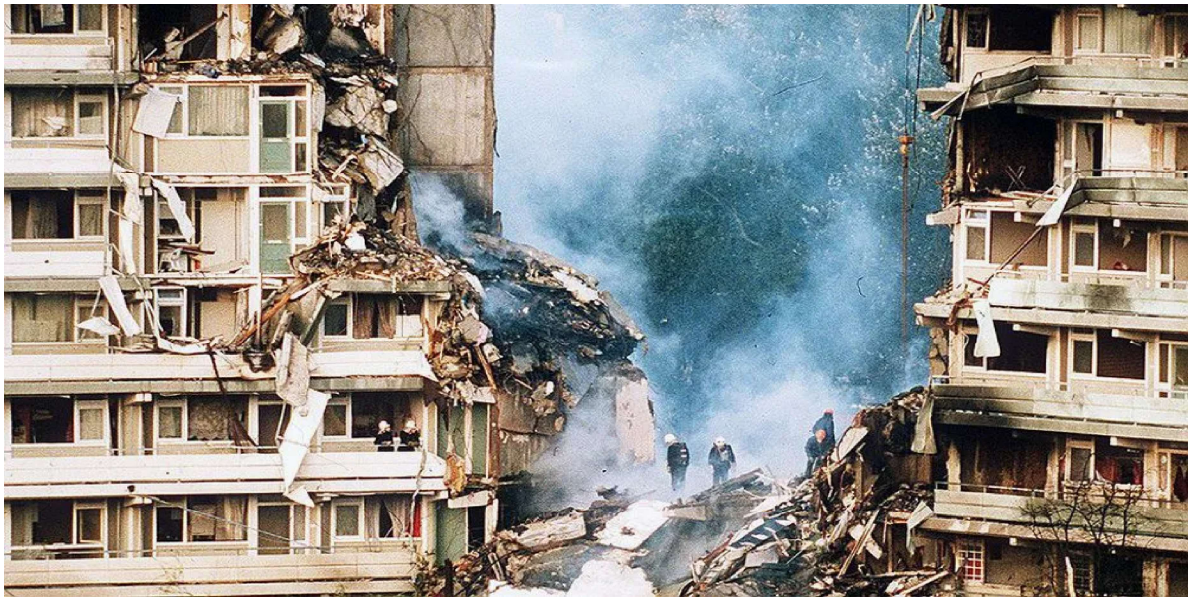
13 Failure Modes, Effects, and Criticality Analysis (FMECA)

Historical Failure Incidents

Collapse of Tacoma Narrows Bridge in 1940: Third largest suspension bridge – connects Seattle and Tacoma (Washington state) – collapsed due to violent vibrations due to *design flaw.*

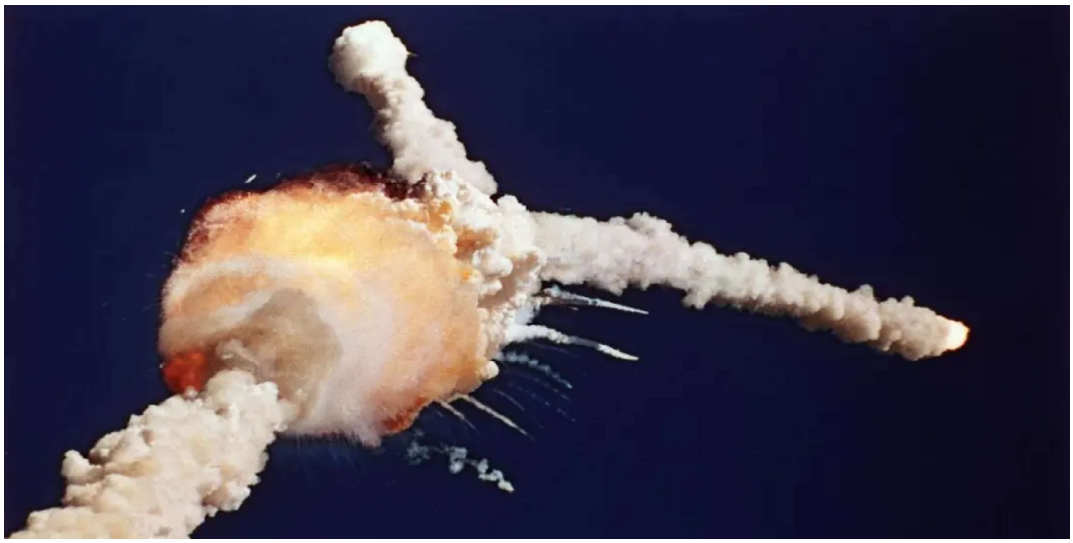
Historical Failure Incidents (cont'd)

Crash of El Al Israel Airlines Boeing 747-200 in 1992: Within 13 mins after takeoff it crashed – primary reason was *manufacturing defects* of the bolts/fuse pins used to attach the engines.



Historical Failure Incidents (cont'd)

Disaster of Space Shuttle Challenger in 1986: NASA's 25th mission. It exploded within 73 seconds after its launch due to *environmental factors.* The temperature was freezing, there was ice built up on shuttle. No data were availabile on how the system is going to perform at such a low temperature. But still it was launched to avoid wasting time in further testing.



Historical Failure Incidents (cont'd)

Fukushima nuclear accident in 2011: Failure of multiple equipment and safety systems. Happened due to *environmental factors/natural hazards* – an earthquake followed by flooding due to Tsunami.

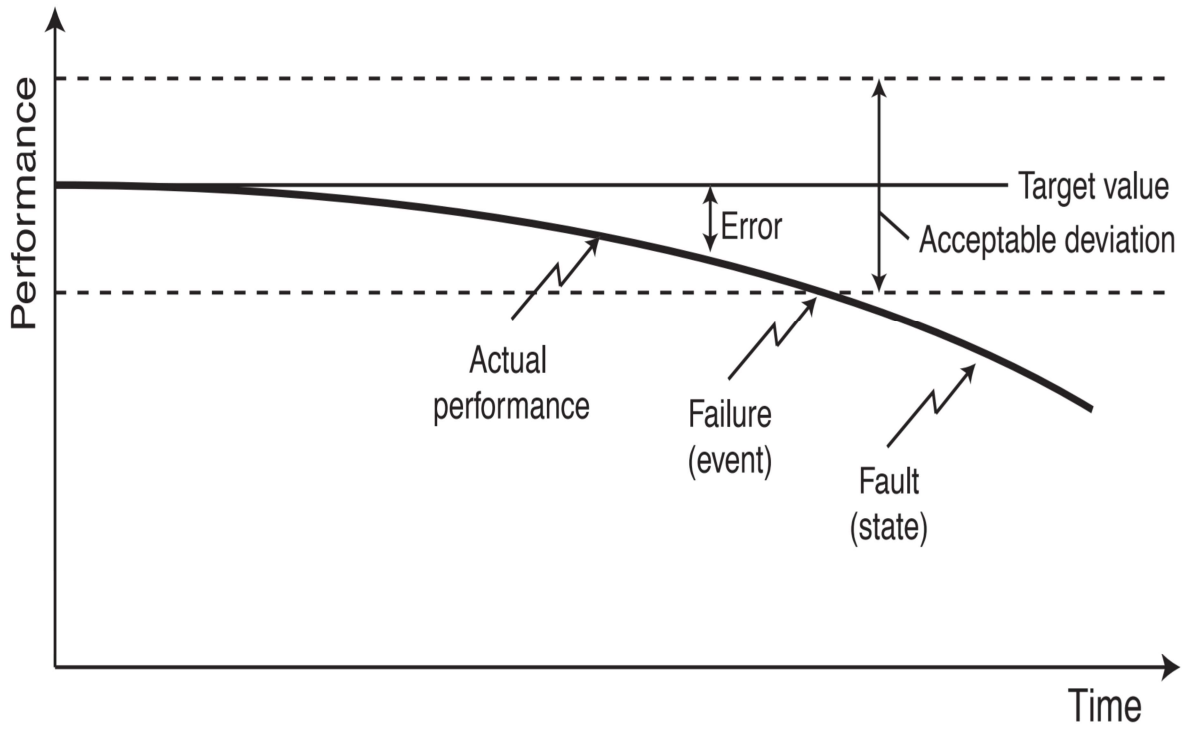
Historical Failure Incidents (cont'd)

Crash of Supersonic aircraft Concorde in 2000: Caused by a *titanium strip fell from another aircraft during its take off.* That strip caused puncture to one of its wheels and then eventually with a series of events, the main engine got effected and it crashed into a hotel.

Why Do Systems Fail?

- Design flaws
- Material/manufacturing defects
- Manufacturing variation
- Stress and overload
- Aging and lack of maintenance
- Incorrect usage or mishandling
- Component obsolescence
- Environmental Factors
- Natural hazards
- Accidents, intentional harm
- Software/firmware errors, electrical surges, cyber attacks
- *Unknown unknowns*

Failure, Fault, & Error



Functions

To identify all *potential failure modes* of an item, we need to identify all the *functions* of the item, and the associated performance requirements.

- Various items may have a high number of functions that are difficult to identify. For example, all the functions of a smart phone.

Function categories: It may sometimes be useful to have a list of general function categories (examples for a water pump):

- Essential functions (e.g., pump water)
- Auxiliary functions (e.g., contain water - prevent leakage out)
- Protective functions (e.g., prevent sparks from electro-motor)
- Information functions (e.g., measure internal pressure, temperature)
- Interface functions (e.g., connect to in/out pipes)
- Superfluous functions (e.g., functions remaining after the system has been modified)

Failure Modes

Failure mode: The way a failure is observed on a failed item.

A failure mode is the way in which an item could fail to perform its required function.

- An item can fail in many different ways – a failure mode is a description of a possible state of the item after it has failed.

Example: The pump must provide (performance requirement) an output between 100 and 110 liters per minute. Associated failure modes may be:

- No output
- Too low output
- Too high output
- Too much fluctuation in output

Failure Modes (cont'd)

A failure mode is always related to a required function and the associated performance requirement.

- A failure mode is description of a fault (i.e., a state) and not of a failure (i.e., an event). [A more correct term would therefore be *fault mode*?]
- Some data sources list, for example, *corrosion* as a failure mode. This is wrong! Corrosion is a *failure mechanism* and may be a cause of a failure mode.

General Failure Modes:

- Failure during operation
- Failure to operate at a prescribed time
- Failure to cease operation at a prescribed time

Failure Modes (cont'd)

Example: Failure modes of a water tap:

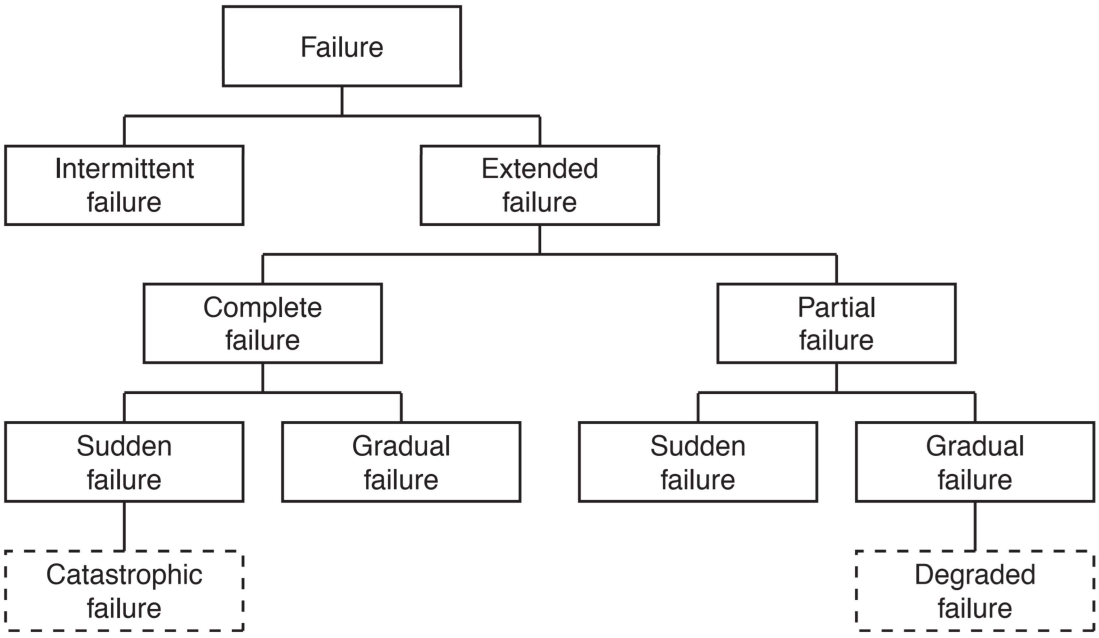
- Fail to open (on demand)
- Fail to close (on demand)
- Cannot fully open
- Fail to regulate flow
- Leakage through (dripping)
- Leakage out (from tap seals)
- Fail to regulate temperature
- Etc.

Failure Classification

Failures may be classified according to:

- *Failure causes:* Primary failure (inherent weakness failure), secondary failure (overstress or misuse failure), command fault
- *Time of failure:* sudden failure, gradual failure
- *Detectability:* evident failure, hidden failure
- *Degree of failure:* partial failure, complete failure

Failure Classification (cont'd)



OREDA Failure Classification

The OREDA project classifies failures according to their *extensiveness.*

- *Critical failure:* Sudden failure that causes termination of one or more fundamental functions.
- *Degraded failure:* Gradual or partial failure – in time, such a failure may develop into a critical failure.
- *Incipient failure:* An imperfection in the state or condition of an item so that a degraded or critical failure can be expected to result if corrective action is not taken.

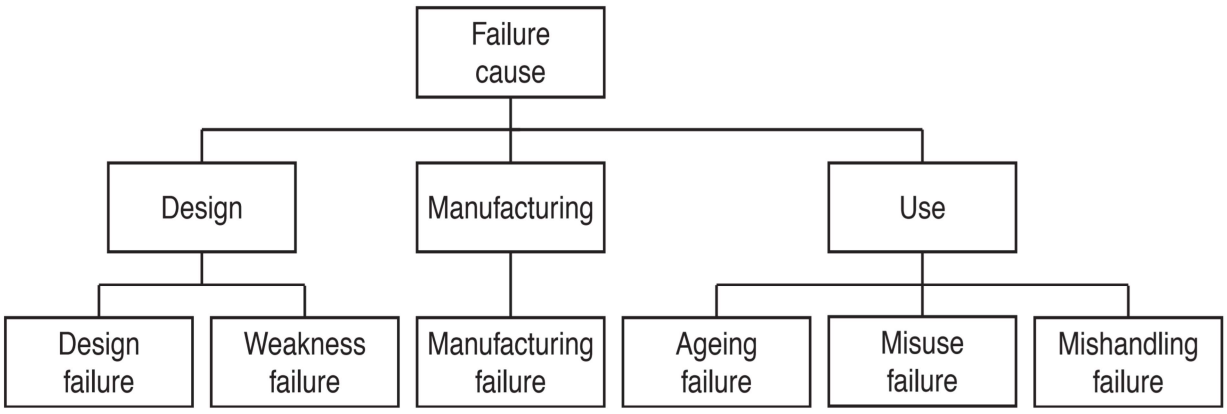
Failure Cause

Failure cause: The circumstances during design, manufacture, or use which have led to a failure.

The following terms can be used when describing the failure causes:

- *Proximate cause:* A condition that is readily identifiable as leading to the failure.
- *Conditioning event:* An event that predisposes a component to failure, or increases its susceptibility to failure.
- *Trigger event:* An event, usually external to the component, that activates the failure, or causes the transition to the failed state.
- *Root cause:* The most basic reasons why the component failed, that - if corrected- would prevent recurrence.

Failure Cause Classification



Failure Mechanism

Failure mechanism: The physical, chemical or other process which has led to a failure.

Examples include: Corrosion, erosion, fatigue, fretting, etc.

What is FMEA/FMECA?

Failure modes, effects, and criticality analysis (FMECA) is a technique used to *identify*, *prioritize*, and *eliminate* potential failures from the system, design or process before they reach the customer.

FMECA is a methodology to identify and analyze:

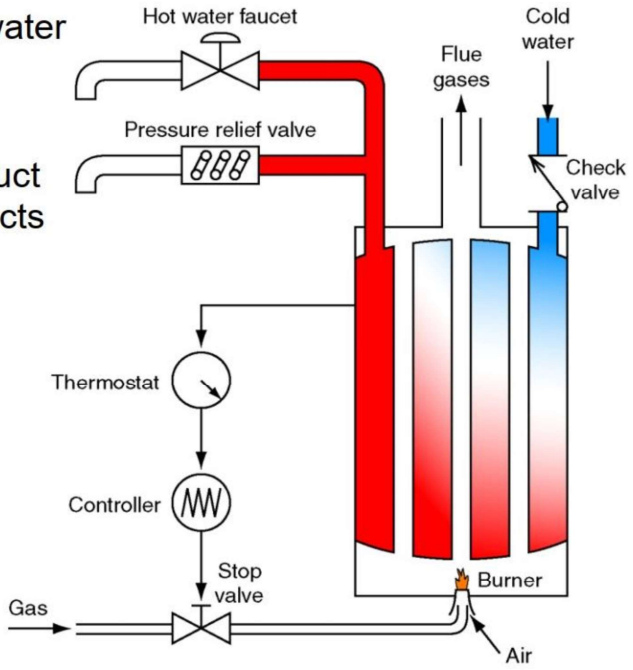
- All potential failure modes of the various parts of a system.
- The effects these failures may have on the system.
- How to avoid the failures, and/or mitigate the effects of the failures on the system.

Initially, the *FMECA* was called *FMEA* (Failure modes and effects analysis). The *C* in FMECA indicates that the criticality (or severity) of the various failure effects are considered and ranked.

FMEA Example

Consider the following water heater system used in a residential home.

The objective is to conduct a failure modes and effects analysis (FMEA) for the system.



FMEA Example (cont'd)

Component	Failure Mode	Effects on other components	Effects on whole system	Consequence Category	Failure Likelihood	Detection Method	Compensating Provisions
Pressure relief valve	Jammed open	Increased gas flow and thermostat operation	Loss of hot water, more cold water input and gas	I - Safe	Occasional	Observe at pressure relief valve	Shut off water supply, reseal or replace relief valve
	Jammed closed	None	None	I - Safe	Probable	Manual testing	No conseq. unless combined with other failure modes
Gas valve	Jammed open	Burner continues to operate, pressure relief valve opens	Water temp. and pressure increase; water turns to steam	III - Critical	Occasional	Water at faucet too hot; pressure relief valve open (obs.)	Open hot water faucet to relieve pres., shut off gas; pressure relief valve compensates
	Jammed closed	Burner ceases to operate	System fails to produce hot water	I - Safe	Remote	Observe at faucet (cold water)	
Thermostat	Fails to react to temp. rise	Burner continues to operate, pressure relief valve opens	Water temp. rises; water turns to steam	III - Critical	Remote	Water at faucet too hot	Open hot water faucet to relieve pressure; pressure relief valve compensates
	Fails to react to temp. drop	Burner fails to function	Water temperature too low	I - Safe	Remote	Observe at faucet (cold water)	

Background

- FMECA was one of the first systematic techniques for failure analysis.
- FMECA was developed by the U.S. Military. The first guideline was Military Procedure MIL-P-1629 "Procedures for performing a failure mode, effects and criticality analysis" dated November 9, 1949.
- FMECA is the most widely used reliability analysis technique in the initial stages of product/system development.
- FMECA is usually performed during the conceptual and initial design phases of the system in order to assure that all potential failure modes have been considered and the proper provisions have been made to eliminate these failures.

What can FMECA be used for?

- Assist in selecting design alternatives with high reliability and high safety potential during the early design phases.
- Ensure that all conceivable failure modes and their effects on operational success of the system have been considered.
- List potential failures and identify the severity of their effects.
- Develop early criteria for test planning and requirements for test equipment.
- Provide historical documentation for future reference to aid in analysis of field failures and consideration of design changes.
- Provide a basis for maintenance planning.
- Provide a basis for quantitative reliability and availability analyses.

FMECA Basic Questions

1. How can each part conceivably fail?
2. What mechanisms might produce these modes of failure?
3. What could the effects be if the failures did occur?
4. Is the failure in the safe or unsafe direction?
5. How is the failure detected?
6. What inherent provisions are provided in the design to compensate for the failure?

When to Perform an FMECA?

The FMECA should be initiated early in the design process, where we are able to have the greatest impact on the equipment reliability.

Types of FMECA

- *Design FMECA* is carried out to eliminate failures during equipment design, taking into account all types of failures during the whole life-span of the equipment.
- *Process FMECA* is focused on problems stemming from how the equipment is manufactured, maintained or operated.
- *System FMECA* looks for potential problems and bottlenecks in larger processes, such as entire production lines.

Two Approaches to FMECA

- *Bottom-up approach:* Used when a system concept has been decided. Each component on the lowest level is studied one-by-one. The bottom-up approach is also called *hardware* approach. The analysis is complete since all components are considered.

- *Top-down approach:* Used in an early design phase before the whole system structure is decided. The analysis is usually function oriented. The analysis starts with the main system functions - and how these may fail. Functional failures with significant effects are usually prioritized in the analysis. The analysis will not necessarily be complete. The top-down approach may also be used on an existing system to focus on problem areas.

FMECA Standards

- MIL-STD 1629 "Procedures for performing a failure mode and effect analysis"

- IEC 60812 "Procedures for failure mode and effect analysis (FMEA)"

- BS 5760-5 "Guide to failure modes, effects and criticality analysis (FMEA and FMECA)"

- SAE ARP 5580 "Recommended failure modes and effects analysis (FMEA) practices for non-automobile applications"

- SAE J1739 "Potential Failure Mode and Effects Analysis in Design (Design FMEA) and Potential Failure Mode and Effects Analysis in Manufacturing and Assembly Processes (Process FMEA) and Effects Analysis for Machinery (Machinery FMEA)"

- SEMATECH (1992) "Failure Modes and Effects Analysis (FMEA): A Guide for Continuous Improvement for the Semiconductor Equipment Industry"

FMECA Main Steps

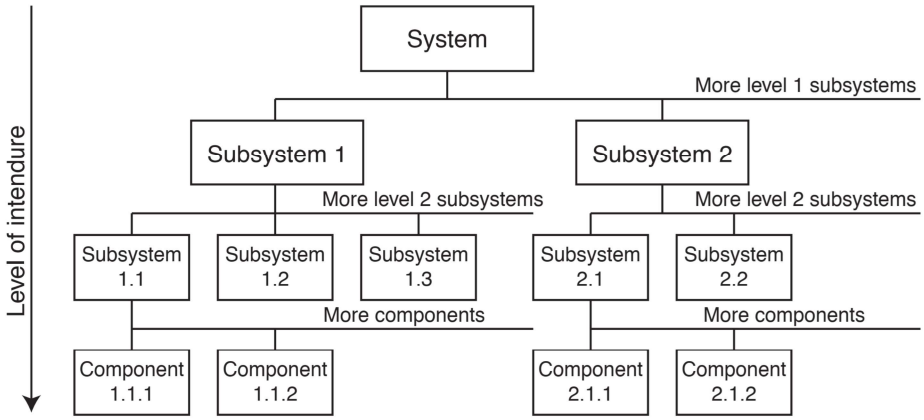
1. FMECA prerequisites
2. System structure analysis
3. Failure analysis and preparation of FMECA worksheets
4. Team review
5. Corrective actions

FMECA Prerequisites

1. Define the system to be analyzed:
   - System boundaries (which parts should be included and which should not).
   - Main system missions and functions (including functional requirements).
   - Operational and environmental conditions to be considered. Additionally, interfaces that cross the design boundary should be included in the analysis.
2. Collect available information that describes the system to be analyzed; including drawings, specifications, schematics, component lists, interface information, functional descriptions, etc.
3. Collect information about previous and similar designs from internal and external sources; including FRACAS data, interviews with design personnel, operations and maintenance personnel, component suppliers, etc.

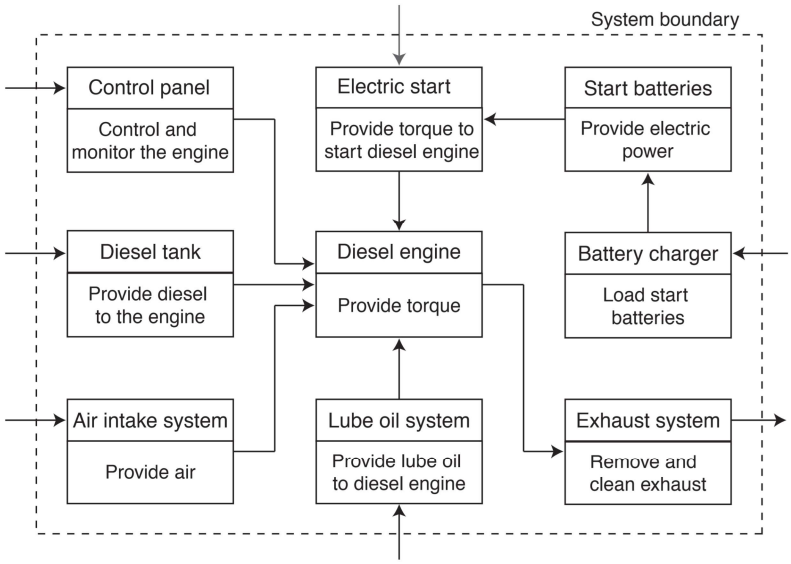
System Structure Analysis

Divide the system into manageable units – typically functional elements. To what level of detail we should break down the system will depend on the objective of the analysis. It is often desirable to illustrate the structure by a hierarchical tree diagram:



System Structure Analysis (cont'd)

In some applications it may be beneficial to illustrate the system by a *functional block diagram (FBD)* as illustrated in the following figure.



FMECA Worksheet

A suitable FMECA worksheet has to be decided. In many cases the client (customer) will have requirements to the worksheet format.

System: Performed by:

Ref. drawing no.: Date: Page: of

Description of unit			Description of failure			Effect of failure		Failure rate	Severity ranking	Risk reducing measures	Comments
Ref. no	Function	Operational mode	Failure mode	Failure cause or mechanism	Detection of failure	On the subsystem	On the system function				
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)	(10)	(11)	(12)

FMECA Worksheet (cont'd)

For each system element (subsystem, component) the analyst must consider all the functions of the elements in all its operational modes, and ask if any failure of the element may result in any unacceptable system effect.

- If the answer is *no*, then no further analysis of that element is necessary.
- If the answer is *yes*, then the element must be examined further.

Various columns in the *FMECA worksheet*:

1. In the first column a unique reference to an element (subsystem or component) is given. It may be a reference to an id. in a specific drawing, a so-called tag number, or the name of the element.
2. The functions of the element are listed. It is important to list all functions. A checklist may be useful to secure that all functions are covered.
3. The various operational modes for the element are listed. Example of operational modes are: idle, standby, and running. In applications where it is not relevant to distinguish between operational modes, this column may be omitted.

FMECA Worksheet (cont'd)

4 For each functional and operational mode of an element the potential failure modes have to be identified and listed. A failure mode should be defined as a nonfulfillment of the functional requirements of the functions specified in column 2.

5 The failure modes identified in column 4 are studied one-by-one. The failure mechanisms (e.g., corrosion, erosion, fatigue) that may produce or contribute to a failure mode are identified and listed. Other possible causes of the failure mode should also be listed. If may be beneficial to use a checklist to secure that all relevant causes are considered. Other relevant sources include: "Failure Mode/Mechanism Distributions" (FMD) published by RAC, and OREDA (for offshore equipment).

6 The various possibilities for detection of the identified failure modes are listed. These may involve diagnostic testing, different alarms, proof testing, human perception, and so on. Some failure modes are *evident*, other are *hidden*. The failure mode "fail to start" of a pump with operational mode "standby" is an example of a hidden failure.

FMECA Worksheet (cont'd)

In some applications, an extra column is added to rank the likelihood that the failure will be detected before the system reaches the end-user/customer. The following detection ranking may be used (SEMATECH-1992):

Rank	Description
1-2	Very high probability that the defect will be detected. Verification and/or controls will almost certainly detect the existence of a deficiency or defect.
3-4	High probability that the defect will be detected. Verification and/or controls have a good chance of detecting the existence of a deficiency/defect.
5-7	Moderate probability that the defect will be detected. Verification and/or controls are likely to detect the existence of a deficiency or defect.
8-9	Low probability that the defect will be detected. Verification and/or control not likely to detect the existence of a deficiency or defect.
10	Very low (or zero) probability that the defect will be detected. Verification and/or controls will not or cannot detect the existence of a deficiency/defect.

FMECA Worksheet (cont'd)

7 The effects each failure mode may have on other components in the same subsystem and on other subsystems as such (*local effects*) are listed.

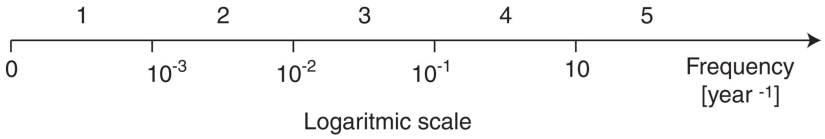
8 The effects each failure mode may have on the system (*global effects*) are listed. The resulting operational status of the system after the failure may also be recorded, that is, whether the system is functioning or not, or is switched over to another operational mode. In some applications it may be beneficial to consider each category of effects separately, like: safety effects, environmental effects, production availability effects, economic effects, and so on.

In some applications it may be relevant to include separate columns in the worksheet for *Effects on safety, Effects on availability*, etc.

FMECA Worksheet (cont'd)

9 Failure rates for each failure mode are listed. In many cases it is more suitable to classify the failure rate in rather broad classes. An example of such a classification is:

1	Very unlikely	Once per 1000 years or more seldom
2	Remote	Once per 100 years
3	Occasional	Once per 10 years
4	Probable	Once per year
5	Frequent	Once per month or more often



Logaritmic scale

In some applications it is common to use a scale from 1 to 10, where 10 denotes the highest rate of occurrence.

FMECA Worksheet (cont'd)

Probability of occurrence rankings

Probability of railure mode	Possible failure rates	Probability	Ranking
Very high: failure is almost inevitable	≥ 1 in 2	$.50 \leq p \leq 1.00$	10
Very high	≥ 1 in 3	$.33 \leq p < .50$	9
High: repeated failures	≥ 1 in 8	$.125 \leq p < .33$	8
High	≥ 1 in 20	$.05 \leq p < .125$	7
Moderate: occasional failures	≥ 1 in 80	$.0125 \leq p < .05$	6
Moderate	≥ 1 in 400	$.0025 \leq p < .0125$	5
Moderate: infrequent failures	≥ 1 in 2000	$.0005 \leq p < .0025$	4
Low: relatively few failures	≥ 1 in 15,000	$.0000667 \leq p < .0005$	3
Low	≥ 1 in 150,000	$6.7 \times 10^{-6} \leq p < 6.67 \times 10^{-5}$	2
Remote: failure is unlikely	≥ 1 in 1,500,000	$6.7 \times 10^{-7} \leq p < 6.67 \times 10^{-6}$	1

* Table adopted from an FMEA reference manual (Chrysler, Ford, General Motors Supplier Quality Requirements Task Force)

FMECA Worksheet (cont'd)

10 The severity of a failure mode is the worst potential (but realistic) effect of the failure considered on the system level (the global effects). The following severity classes for health and safety effects are sometimes adopted:

Rank	Severity class	Description
10	Catastrophic	Failure results in major injury or death of personnel.
7-9	Critical	Failure results in minor injury to personnel, personnel exposure to harmful chemicals or radiation, or fire or a release of chemical to the environment.
4-6	Major	Failure results in a low level of exposure to personnel, or activates facility alarm system.
1-3	Minor	Failure results in minor system damage but does not cause injury to personnel, allow any kind of exposure to operational or service personnel or allow any release of chemicals into the environment

FMECA Worksheet (cont'd)

In some applications, the following severity classes are used (SEMATECH-1992):

Rank	Description
10	Failure will result in major customer dissatisfaction and cause non-system operation or non-compliance with government regulations.
8-9	Failure will result in high degree of customer dissatisfaction and cause non-functionality of system.
6-7	Failure will result in customer dissatisfaction and annoyance and/or deterioration of part of system performance.
3-5	Failure will result in slight customer annoyance and/or slight deterioration of part of system performance.
1-2	Failure is of such minor nature that the customer (internal or external) will probably not detect the failure.

FMECA Worksheet (cont'd)

11 Possible actions to correct the failure and restore the function or prevent serious consequences are listed. Actions that are likely to reduce the frequency of the failure modes should also be recorded. We come bach to these actions later in the presentation.

12 The last column may be used to record pertinent information not included in the other columns.

Risk Ranking

The risk related to the various failure modes is often presented by:

1. Risk matrix
2. Risk priority number (RPN)

Risk Matrix: The risk associated to failure mode is a function of the frequency of the failure mode and the potential end effects (severity) of the failure mode. The risk may be illustrated in a risk matrix.

Frequency/ consequence	1 Very unlikely	2 Remote	3 Occasional	4 Probable	5 Frequent
Catastrophic					
Critical					
Major					
Minor					

Acceptable - only ALARP actions considered

Not acceptable - risk reducing measures required

Acceptable - use ALARP principle and consider further investigations

Risk Ranking (cont'd)

Risk Priority Number (RPN): An alternative to the risk matrix is to use the RPN.

- O = The rank of the occurrence of the failure mode
- S = The rank of the severity of the failure mode
- D = The rank of the likelihood that the failure will be detected before the system reaches the end-user/customer.

All ranks are given on a *scale* from 1 to 10. The risk priority number (*RPN*) is defined as

$$RPN = S \times O \times D$$

Note: The smaller the RPN the better – and – the larger the worse.

Alternative FMECA Worksheet

When using the risk priority number, we sometimes use an alternative worksheet with separate columns for O, S, and D. An example is shown below:

Project: Version: Date:

System: Subsystem: Teamwork leader:

Id.	Comp.	Function	Failure mode	Failure cause	Local effects	Global effects	S	O	D	RPN	Corrective actions

FMECA Review Team

A design FMECA should be initiated by the design engineer, and the system/process FMECA by the systems engineer. The following personnel may participate in reviewing the FMECA (the participation will depend on type of equipment, application, and available resources):

- Project manager
- Design engineer (hardware/software/systems)
- Test engineer
- Reliability engineer
- Quality engineer
- Maintenance engineer
- Field service engineer
- Manufacturing/process engineer
- Safety engineer

Review Objectives

The review team studies the FMECA worksheets and the risk matrices and/or the risk priority numbers (RPN). The main objectives are:

1. To decide whether or not the system is acceptable
2. To identify feasible improvements of the system to reduce the risk. This may be achieved by:
   - Reducing the likelihood of occurrence of the failure
   - Reducing the effects of the failure
   - Increasing the likelihood that the failure is detected before the system reaches the end-user.

Note: If improvements are decided, the FMECA worksheets have to be revised and the RPN should be updated.

Problem solving tools like brainstorming, flow charts, Pareto charts and nominal group technique may be useful during the review process.

Selection & Reporting of Actions

The risk may be reduced by introducing:
- Design changes
- Engineered safety features
- Safety devices
- Warning devices
- Procedures/training

The suggested corrective actions can be reported, for example, as illustrated in the printout from the *Reliasoft Xfmea* program:

Xfmea®

RECOMMENDED ACTIONS
(Summary Report)

Date: 3/26/2003
Page 5 of 9

#	Recommended Action(s)	Target Completion Date	Responsibility	Actions Taken	Item	Potential Cause(s)/Mechanism(s) of Failure	Priority
1	Add laboratory accelerated corrosion testing.	2/25/2003	A. Tate Body Engrg	Based on test results (Test No. 1481) upper edge spec raised 125 mm.	Front Door L.H.	Upper edge of protective wax application specified for inner door panels is too low.	
2	Add laboratory accelerated corrosion testing.	3/28/2003	A. Tate Body Engrg	Test results (Test No. 1481) show specified thickness is adequate.	Front Door L.H.	Insufficient wax thickness specified.	
3	Conduct Design of Experiments (DOE) on wax thickness.	3/28/2003	A. Tate Body Engrg	DOE shows 25% variation in specified thickness is acceptable.	Front Door L.H.	Insufficient wax thickness specified.	
4	Add team evaluation using production spray equipment and specified wax.	3/28/2003	Body Engrg & Assy Ops	Based on test, addition vent holes will be provided in affected areas.	Front Door L.H.	Entrapped air prevents wax from entering corner/edge access.	
5	Add team evaluation using design aid buck and spray head.	3/28/2003	Body Engrg & Assy Ops	Evaluation showed adequate access.	Front Door L.H.	Insufficient room between panels for spray head access.	

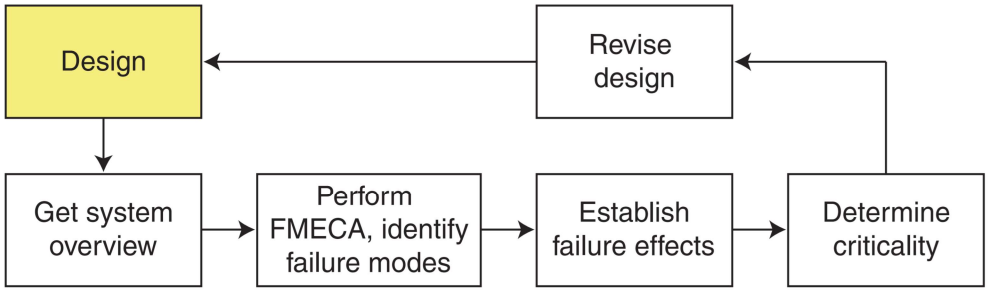
RPN Reduction

The risk reduction related to a corrective action may be comparing the RPN for the initial and revised concept:

	Occurrence O	Severity S	Detection D	RPN
Initial	7	8	5	280
Revised	5	8	4	160
% Reduction in RPN				43%

Application

- *Design engineering:* The FMECA worksheets are used to identify and correct potential design related problems.



- *Manufacturing:* The FMECA worksheets may be used as input to optimize production, acceptance testing, etc.

- *Maintenance planning:* The FMECA worksheets are used as an important input to maintenance planning – for example, as part of reliability centered maintenance (RCM). Maintenance related problems may be identified and corrected.

Summing Up: Three Main Phases of FMECA

Phase	Question	Output
Identify	What can go wrong?	Failure descriptions Causes → Failure modes → Effects
Analyze	How likely is a failure? What are the consequences?	Failure rates RPN = Risk priority number
Act	What can be done? How can we eliminate the causes? How can we reduce the severity?	Design solutions, Test plans, manufacturing changes, Error proofing, etc.