# Chapter 8 - Reliability, Maintainability, and Availability
## by Michael Pecht (pages 303-326)

from Handbook of Systems Engineering and Management, edited by Andrew P. Sage and William B. Rouse (Wiley-Interscience, 1999). See pages 37-38 for chapter synopsis.

## *What should be gained from reading this chapter?*

(1) You should be able to define reliability, maintainability, and availability, and identify their differences.

(2) You should be able to describe some benefits of reliability, maintainability, and availability.

(3) You should be able to describe qualification and quality conformance, and identify their differences.

(4) You should be able to define and describe the nature of some basic system reliability models.

(5) You should have the ability to convey a general understanding of Failure Modes and Effects Analysis (FMEA)

(6) You should be able to differentiate between readiness and availability.

# RELIABILITY MAINTAINABILITY AVAILABILITY

Disciplinary areas yielding means of addressing:

- system failure(s)
- operational readiness and success
- maintenance and service requirements
- system effectiveness evaluation and improvement

Key benefit of integrating reliability, maintainability, and availability concepts into the design process ~

***early determination of feasibility and risk***

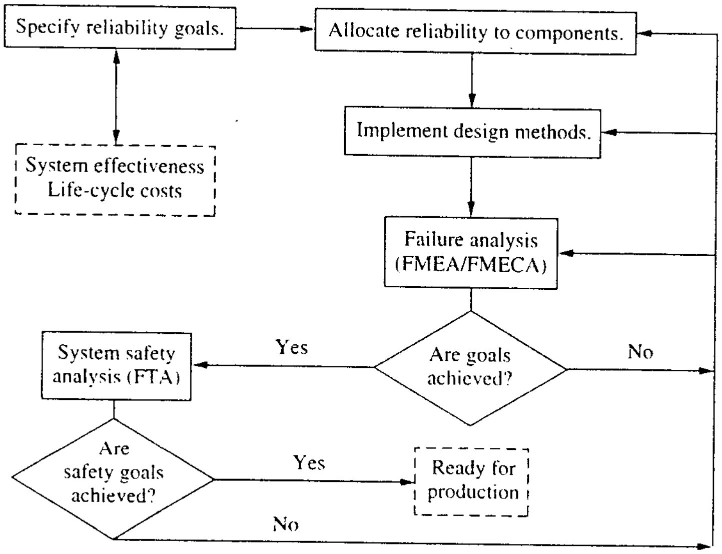
# Design for Reliability Tasks:

**(Pecht, pp 305-306, Sage & Rouse)**

- **Define realistic system requirements**
- **Define the system usage environment**
- **Identify potential failure sites and mechanisms**
- **Characterize materials and processes**
- **Design within materials and processes capabilities**
- **Qualify processes**
- **Control processes**
- **Manage system life cycle**

# Reliability Design Process:

**(Ebeling, pp 145-147)**



Specify reliability goals.
Allocate reliability to components.
System effectiveness
Life-cycle costs
Implement design methods.
Failure analysis
(FMEA/FMECA)
Are goals achieved?
Yes
No
System safety analysis (FTA)
Are safety goals achieved?
Yes
Ready for production
No

**Design Methods:**

- **Proper selection of parts and material**
- **Stress-strength analysis**
- **Derating (operating system below rated stress level)**
- **Simplification**
- **Identification of technologies**
- **Use of redundancy**

# Reliability and Product Life Cycle:

(Ebeling, pp 145-147)

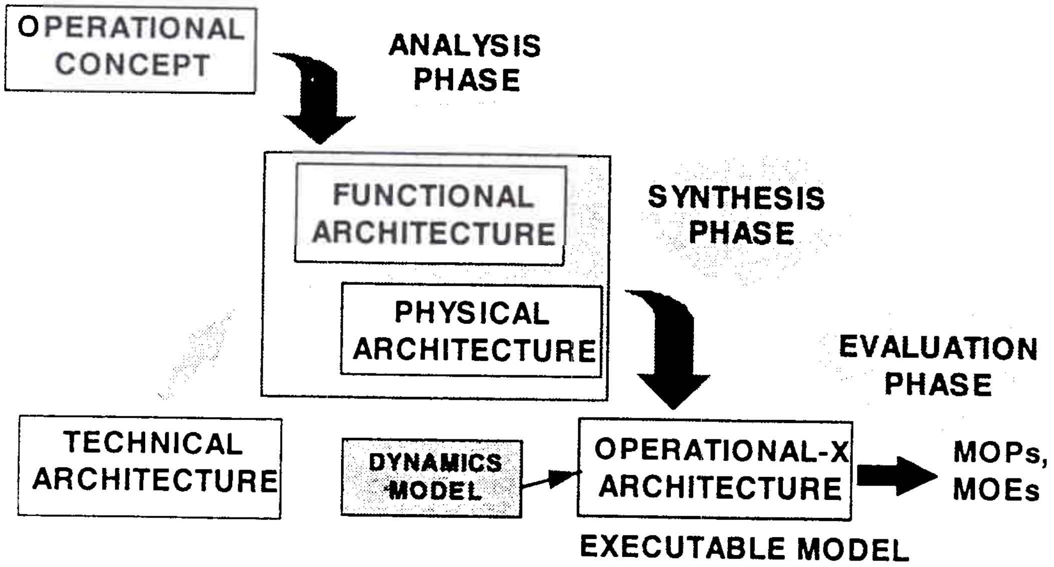
| Phase or Stage | Reliability Activities |
|---|---|
| Conceptual Preliminary Design | Specification<br>Allocation<br>Design methods |
| Detailed Design, Development, and Prototyping | Design methods<br>Failure analysis<br>Growth testing<br>Safety analysis |
| Production and Manufacture | Acceptance testing<br>Quality control<br>Burn-in and screening |
| Product Use and Support | Preventive maintenance<br>Predictive maintenance<br>Modifications<br>Parts replacement |

**Reliability influenced throughout product life cycle by factors external to product itself**

# Architectures and Reliability

## Several Types of Architectures:

(Levis, pp 430-432, Sage & Rouse)



Functional Architecture: *Set of activities or functions, arranged in an order that achieves requirements when activated*

Physical Architecture: *Representation of physical resources, and their connectivity, that constitute the system*

Technical Architecture: *Rules governing arrangement, interaction, and interdependence of parts or elements ensuring that system satisfies requirements*

Operational/Executable Architecture: *Executable, dynamic model for performance evaluation of the system, with information traceable to at least one of the three static architectures*

# Protective Architectures:

✓ Proper hardware and software selections

✓ Interactions of system components and subsystems

✓ Redundancy approaches include

  - sensing for failures or potential failures
  - protecting against secondary effects

# System Stress:

✓ Emphasis on hardware

- inherent characteristics
- external operating conditions

✓ General stress failure categories include

- electrical
- thermal
- chemical
- mechanical

Examples: temperature, humidity, vibration, radiation, power, current, voltage, corrosion

✓ Costs associated with lowering stresses include

- money
- weight
- velocity
- complexity

# Qualification:

***process of confirming ability of nominal design and production specifications to meet customer needs***

**Perform reliability testing for qualification**

- **during initial product development**
- **after any design or production changes in existing product**

***for example,***

**reliability tests for environmental qualification of hardware might include**

- **shock and vibration**
- **humidity**
- **salt spray**
- **electromagnetic interference**

# Quality Conformance:

*Process of monitoring, verifying, and controlling critical material variables and process parameters*

*to ensure that parameters which have been qualified are maintained within specified tolerances*

Fundamental aspect of quality conformance program:

understanding potential defects introduced prior to and during the production cycle

*Evaluation testing (screening):*

*audit process to ensure that product's materials and production conform to the control limits of the production processes*

# Reliability Assessment:

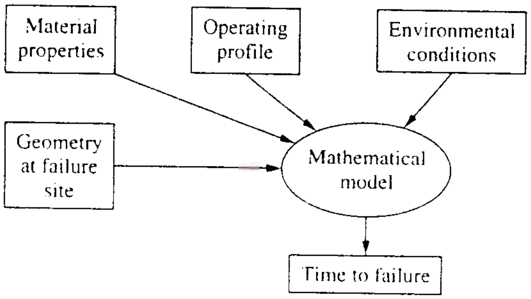
- **Understanding possible failure mechanisms**

  **allows identification and solution of potential problems in new and existing technologies *before* they occur**

- **Physics-of-failure models**

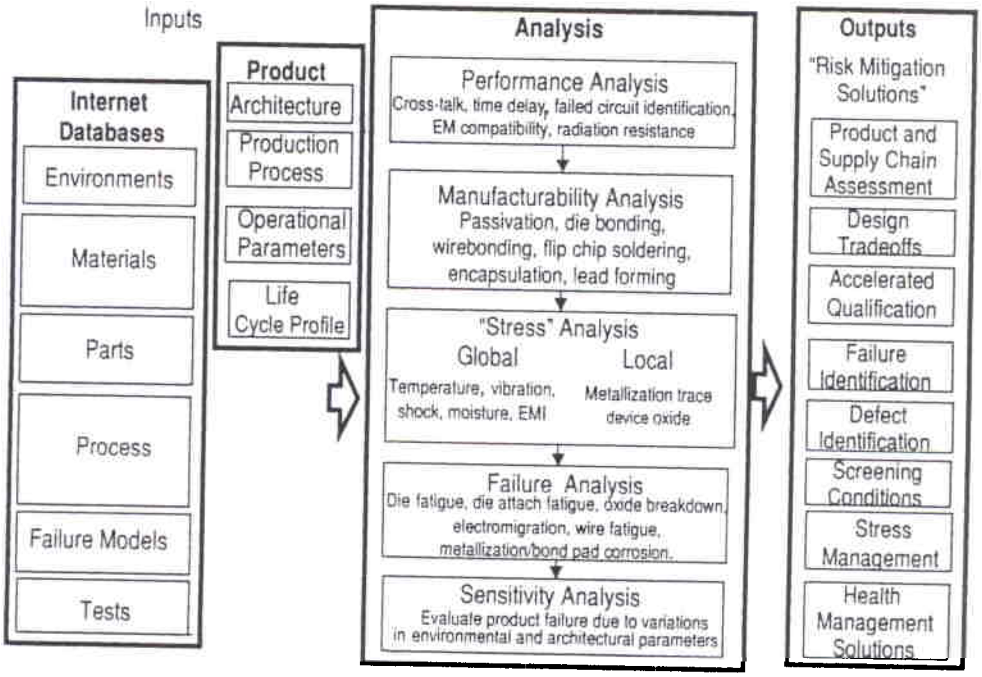
  **mathematically derived models based on knowledge of failure mechanisms and their root causes**

- **Physics-of-failure conceptual model**
  **(Ebeling, p 138)**



# Physics-of-failure process model example

**(Pecht, p 314, Sage & Rouse)**


Inputs
Internet Databases
Environments
Materials
Parts
Process
Failure Models
Tests
Product
Architecture
Production Process
Operational Parameters
Life Cycle Profile
Analysis
Performance Analysis
Cross-talk, time delay, failed circuit identification, EM compatibility, radiation resistance
Manufacturability Analysis
Passivation, die bonding, wirebonding, flip chip soldering, encapsulation, lead forming
"Stress" Analysis
Global
Temperature, vibration, shock, moisture, EMI
Local
Metallization trace device oxide
Failure Analysis
Die fatigue, die attach fatigue, oxide breakdown, electromigration, wire fatigue, metallization/bond pad corrosion.
Sensitivity Analysis
Evaluate product failure due to variations in environmental and architectural parameters
Outputs
"Risk Mitigation Solutions"
Product and Supply Chain Assessment
Design Tradeoffs
Accelerated Qualification
Failure Identification
Defect Identification
Screening Conditions
Stress Management
Health Management Solutions

# System Reliability Assessment Modeling:

*Evaluation of system design configurations based on subsystem and component reliabilities*

Facilitates tradeoffs between

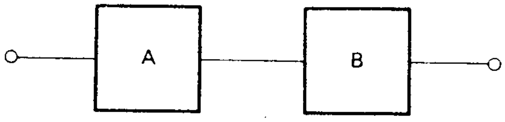
- reliability (e.g., redundancy)
- resources (e.g., cost, weight, power)

Five basic system model types:

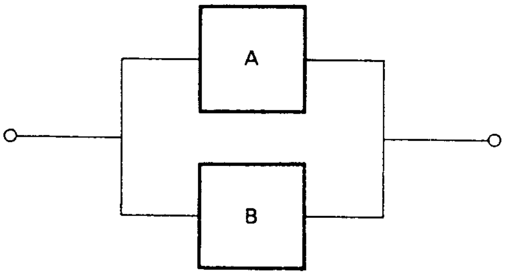
- Series
- Parallel
- Mixed Series & Parallel
- Complex
- Standby

# System Reliability Assessment Models:

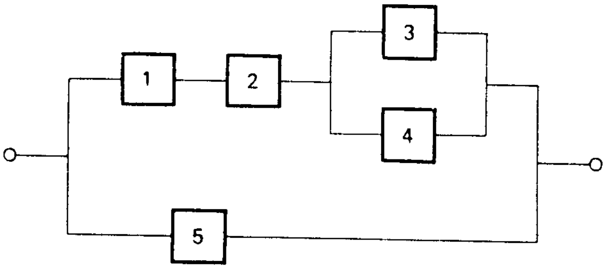
## *Series*



## *Parallel*

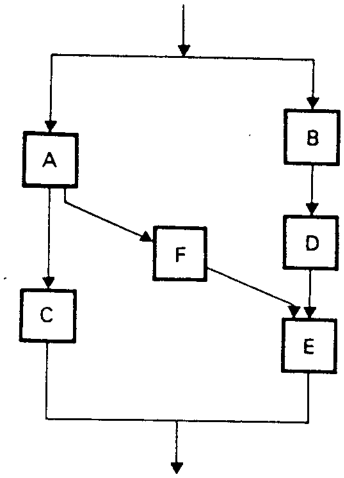


## *Mixed Series & Parallel*

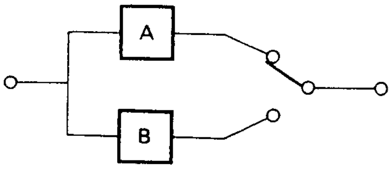


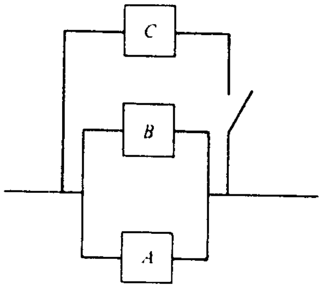
# System Reliability Assessment Models:

## *Complex*



## *Standby*



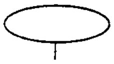
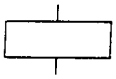
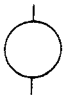
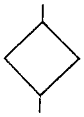
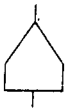
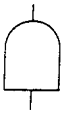
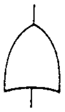
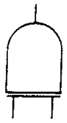
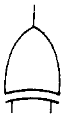


# Fault-Tree Analysis:

## Logical deductive approach using graphical enumeration of ways in which system failure can occur, and probability of occurrence

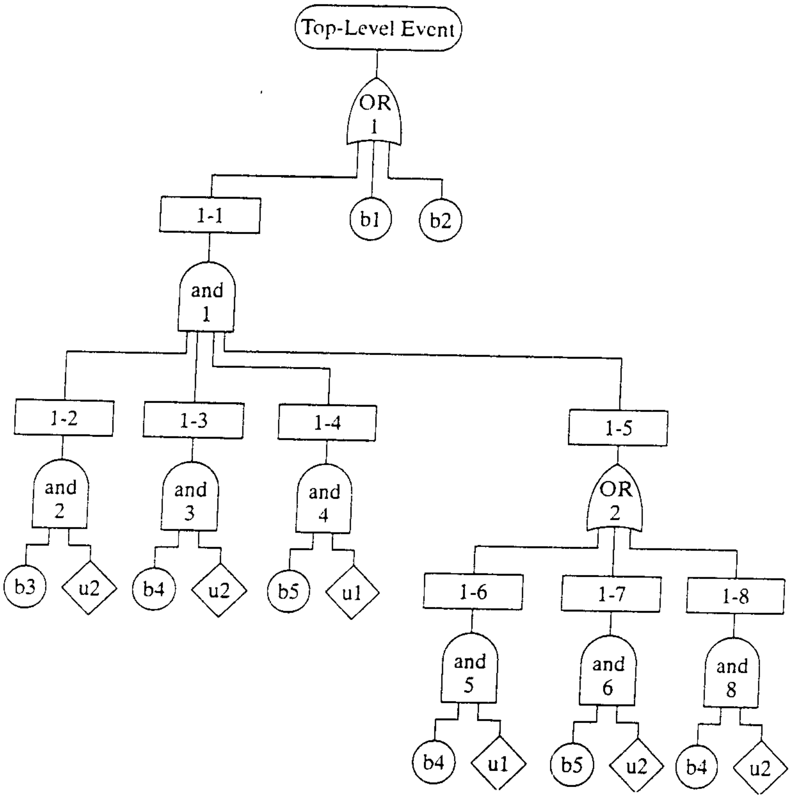
## Fault-Tree Symbology

**(Blanchard, p 221)**

| Fault-Tree Symbol | Discussion |
|---|---|
|  | The ellipse represents the *top-level event.* Obviously, the ellipse always appears at the very top of a fault tree. |
|  | The rectangle represents an *intermediate fault event.* A rectangle can appear anywhere in a tree except at the lowest level in the hierarchy. |
|  | A circle represents the *lowest-level failure event,* also called a basic event. Basic events are likely to appear at the lowest level in a fault tree. |
|  | The diamond represents an *undeveloped event.* Undeveloped events could be further broken down but are not for the sake of simplicity. Very often, complex undeveloped events are analyzed through a separate fault tree. Underdeveloped events appear at the lowest level in a fault tree. |
|  | This symbol, sometimes called the house, represents an *input event.* An input event refers to a signal or input that could cause a system failure. |
|  | This symbol represents the *AND logic gate.* In this case, the output is realized only after all the associated inputs have been received. |
|  | This symbol represents the *OR logic gate.* In this case, any one or more of the inputs need to be received for the output to be realized. |
|  | This symbol represents the *ORDERED AND logic gate.* In this case, the output is realized only after all the associated inputs have been received in a particular predetermined order. |
|  | This symbol represents the *EXCLUSIVE OR logic gate.* In this case, one and only one of the associated inputs needs to be received for the input to be realized. |

# Illustrative Fault Tree:

**(Blanchard, p 220)**



# Failure Modes and Effects Analysis (FMEA):

*Process of evaluating a system relative to*

- possible failures
- anticipated modes and expected frequency of failure
- causes of failure
- consequences of failure and impact(s) on the system overall
- areas where preventive measures can be initiated to preclude future such failures

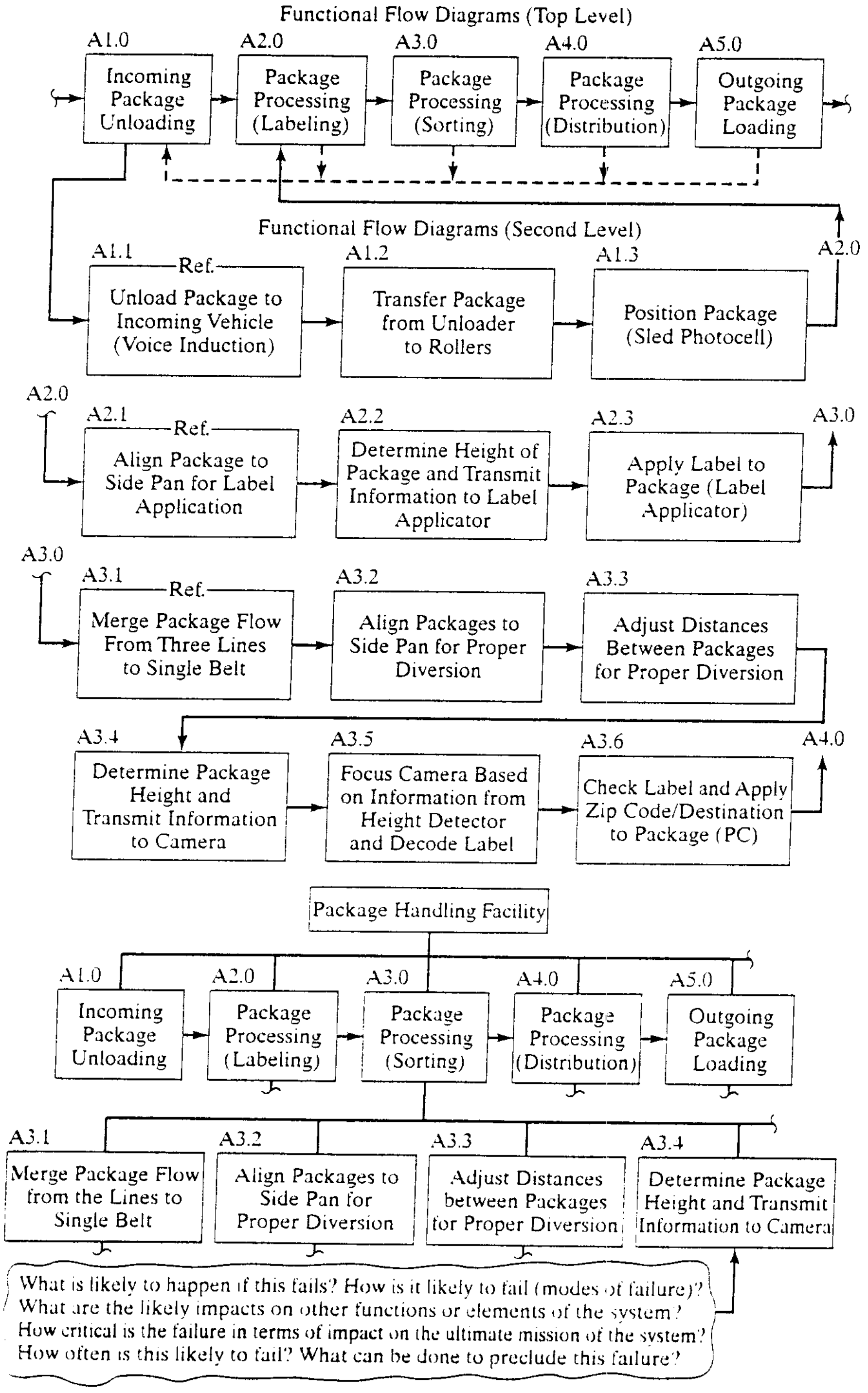
*Objective is to identify*

- weak links in the system
- criticality and impact of failures on system in completing its mission
- potential safety problems
- areas of high risk

# Illustrative FMEA:

**(Blanchard, p 277)**

## Application of FMEA to Package Handling System



Functional Flow Diagrams (Top Level)

A1.0 Incoming Package Unloading

A2.0 Package Processing (Labeling)

A3.0 Package Processing (Sorting)

A4.0 Package Processing (Distribution)

A5.0 Outgoing Package Loading

Functional Flow Diagrams (Second Level)

A1.1 Ref. Unload Package to Incoming Vehicle (Voice Induction)

A1.2 Transfer Package from Unloader to Rollers

A1.3 Position Package (Sled Photocell)

A2.0

A2.0

A2.1 Ref. Align Package to Side Pan for Label Application

A2.2 Determine Height of Package and Transmit Information to Label Applicator

A2.3 Apply Label to Package (Label Applicator)

A3.0

A3.0

A3.1 Ref. Merge Package Flow From Three Lines to Single Belt

A3.2 Align Packages to Side Pan for Proper Diversion

A3.3 Adjust Distances Between Packages for Proper Diversion

A3.4 Determine Package Height and Transmit Information to Camera

A3.5 Focus Camera Based on Information from Height Detector and Decode Label

A3.6 Check Label and Apply Zip Code/Destination to Package (PC)

A4.0

Package Handling Facility

A1.0 Incoming Package Unloading

A2.0 Package Processing (Labeling)

A3.0 Package Processing (Sorting)

A4.0 Package Processing (Distribution)

A5.0 Outgoing Package Loading

A3.1 Merge Package Flow from the Lines to Single Belt

A3.2 Align Packages to Side Pan for Proper Diversion

A3.3 Adjust Distances between Packages for Proper Diversion

A3.4 Determine Package Height and Transmit Information to Camera

What is likely to happen if this fails? How is it likely to fail (modes of failure)? What are the likely impacts on other functions or elements of the system? How critical is the failure in terms of impact on the ultimate mission of the system? How often is this likely to fail? What can be done to preclude this failure?

# Design for Maintainability:

## *Maintainability:*

Probability that a failed component or system will be restored or repaired to a specified condition within a specified period of time when maintenance is performed in accordance with prescribed procedures

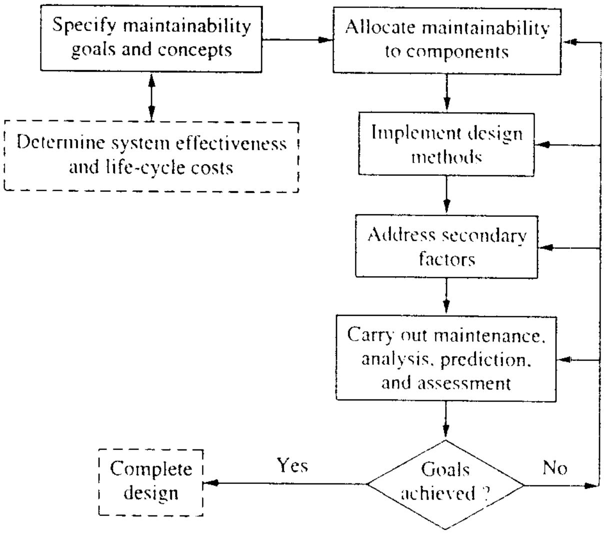
## *Quantifiable measures:*

- Mean time to repair
- Median time to repair
- Maximum time in which a certain percentage of the failures must be repaired
- Mean system downtime
- Mean time to restore
- Maintenance work hours per operating hour

# Design for Maintainability:

**(Ebeling, pp 219-221)**

## Design process determines conditions under which maintenance and repair are to be accomplished

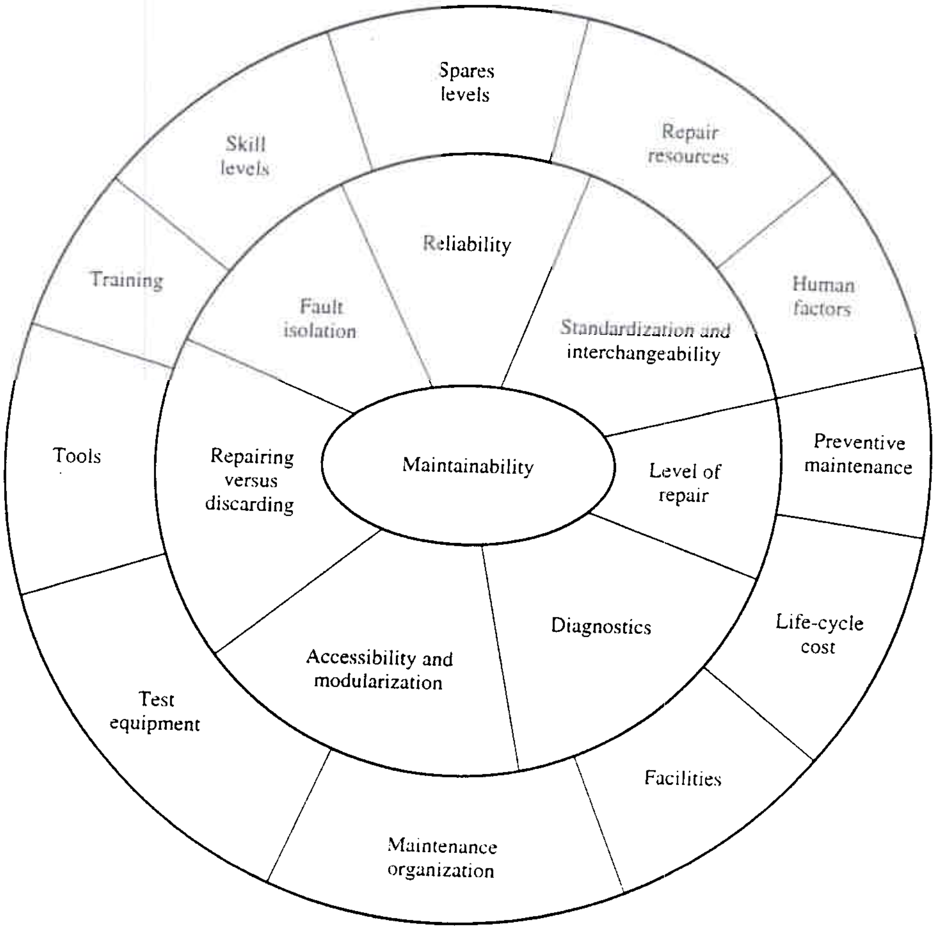

Specify maintainability goals and concepts
Allocate maintainability to components
Determine system effectiveness and life-cycle costs
Implement design methods
Address secondary factors
Carry out maintenance, analysis, prediction, and assessment
Complete design
Yes
Goals achieved ?
No

- **Which units are to be repaired rather than discarded and replaced**
- **Preventive maintenance schedule and associated tasks**
- **For repairable units, the level of repair (such as local, service center, or factory) for each failure mode**
- **For each repair task, the required skill levels, tools, test equipment, and technical manuals**
- **The number of repair channels and spare parts (inventory)**

# Design for Maintainability:

(Ebeling, p 223)

## Maintainability Design Features



# Design for Maintainability:

## *Design Methods*

(Ebeling, pp 225-227)

### 1 ~ Fault Isolation and Self-Diagnostics

- Diagnostics is process of locating the fault at the level in which restoration may be accomplished

- Diagnosis of failure with identification of fault is major task in repair process; often the longest task and the one having greatest variability in task times

### 2 ~ Parts Standardization and Interchangeability

- Standardization results in reducing to a minimum the range of parts that must be maintained and stocked

- Interchangeability is a design policy that allows specified parts to be substituted within an assembly for any like part; requires both functional and physical substitutability

# Design for Maintainability:

## *Design Methods*

(Ebeling, pp 227-229)

### 3 ~ Modularization and Accessibility

- Modularization (packaging of components in self-contained functional units) facilitates maintenance
- Design for accessibility is concerned with the configuration of the hardware down to the discard (replacement) level

### 4 ~ Repair versus Replacement

- Indenture level is level at which it is no longer economical to repair the failed unit; instead the failed unit is discarded and replaced with a new one
- Decision criterion is most often an economical one

# Data Classification:

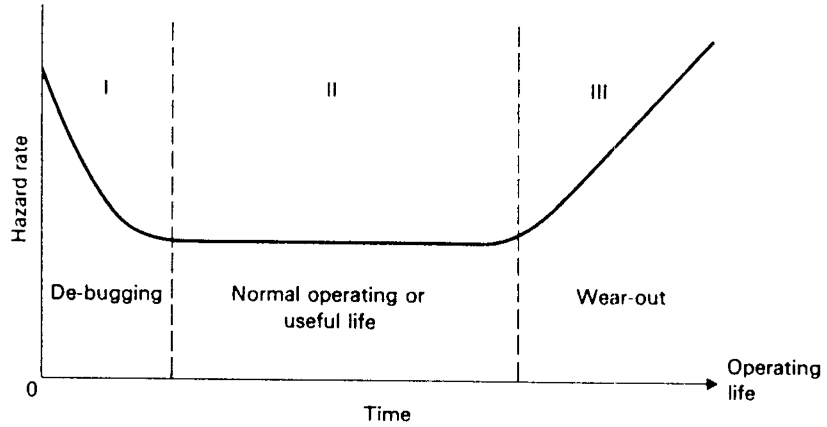
## Three classifications typically used, based on when the failure occurs

- *infant mortality*
- *useful life*
- *wearout*

## Bathtub curve: x = time *and* y = hazard rate

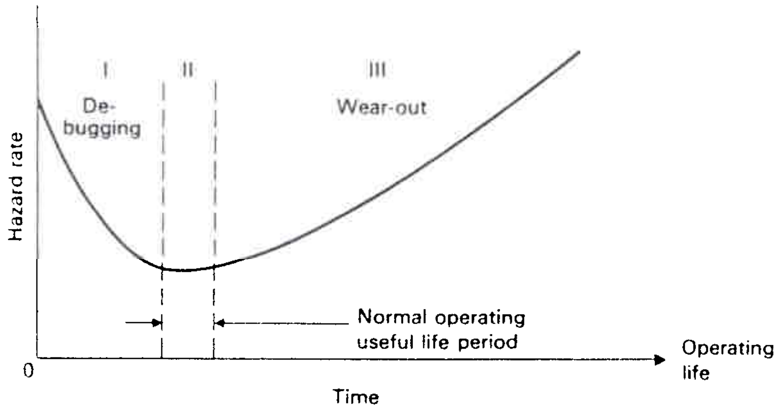
**typical electronic component:**

**(Billinton and Allan, p 166)**



**typical mechanical component:**

**(Billinton and Allan, p 166)**



# Availability:

(Ebeling, pp 254-261)

*probability that a system or component is performing its required function at a given point in time or over a stated period of time when operated and maintained in a prescribed manner*

## Availability measures include:

- Inherent Availability
- Achieved Availability
- Operational Availability
- Generalized Operational Availability
- Total System Availability

# Availability Measures:

**Inherent Availability**

design parameter based on failure distribution and repair-time distribution

**Achieved Availability**

based on distributions for mean time between maintenance and mean system maintenance downtimes

**Operational Availability**

based on distributions for mean time between maintenance and mean time for all unscheduled downtimes (e.g., supply delays)

**Generalized Operational Availability**

based on distributions for mean time between maintenance and mean time for all ready times

**Overall System Availability**

Models similar to those for System Reliability; Markov processes typically required

# Software:

## *Software Reliability*

(Blanchard, pp 115-116)

probability of failure-free operation of a software component or system in a specified environment for a specified time, where a failure is an unacceptable departure of program operation from program requirements

## *Software Reliability Measures of Quality*

(SMDC, Sec 15)

Correctness

= Correct Normal Transactions

÷ Normal Transactions

Robustness

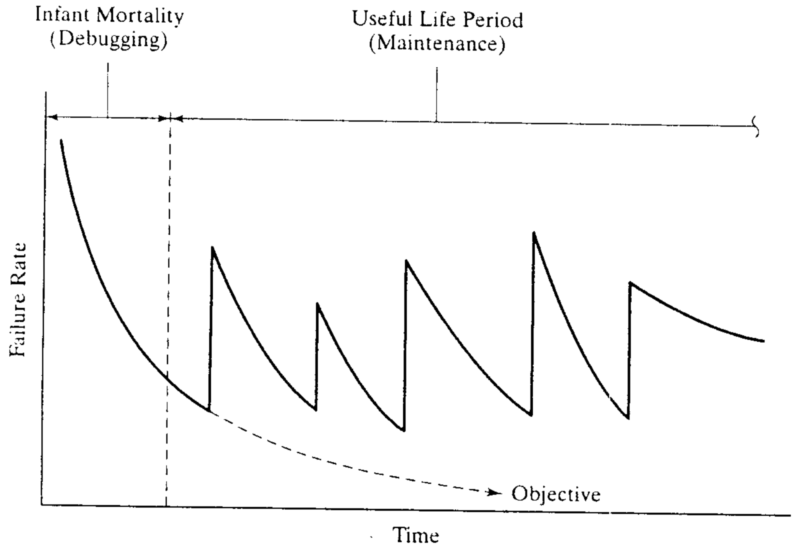
= Correctly Handled Abnormal Transactions

÷ Normal Transactions

# Software:

## *Software (incl. maintenance) Hazard Function*

**(Blanchard, p 53)**



## *Software Maintainability Measures of Quality*

**(SMDC, Sec 15)**

**Correctability**

**= (Module Development Cost - Module Correction Cost) ÷ (Module Development Cost)**

**Editability**

**= (Development Cost - Editing Cost) ÷ (Editing Cost)**

# References:

Billinton, Roy and Ronald N. Allan, Reliability Evaluation of Engineering Systems (Plenum, 1992)

Blanchard, Benjamin S., Logistics Engineering and Management (Pearson Prentice Hall, 2004)

Ebeling, Charles E., An Introduction to Reliability and Maintainability Engineering (McGraw-Hill, 1997)

Sage, Andrew P. and William B. Rouse, ed, Handbook of Systems Engineering and Management (Wiley-Interscience, 1999)
- Levis, Alexander H., System Architectures
- Pecht, Michael, Reliability, Maintainability, and Availability

SMDC (Systems Management & Development Corp), The Systems Engineering Course (SMDC, 2000)