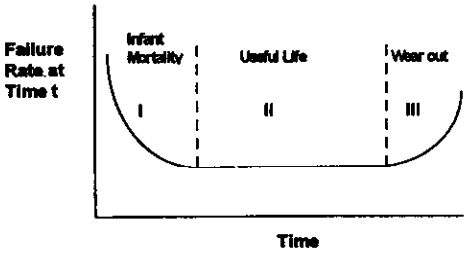
Principles of Nuclear Safety

Module 6

Reliability Concepts

Slide 1

Bathtub Curve



Slide 2

Useful Life and Preventive Maintenance

- A component's failure rate is lowest during its useful life era
- For maximum reliability, components must be operated only during their useful lives
- Therefore, ageing components are replaced through preventive maintenance programs, before the end of their useful lives, even though they have not yet failed

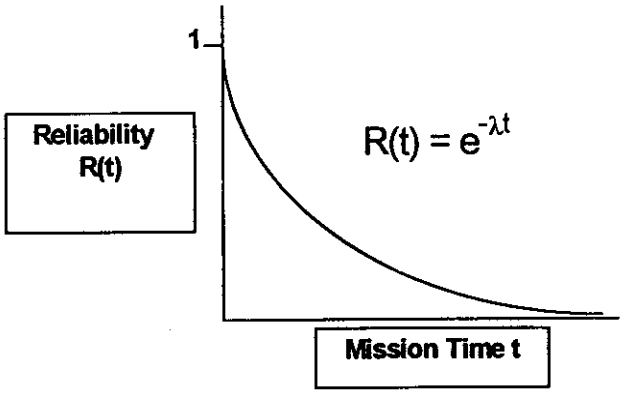
Slide 3

Reliability versus Availability

- *Reliability, R(t),* is the probability that a component or system will perform its design function for a specified mission time, under given operating conditions.
- Unreliability, U = 1 - R
- The concepts of reliability and mission time apply to *active* (continuously operating) systems

Slide 4

General Reliability Function



Slide 5

Availability

- *Availability, A,* is the fraction of time a component or system is available to perform its intended purpose
- *Unavailability, Q,* is the fraction of time a component or system is unavailable
- Q = 1 - A
- The concept of availability applies to *poised* systems

Slide 6

Unavailability of Poised Systems

- The unavailability of a poised system is measured by testing it periodically
- If λ is the number of failures per annum,
  T is the test period in years, and
  r is the repair time in years, then

$$Q = \lambda(T/2 + r)$$

- safety systems are tested often enough to demonstrate compliance with design availability requirements

Reliability of Air, Water & Power

- Air, water and power supplies are *essential* to process monitoring, control, and protection, whether unit is at power or shut down.
- class IV power is required to support operation at power, but not shut down
- class III power is required to cool the fuel during shutdown, and is therefore higher reliability than class IV power

Class II and I Electrical Power

- required for vital monitoring, control and equipment protection functions
- considered uninterruptable
- normally supplied by class III, but backed up by battery banks designed to last for about 40 minutes

Slide 9

Instrument Air Reliability

- compressors powered by class III
- redundant distribution headers, which can be independently isolated
- local receivers
- key control valves fail safe on loss of instrument air

Slide 10

Design Strategies for Improving System Reliability

- Redundancy
- Diversity
- Independence
  - odd and even power
  - group I and II systems
  - channelization of special safety systems
- Fail safe

Redundancy

Redundancy is the provision of components or capacity in excess of 100% of system requirements, such that failures of excess components or capacity do not disable the system function.

- eg, two 100% capacity pumps placed in parallel

Diversity

Diversity is variety in design, manufacture, operation and maintenance of redundant components or systems for the purpose of reducing unavailability due to common cause effects, such as design or manufacturing flaws, and O&M errors.

- eg, SDS1 achieves emergency shutdown by dropping absorber rods into core under gravity, whereas SDS2 injects liquid absorber under pressure. Diverse design principles, construction, and O&M procedures protect against unforeseen failure modes and human error.

Independence

Components or systems are said to be ***independent*** if a failure in one cannot cause related failures in the others. ***Independence*** is achieved by having no shared components or common services (functional separation), and by physical separation

- eg, two 100% pumps, one supplied by odd power, the other by even

Common Mode Failures

- ***Common mode*** failures are multiple failures resulting from a single initiating cause
  - eg, contamination of fuel supply to more than one standby generator
- Tornado, earthquake, fire, flood, plane crash, turbine missiles, and sabotage are common mode incidents

Fail Safe

- A component or system is ***fail safe*** if it performs its required function immediately and automatically as a result of the failure--ie, the failure does not contribute to unavailability
  - eg, shutoff rods drop into core on loss of electrical power to clutches
- In some cases there is no fail safe state
  - eg, HT relief valves, circuit breakers supplying vital loads,...

Odd and Even Equipment

- Electrical power supplies are designated as *odd* or *even*
- *odd* and *even* supplies are independent
- Typically, half the equipment providing a function is supplied by an even source, and half from an odd source, so that the effect of one power supply failure is limited to either *odd* or *even* equipment. This eliminates a *cross-link failure mode*.

Slide 17

Seismic Qualification

- Sufficient safety related systems seismically qualified (ie, remain operable during and after design basis earthquake) to provide:
  - freedom from seismically-induced LOCA
  - control, cool and contain functions
- Eliminates *design basis earthquake* as *common failure mode.*
  - A seismic event acts on all equipment regardless of other reliability design strategies--separation, diversity, etc.

Slide 18

Environmental Qualification

- Makes failures of mitigating equipment independent of certain major process failures, which impose harsh operating environments
  - eg, ECI and Containment equipment, which might otherwise fail due to high temperature, high radiation, and wetting under LOCA conditions
- Sufficient safety related systems should be environmentally qualified to ensure capability to control, cool and contain after such incidents

Group I and II Systems

To cater to *common mode* events such as fire, turbine missiles, earthquake, adverse environment, and plane crash, systems are physically separated into group I and group II (seismically qualified), each having the following capabilities:

- reactor shutdown and hold-down capability
- decay heat removal
- containment of radioactivity
- post-accident monitoring and control

Channelization

- ***Channelization*** is the provision of more than one independent means of transmitting energy or signals
- Advantages of 2/3 or 3/4 channel initiation logic relative to single-channel system:
  - channel redundancy increases system availability
  - permits on-line testing and maintenance
  - reduced vulnerability to spurious system operation

Reasons to test Special Safety Systems

- to discover and correct failures, thus limiting system unavailability
- to obtain failure rate, so that preventive maintenance program can be optimized
- to demonstrate compliance with Siting Guide unavailability requirements
- to obtain site specific reliability data for predicted reliability calculations, and for design modifications

Reasons to Limit Test Frequency

- excessive testing can cause wear-out failures
- testing itself contributes to system unavailability if component cannot be put into safe state for test
- risk of human error leaving system in compromised state
- risk of forced outage due to human error or random equipment failure
- divert resources from other surveillance activities important to reactor safety