Basics of Traditional Reliability

Where we are going

- Basic Definitions
- Life and times of a Fault
- Reliability Models
- N-Modular redundant systems

Definitions

- **RELIABILITY:**
  SURVIVAL PROBABILITY
  - When repair is costly or function is critical

- **AVAILABILITY:**
  THE FRACTION OF TIME A SYSTEM MEETS ITS SPECIFICATION
  - When service can be delayed or denied

- **REDUNDANCY:**
  EXTRA HARDWARE, SOFTWARE, TIME

- **FAILSAFE:**

  SYSTEM FAILS TO A KNOWN SAFE STATE
  - i.e. All red traffic signals

Stages in System Development

STAGE	ERROR SOURCES	ERROR DETECTION
Specification & design	Algorithm Design Formal Specification	Simulation Consistency checks
Prototype	Algorithm design Wiring & assembly Timing Component Failure	Stimulus/response Testing
Manufacture	Wiring & assembly Component failure	System testing Diagnostics
Installation	Assembly Component failure	System Testing Diagnostics
Field Operation	Component failure Operator errors Environmental factors	Diagnostics

Cause-Effect Sequence and Duration

- **FAILURE:** **component does not provide service**
- **FAULT:** **a defect within a system**
- **ERROR:** **a deviation from the required operation of the system or subsystem (manifestation of a fault)**

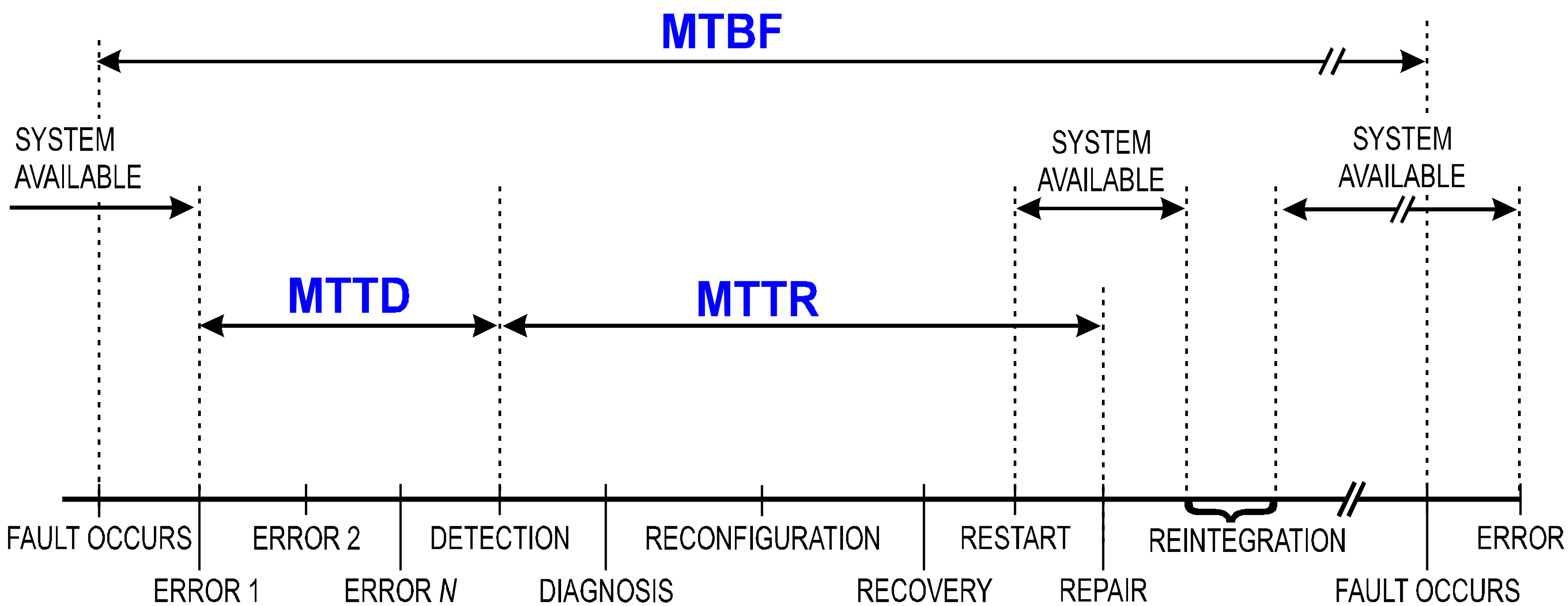
- **DURATION:**
  - Transient- design errors, environment
  - Intermittent- repair by replacement
  - Permanent- repair by replacement

Basic Steps in Fault Handling

- **Fault Confinement**
- **Fault Detection**
- **Fault Masking**
- **Retry**
- **Diagnosis**
- **Reconfiguration**
- **Recovery**
- **Restart**
- **Repair**
- **Reintegration**

MTBF -- MTTD -- MTTR

$$\textbf{Availability} = \frac{\text{MTBF}}{\text{MTBF} + \text{MTTR}}$$

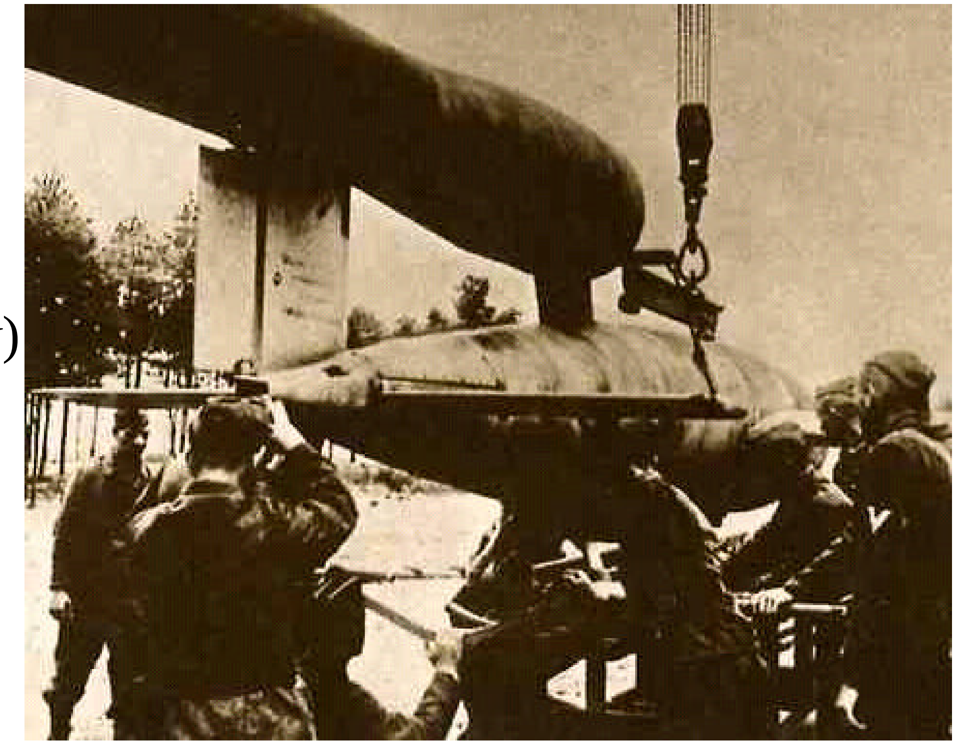


A Scenario for on-line detection and off-line repair. The measures -- MTBF, MTTD, and MTTR are the average times to failure, to detection, and to repair.

First predictive reliability models - Von Braun

Wernher Von Braun - German Rocket Engineer, WWII

- V1 was 100% Unreliable
- Fixed weakest link - still unreliable



Eric Pieruschka - German Mathematician

- 1/x^n - for identical components
- Rs=R1 x R2 x … x Rn (Lusser’s law)

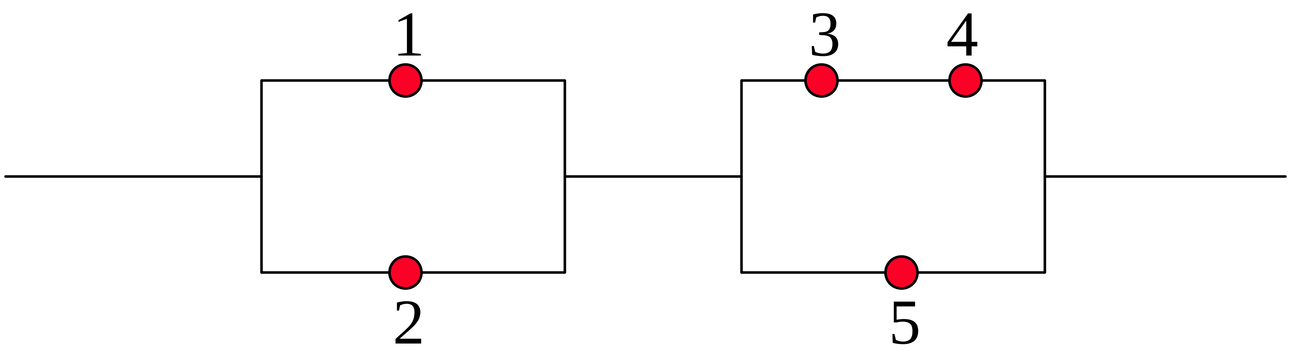
Serial Reliability

$$R(t) = \prod_{i=1}^{N} R_i(t)$$

Thus building a serially reliable system is extraordinarily difficult and expensive.

For example, if one were to build a serial system with 100 components each of which had a reliability of .999, the overall system reliability would be $0.999^{100} = 0.905$

Reliability of a system of components



$$\Phi(x) = \begin{cases} 1, \text{ functioning when state vector x} \\ 0, \text{ failed when state vector x} \end{cases}$$

$$\Phi(x) = \max(x_1,x_2)\max(x_3x_4,x_5)$$

Minimal path set: minimal set of components whose functioning ensures the functioning of the system

{1,3,4} {2,3,4} {1,5} {2,5}

Parallel Reliability

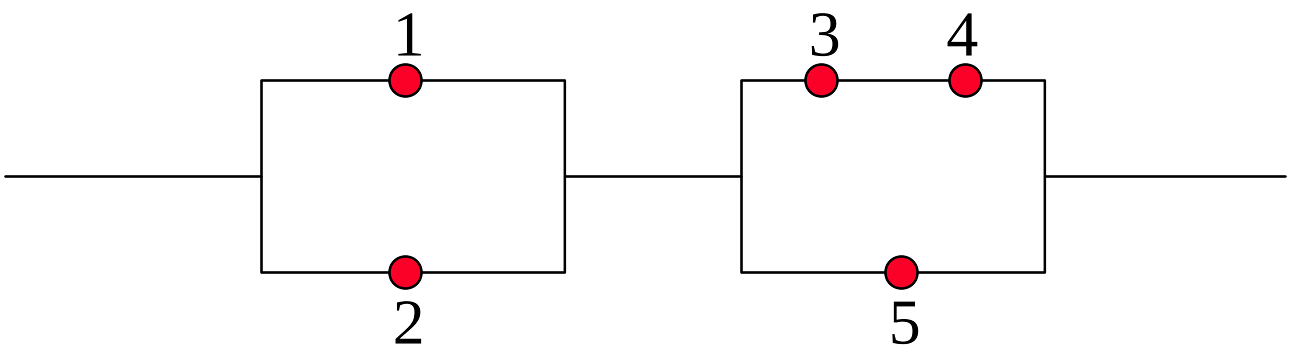
$$R(t) = 1 - \prod_{i=1}^{N} [1 - R_i(t)]$$

Consider a system built with 4 identical modules which will operate correctly provided at least one module is operational. If the reliability of each module is .95, then the overall system reliability is:

$1-[1-.95]^4 = 0.99999375$

In this way we can build reliable systems from components that are less than perfectly reliable - for a cost.

Parallel - Serial reliability



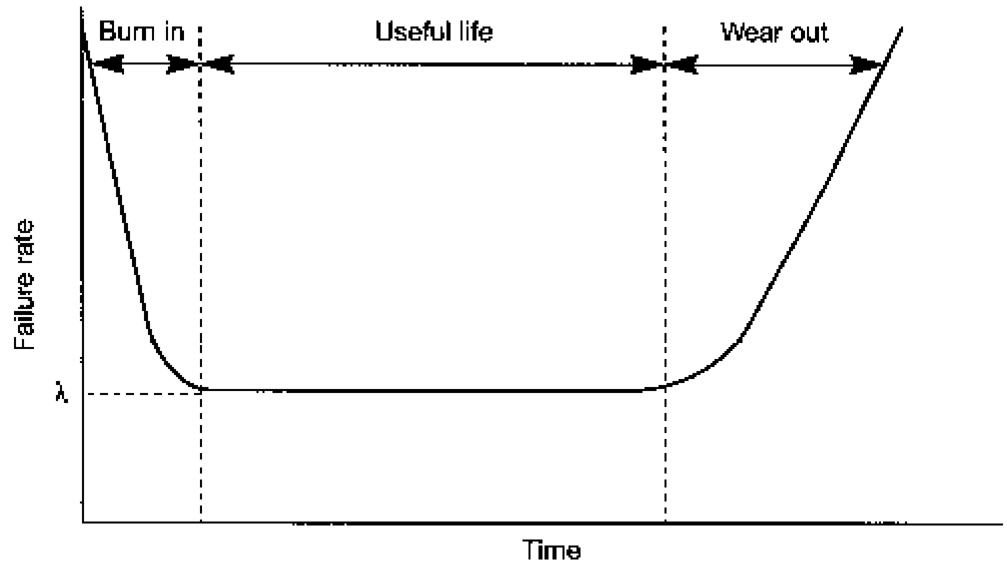
Total reliability is the reliability of the first half, in serial with the second half.

Given that R1=.9, R2=.9, R3=.99, R4=.99, R5=.87

$$Rt=[1-(1-.9)(1-.9)][1-(1-.87)(1-(.99*.99))] =.987$$

Component Reliability Model

But… It isn't quite so straight forward...



During useful life components exhibit a constant failure rate λ. Accordingly, the reliability of a device can be modeled using an exponential distribution.

$$R(t) = e^{-\lambda t}$$

N-Modular redundant systems

Redundant system implementations typically use a voting method to determine which outputs are correct. This voting overhead means that true parallel module reliability is typically only approached

$$R_{M.of.N}(t) = \sum_{i=0}^{N-M} \left(\frac{N!}{(N-i)!i!}\right) R_m^{N-i}(t)[1 - R_m(t)]^i$$

Consider a 5 module system requiring 3 correct modules, each with a reliability of 0.95 (example 7.9).

$$R_{3.of.5}(t) = \sum_{i=0}^{2} \left(\frac{5!}{(5-i)!i!}\right) R_m^{5-i}(t)[1 - R_m(t)]^5$$

$$= R_m^5(t) + 5R_m^4(t)[1 - R_m(t)] + 10R_m^3(t)[1 - R_m(t)]^2$$

$$= 10(0.95)^3 - 15(0.95)^4 + 6(0.95)^5$$

$$= 0.9988$$

Conclusions

- The common techniques for fault handling are fault avoidance, fault detection, masking redundancy, and dynamic redundancy.

- Any reliable system will have its failure response carefully built into it, as some complementary set of actions and responses.

- System reliability can be modeled at a component level, assuming the failure rate is constant (exponential distribution).

- Reliability must be built into the project from the start.