Reliability of Technical Systems

Main Topics

1. Short Introduction, Reliability Parameters: Failure Rate, Failure Probability, etc.
2. Some Important Reliability Distributions
3. Component Reliability
4. Introduction, Key Terms, Framing the Problem
5. System Reliability I: Reliability Block Diagram, Structure Analysis (Fault Trees), State Model.
6. System Reliability II: State Analysis (Markovian chains)
7. System Reliability III: Dependent Failure Analysis
8. Data Collection, Bayes Theorem, Static and Dynamic Redundancy
9. Advanced Methods for Systems Modeling and Simulation (Petri Nets, network theory, object-oriented modeling)
10. Software Reliability, Fault Tolerance
11. Human Reliability Analysis
12. Case study: Building a Reliable System

Data Collection

- **Specific Data**

  Available data for a specific unit same as the unit being subject of analysis; its validity hence is provided.

  This kind of data is ideal for a reliability analyis. Nevertheless, often there is a lack of it in practice.

- **Generic Data**

  Such data often are given in publications for „similar“ units; the validity of this data is not given per se.

  Application to other units is questionable. However, convenient increase of the data basis

- **„expert judgement“**

  subjective judgement of an expert regarding the unit behavior.

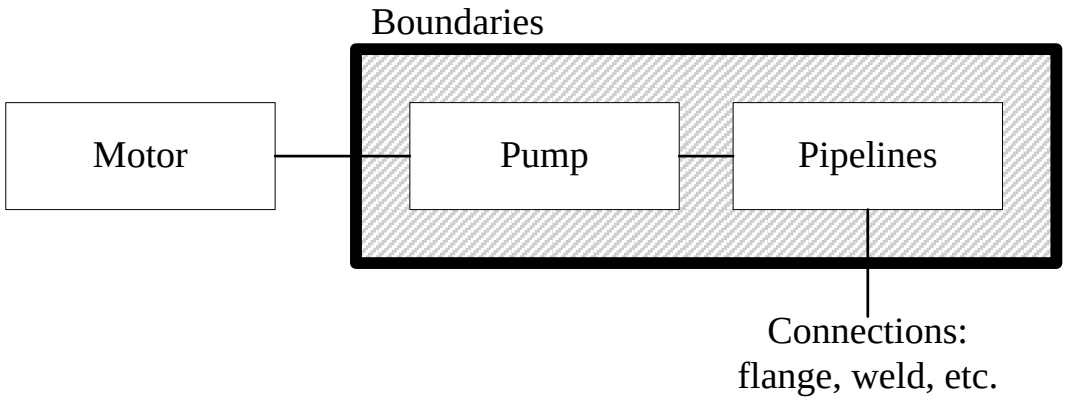
  Rather inappropriate for a reliability analysis, but often the only available data source.

Data Collection

Assumptions

Characterizing a unit / component

- Ensure statistical **similarity** between database and analysis
  - Construction
  - Conditions, i.e. process parameters (pressure, temperature), Medium, Environment u.a.
  - Operational conditions, e.g. active versus stand-by
- Definition of a failure
- Definition of an observation period
- Definition of the boundary elements.



Data Collection

Plant specific data sources

Current basic documents are business documents (BU), i.e. damage reports, repair orders, etc.

- Loss of species, causes, impacts are rarely held

- BU are usually not designed for reliability data function, must represent at least 90% of all failures (events).

Bayes Theorem

Conditional Probability

- It is important to compute the probability of an event A given that another event B has occurred, which is called *conditional probability* of A given B

$$P(A|B) = \frac{P(A \cap B)}{P(B)}$$

Where P(A|B) gives the probability of the event A not on the entire possible sample space Ω, but on the sample space relative to the occurrence of B

- Event A is said to be *statistically independent* from event B if P(A|B)=P(A)

- Statistical independence should not be confused with mutual exclusivity ($X_A X_B = 0$), which represents a logical dependence: knowing that A has occurred, guarantees that B cannot occur

Bayes Theorem

Conditional Probability : Exercise Example

There are two streams flowing past an industrial plant. The dissolved oxygen, DO, level in the water downstream is an indication of the degree of pollution caused by the waste dumped from the plant. Let A denote the event that stream a is polluted, and B denote the event that stream b is polluted. From measurement taken on the DO level of each stream over the last year, it was determined that in a given day

$P(A) = 2/5$ and $P(B) = 3/4$

and the probability that at least one stream will be polluted in any given day is $P(A \cup B) = 4/5$

Q1: Determine the probability that stream a is also polluted given that stream b is polluted.

Q2: Determine the probability that stream b is also polluted given that stream a is polluted.

Bayes Theorem

Conditional Probability : Exercise - Solution

We have

$$P(A \cup B) = P(A) + P(B) - P(A \cap B)$$

The probability that both streams are polluted

$$P(A \cap B) = P(A) + P(B) - P(A \cup B) \quad = (2/5)+(3/4)-(4/5)=7/20$$

For Q1:

$$P(A|B) = \frac{P(A \cap B)}{P(B)} = \frac{7/20}{3/4} = 0.46$$

For Q2:

$$P(B|A) = \frac{P(A \cap B)}{P(A)} = \frac{7/20}{2/5} = 0.875$$

Bayes Theorem

Theorem of Total Probability

- Consider a partition of the sample space Ω into n mutually exclusive and exhaustive events E_j , j = 1,2,…..,n.

$$E_i \cap E_j = 0 \ \forall i \neq j \qquad \bigcup_{j=1}^{n} E_j = \Omega$$

- Given any event A in Ω, its probability can be computed in terms of the partitioning events E_j (j = 1,2,…..,n), and conditional probabilities of A on these events :

$$P(A) = P(A|E_1)P(E_1) + P(A|E_2)P(E_2) + \cdots + P(A|E_n)P(E_n)$$

Bayes Theorem

Bayes Theorem

- What is the probability that event E_j has occurred if there is the evidence that event A has occurred ?

$$P(E_j|A) = \frac{P(A|E_j)P(E_j)}{P(A)} = \frac{P(A|E_j)P(E_j)}{\sum_{j=1}^{n} P(A|E_j)P(E_j)}$$

- Equation above updates the *prior probability* value $P(E_j)$ of event E_j to the *posterior probability* value $P(E_j|A)$ where P(A) can be computed by applying the theorem of *total probability.*

$$P(A) = P(A|E_1)P(E_1) + P(A|E_2)P(E_2) + \cdots + P(A|E_n)P(E_n)$$

Bayes Theorem

Bayes Theorem : Exercise Example

Same components are purchased from 3 suppliers (S1, S2, S3) in quantities of 1000, 600, 400 pieces, respectively. The probabilities for one component to be defective are 0.006 for S1, 0.02 for S2, and 0.03 for S3. All the components are stored in a common container disregarding their source.

Q1. What is the probability that one component randomly selected from the stock is defective ?

Q2. Let one component as selected in previous question be defective. What is the probability that it is from S1 ?

Bayes Theorem

Bayes Theorem : Exercise Solution

Q1: Pr(the selected component is defective) =

$$\frac{1000}{2000} \times 0.006 + \frac{600}{2000} \times 0.02 + \frac{400}{2000} \times 0.03 = 0.015$$

Q2: Pr (component from S1 | component is defective)

Using Bayes Theorem equation

Pr(component from S1 | component is defective) =

$$\frac{\Pr(\text{component from S1}) \times \Pr(\text{comonent is defective} \mid \text{component from S1})}{Pr(component\ is\ defective)} =$$

$$\frac{(1000/2000) \times 0.006}{0.015} = 0.2$$

Redundancy

Redundancy

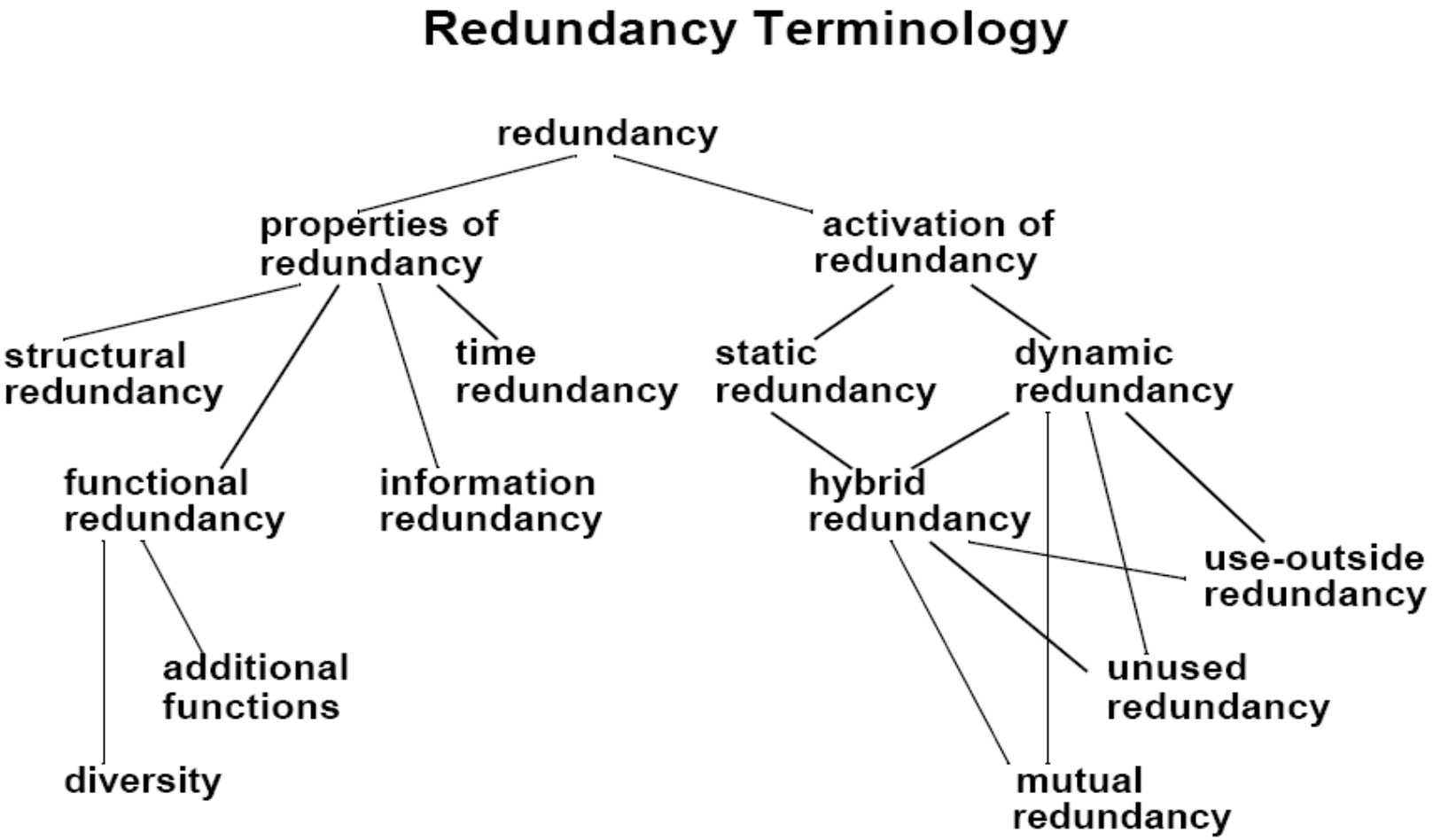
Existence of more than one means for performing a required function in item.

• For hardware, distinction is made between *active* (hot, parallel), *warm* (lightly loaded), and *standby* (cold) redundancy.

• Redundancy does not necessarily imply a duplication of hardware, it can be implemented, for example, by coding or by software.

•To avoid common mode failures, redundant elements should be realized independently from each other.

Redundancy


Redundancy Terminology
redundancy
properties of redundancy
activation of redundancy
structural redundancy
time redundancy
static redundancy
dynamic redundancy
functional redundancy
information redundancy
hybrid redundancy
use-outside redundancy
additional functions
unused redundancy
diversity
mutual redundancy

Redundancy

The properties of redundancy characterize various issues of redundancy rather than distinguishing different types of redundancy:

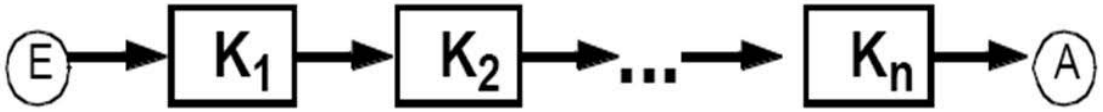
- The extension by extra components in the structure and functions model.
- The extension by extra functions in the structure and functions model. These extra functions can be different from the already existing ones (additional functions) or satisfy the same specification by a different implementation (diversity).
- The additional information to be stored, transferred and processed.
- The additional time requirements.

Redundancy is either used from the beginning of the system operation (active / hot) or activated on fault occurrence (standby / cold) or used in a combination thereof (lightly loaded).

Redundancy

Non-Redundant System

Serial system:



Minimal cuts: $\sigma_1 = \{K_1\}, \quad \sigma_2 = \{K_2\}, \quad \ldots, \quad \sigma_n = \{K_n\},$

System function probability: $\varphi(S) = 1 - \varphi(\overline{K_1} \vee \ldots \vee \overline{K_n}) = \ldots$

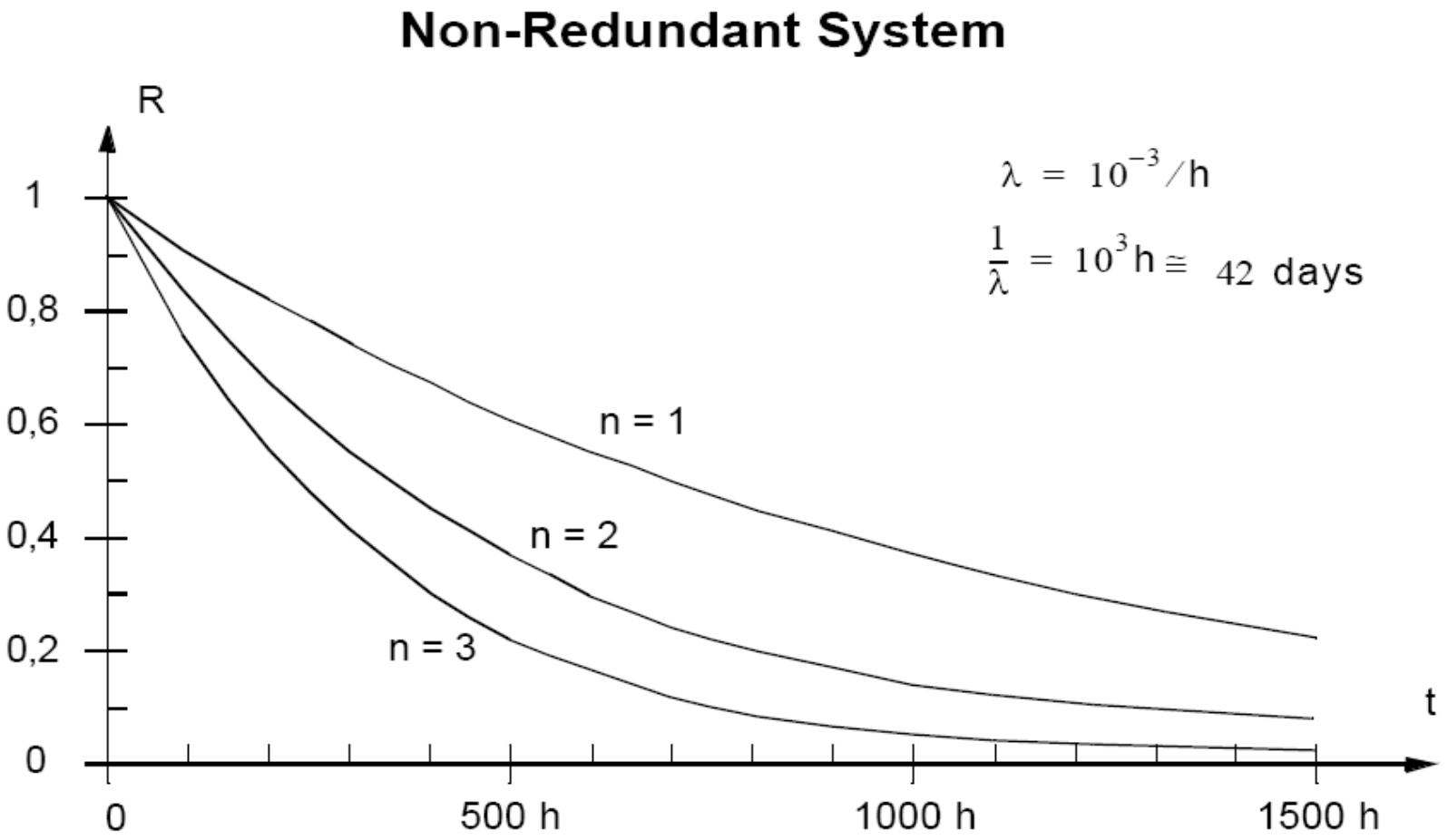
$$1 - \varphi(\overline{K_1 \wedge \ldots \wedge K_n}) = 1 - \bar{\varphi}(K_1 \wedge \ldots \wedge K_n) = \varphi(K_1 \wedge \ldots \wedge K_n) = \prod_{i=1}^{n} \varphi(K_i)$$

Reliability:

Let be for all components $\varphi(K_i) = R_i(t) = e^{-\lambda t}$.

Then we obtain for the system: $\varphi(S) = R_S(t) = e^{-n\lambda t}$ MTTF (S) = $\frac{1}{n\lambda}$

Redundancy


Non-Redundant System
R
1
0,8
0,6
0,4
0,2
0
n = 1
n = 2
n = 3
t
0
500 h
1000 h
1500 h
$\lambda = 10^{-3}/\mathrm{h}$
$\frac{1}{\lambda} = 10^{3}\,\mathrm{h} \cong 42$ days

Redundancy

Supposing a system consists of components which will not fail with a probability of 99% (p=0.99) and which are connected in series. Then the probability that the entire system will not fail changes with the number of components as follows:

10 components lead to a survival probability of 90.40%

20 components lead to a survival probability of 81.71 %

30 components lead to a survival probability of 73.86 %

40 components lead to a survival probability of 66.76 %

50 components lead to a survival probability of 60.35 %

100 components lead to a survival probability of 36.40 %

Static Redundancy: n-out-of-m system

- The system is faultless, if at least n out of m existing components are faultless.

- If n=1, complete redundancy occurs (in parallel), and if n=m, the m components are, in effect, in series.

- The reliability may be obtained from the binomial probability distribution.

- If R is reliability of each independent trial, then the probability of n or more successes among the m components may be represented as:

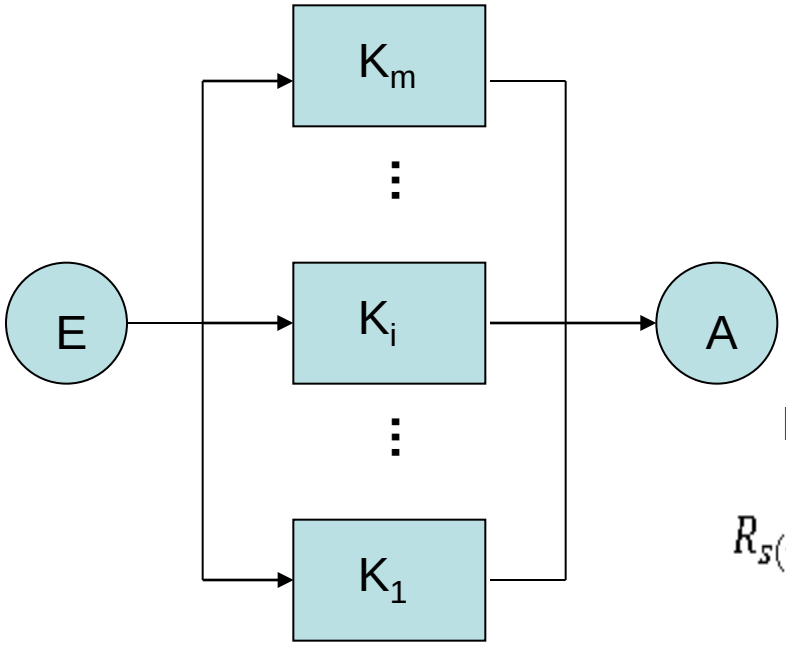
$$R_s = \sum_{x=n}^{m} \left[\binom{m}{x} R^x (1-R)^{m-x} \right]$$

$$\binom{m}{x} = \frac{m!}{x!(m-x)!}$$

$$\text{MTTF} = \int_0^\infty R_s(t)\,dt$$

Static Redundancy: n-out-of-m system

Parallel System: 1-out-of-m system



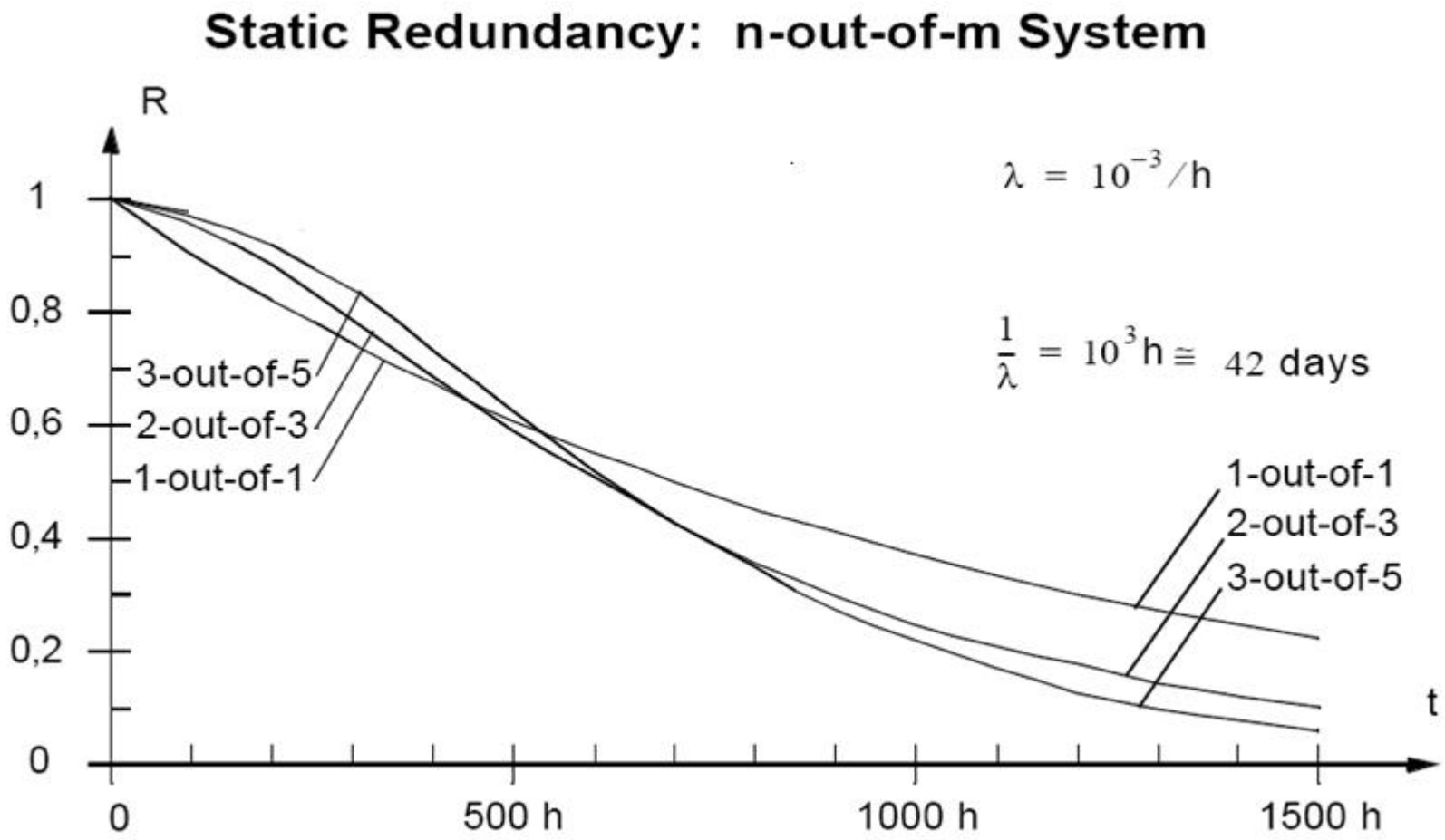
Reliability of the parallel system :

$$R_{s(parallel)} = \sum_{x=1}^{m} \left[\binom{m}{x} R^x (1-R)^{m-x} \right]$$

Compare with reliability of the series system (non redundancy):

$$R_{s(series)} = \sum_{x=m}^{m} \left[\binom{m}{m} R^x (1-R)^{m-x} \right] = R^m$$

Static Redundancy: n-out-of-m system



Case Study

Learning from Deficits: Gulf Oil Spill and Breach of Basic Principles

March – April 2010

- Oil rig in preparation to move to another job
- Temporarily plug and cap the well with cement
  - Rise in pressure from the well that suggested the cement was not holding
  - First test showed large abnormality, second test was misread and declared as safe

April 20

- Jump in pressure from oil and gas rising in the well
- Methane expanded on the rig without given warnings
  - All applications in operation, including those dangerous to ignite the methane
- Explosion on rig, chaotic conditions to evacuate the rig, weak clear directives
- Closing of blowout preventer failed
- Consequences
  - 11 victims, 17 injured
  - ~780 x10^3 m^3 oil spilled in ocean (2 Super-tankers)

InTech, August 10

Learning from Deficits: Gulf Oil Spill and Breach of Basic Principles

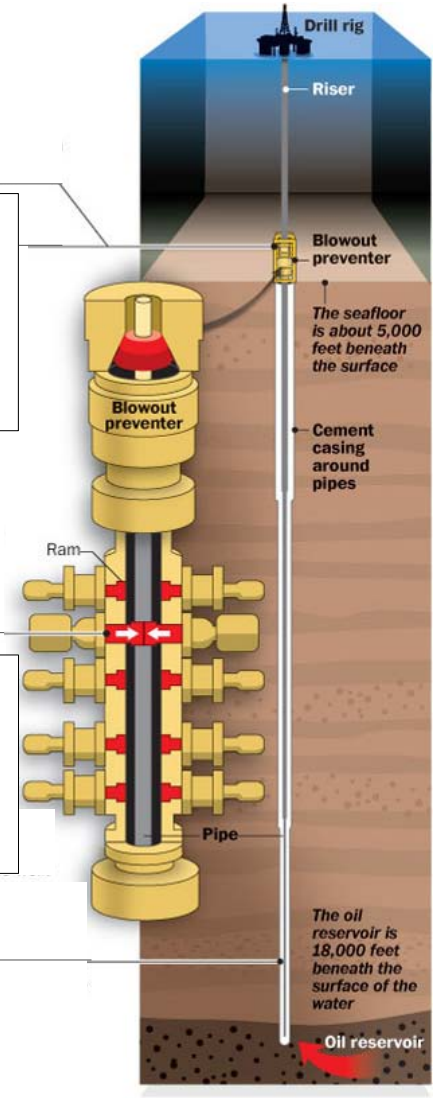
A dead battery in the BOP's „brain" which gives pressure readings and controls other functions in the giant stack of valves.

A leak in the hydraulic system that sends emergency power to **rams,** valves that are supposed to close off the space around the pipe.

The shear ram, the BOP's valve of last resort, wasn't strong enough to cut through joints in the pipe. Those joints account for about 10 percent of the pipe's length.

Several "unexpected" modifications to the BOP, including **test ram** in place of a real one. Schematics didn't match the actual device.

The cement seal around the casing pipes in the well failed pressure tests before the explosion - gas may have been building up in the well.



Washington Post, May 13

References:

- Zio, Enrico. (2007) *An Introduction To the Basics of Reliability and Risk Analysis. World scientific Publishing Co.*
- Birolini, Alessandro. (2007) Reliability Engineering: Theory and Practice *(5th edition). Springer-Verlag: Berlin*

Practical Problems of the Reliability Experiment

- What is a **realistic** stress ?
- Does a realistic stress of **software** exist by some input data ?
- Can we choose an increased stress for a **worst case estimation** ?
- **Which function** should be required from the components under test ?
- Do the **tests** cover all malfunctions ?
- What is the cost of this component **destroying** experiment ?
- How can the **number of components** under test be minimized ?
- **Duration** of the reliability experiment ?
- Are there techniques for a **speed-up** of the experiment ?

Malfunctions of an unit (failure modes)

Functions	**Types of failure**
Closing	Fails open Only partly closed
Opening	Fails closed Only partly opened
Remain closed	Opens completely Partly opens
Remain opened	Closes completely Partly closes

Techniques to speed up the experiment

- Sequential test
- Accelerated test
- Extrapolation

Sequential Test (I)

If the actual failure rate λ does not exceed the limit λ_1 ($\lambda < \lambda_1$) with high probability w_1, the components are to be accepted.

On the other hand, if λ does not under-run the limit λ_2 ($\lambda > \lambda_2$) with high probability w_2, the components are to be rejected.

Given: λ_1, sample size n, acceptance threshold k, time of experiment t.

Let X be the number of failures (Poisson distributed) within the time interval [0, t].

$$p(X \leq k) = \sum_{i=0}^{k} \frac{(n \cdot \lambda_1 \cdot t)^i}{i!} e^{-n \cdot \lambda_1 \cdot t}$$

Sequential Test (II)

For given probabilities α and β is true:

	For λ= λ1	For λ= λ2
Probability of acceptance	1- α	β
Probability of rejection	α	1- β

Accept decision if:

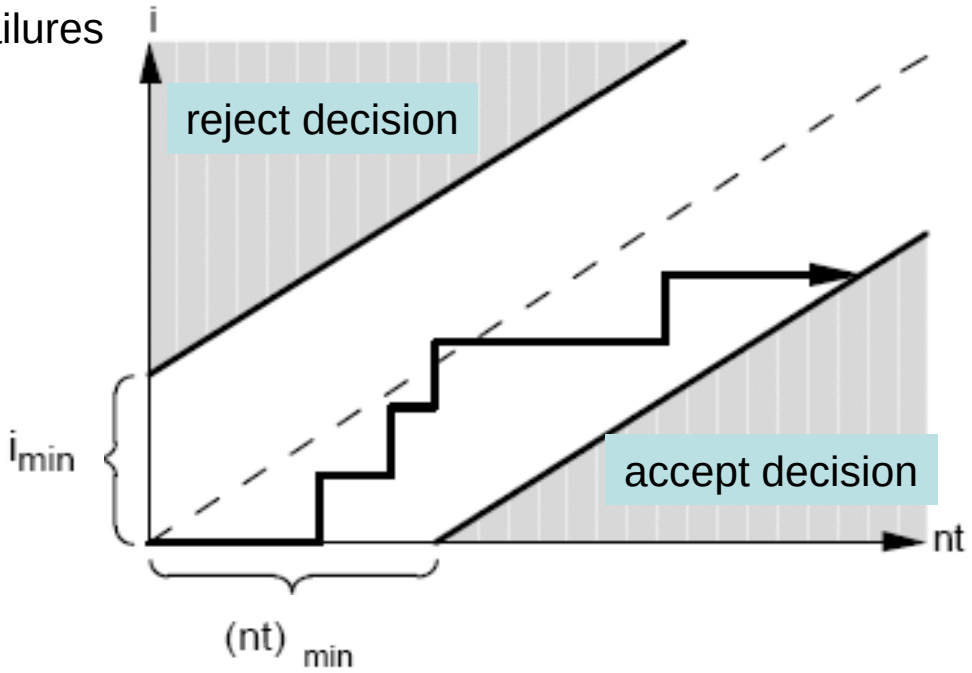
$$i \leq \frac{\ln \frac{\beta}{1-\alpha}}{\ln \frac{\lambda_2}{\lambda_1}} + \frac{\lambda_2 - \lambda_1}{\ln \frac{\lambda_2}{\lambda_1}} \cdot n \cdot t$$

Reject decision if:

$$i \geq \frac{\ln \frac{1-\beta}{\alpha}}{\ln \frac{\lambda_2}{\lambda_1}} + \frac{\lambda_2 - \lambda_1}{\ln \frac{\lambda_2}{\lambda_1}} \cdot n \cdot t$$

Sequential Test (III): Illustration

number of failures



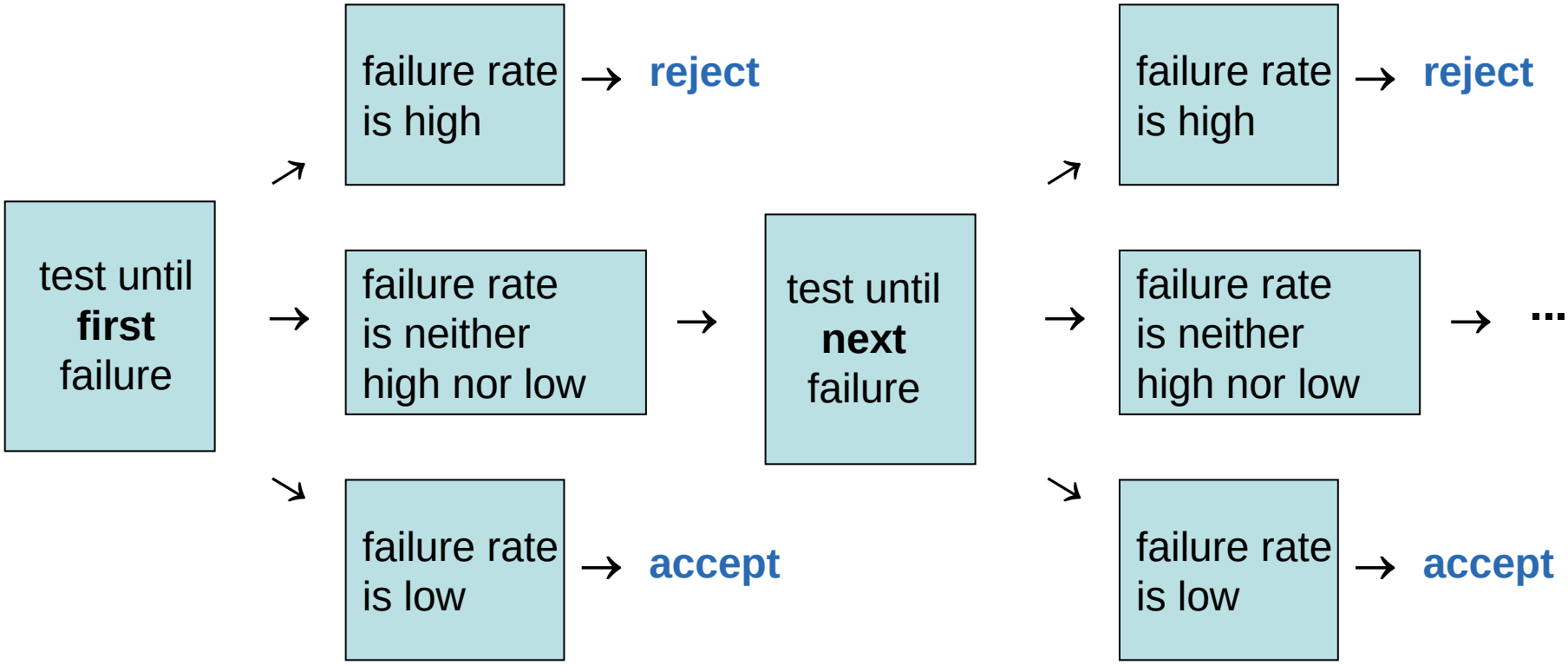
cumulative testing time

The minimum testing time $(nt)_{min}$ and the minimum number of failure i_{min} amount to:

$$(n \cdot t)_{min} = \frac{\ln \frac{\beta}{1-\alpha}}{\lambda_1 - \lambda_2} \qquad i_{min} = \frac{\ln \frac{1-\beta}{\alpha}}{\ln \frac{\lambda_2}{\lambda_1}}$$

where α and β are probabilities

Sequential Test (IV): Algorithm



Extrapolation (I)

Failure prediction by extrapolation:

✓Shorter testing time

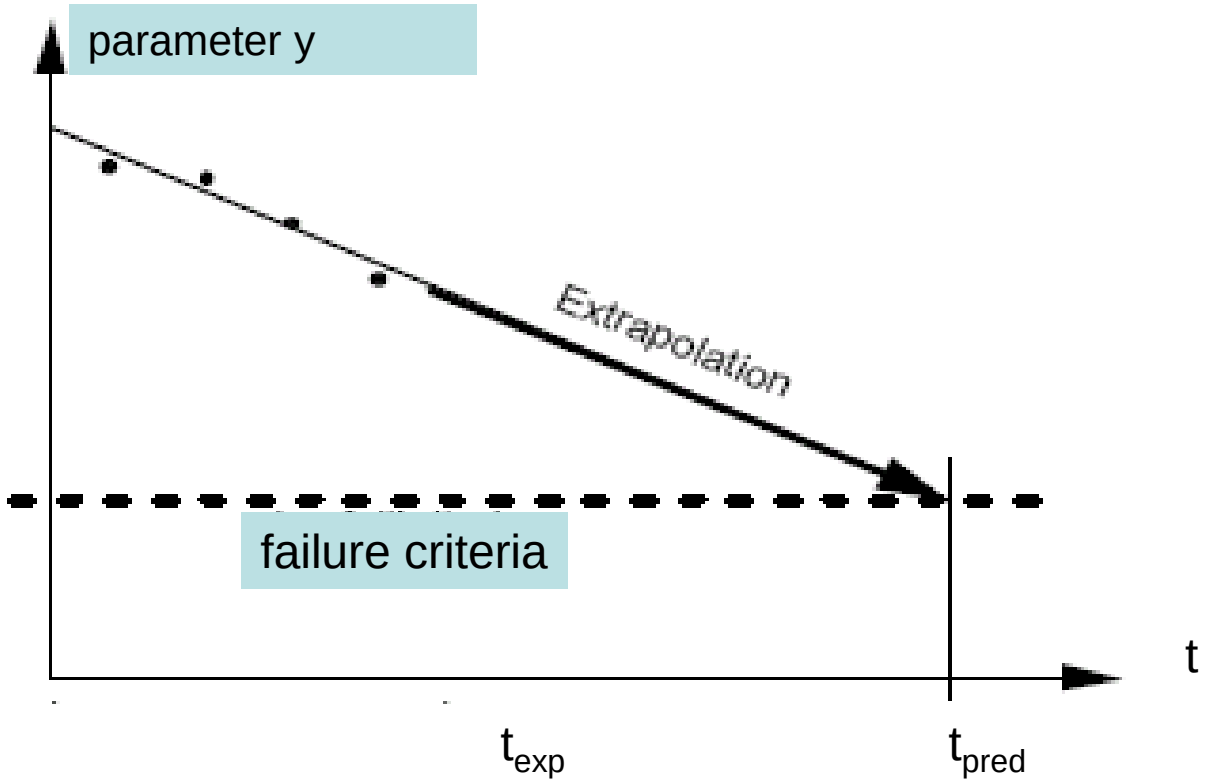
✓ Test is non-destructive

Conditions:

✓Just drift failures

✓ Failure criteria are known

Extrapolation (II): Illustration



t_{exp} testing time

t_{pred} predicted life time (forecast through extrapolation)

Accelerated Test (I)

The Arrhenius acceleration model is widely used to predict life as a function of temperature. It applies specifically to those failure mechanisms that are temperature related and which are within the range of validity for the model.

It states that : $$\text{Life} = A(e)^{\frac{E}{kT}} \qquad (8.43)$$

where:

Life	=	a measure of life e.g., median life of a population of parts
A	=	a constant determined by experiment for the parts involved
e	=	the base of the natural logarithms
E	=	activation energy (electron volts - a measure of energy) this is a unique value for each failure mechanism (Examples of the activation energies for some silicon semiconductor failure mechanisms are shown in Table 8.7-1.)
k	=	Boltzman's constant = 8.62×10^{-5} eV/K
T	=	Temperature (Degrees Kelvin)

MIL-HDBK-338B
ELECTRONIC RELIABILITY DESIGN HANDBOOK

Accelerated Test (II): Algorithm

Acceleration factor $$F_{1,2} = \frac{L_1}{L_2} = e^{\frac{E}{K}(\frac{1}{T_1} - \frac{1}{T_2})}$$

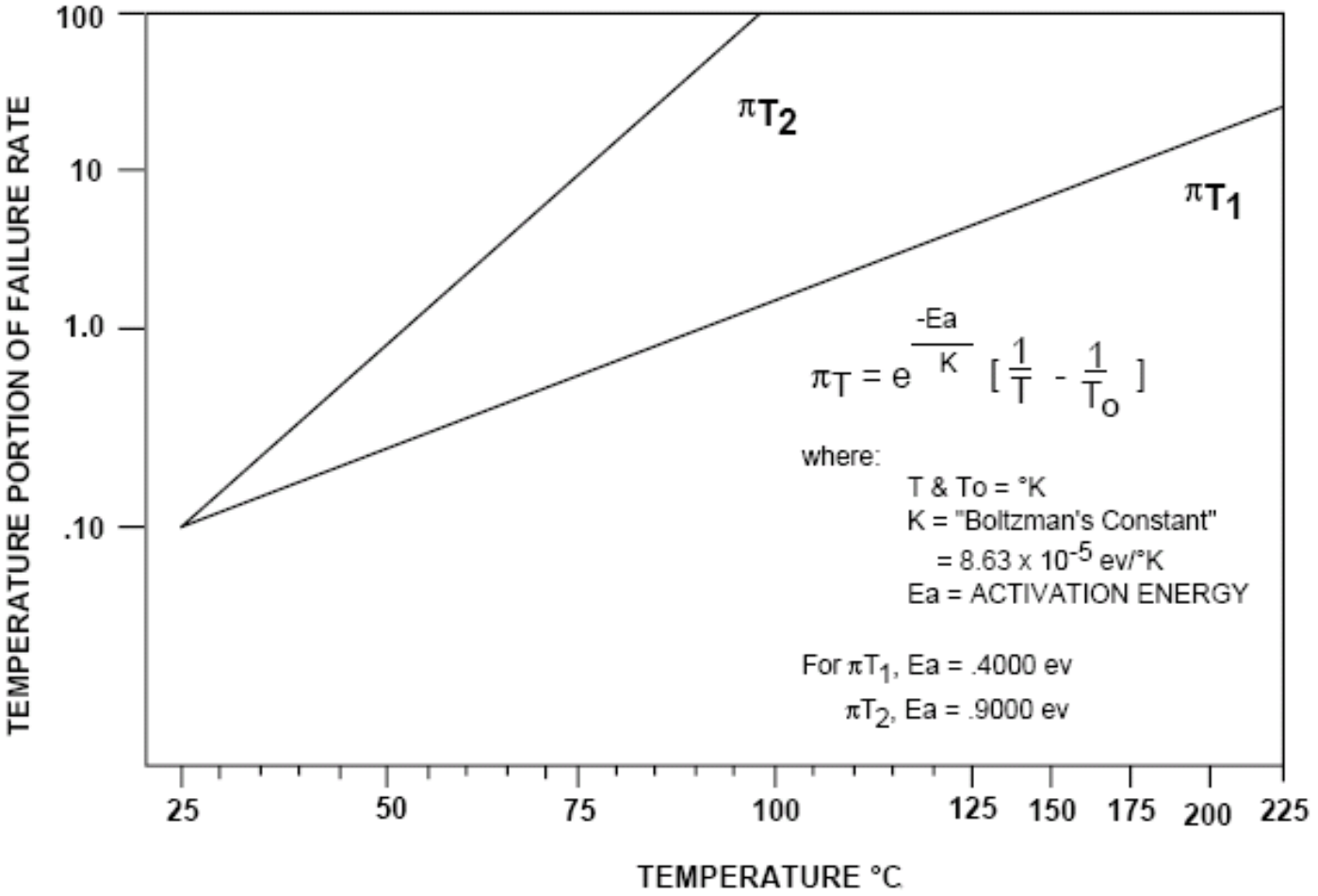
Measure mean life time L_2 of component by $T_2 > T_1$, where T_1 is a low temperature.

If the quotient E/K is unknown, repeat the test by $T_3 > T_1$ and find it from

$$\frac{L_2}{L_3} = e^{\frac{E}{K}(\frac{1}{T_2} - \frac{1}{T_3})}.$$

Then calculate $$L_1 = L_2 \cdot e^{\frac{E}{K}(\frac{1}{T_1} - \frac{1}{T_2})}.$$

Accelerated Test (III): Illustration



MIL-HDBK-338B
ELECTRONIC RELIABILITY DESIGN HANDBOOK