Mathematics - Course 121

BASIC RELIABILITY CONCEPTS

I THE GENERAL RELIABILITY FUNCTION

Suppose N_o identical components are placed into service at time $t = 0$, and that $N(t)$ of these components survive until time t. Then the probability that any one of the original components is still working at time t, ie, the component reliability $R(t)$, is given by

$$R(t) = \frac{N(t)}{N_o}$$

The number of components failing per unit time at time t is $\dot{N}(t)$ - the dot in "$\dot{N}(t)$" indicates the time derivative. Then the probability that any one of the original components fails during unit time at time t is

$$f(t) = -\frac{\dot{N}(t)}{N_o} = -\dot{R}(t)$$

where $f(t)$ is the failure distribution function (see 121.00-7, section III). A hypothetical failure distribution function is shown in Figure 1.

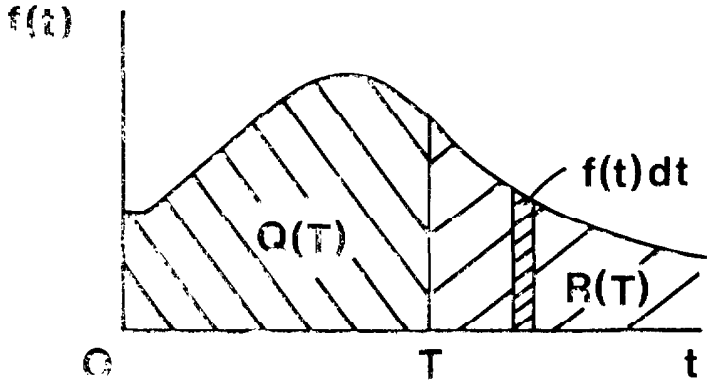


Figure 1: A Hypothetical Distribution Function

Notes re Figure 1:

(1) $f(t)dt$, represented as an incremental slice of the area under the curve, is the probability that a component fails during the interval $(t, t+dt)$.

(2) The total area under the curve,

$$\int_0^\infty f(t)dt = \frac{N_o}{N_o} = 1$$

(There are only N_o components to fail, and all will have failed by $t = \infty$).

(3) By definition, $R(T)$, the component reliability at $t = T$, is the probability that the component is still performing its intended purpose at time T, ie, the probability that it fails <u>after</u> $t = T$. Therefore,

$$R(T) = \int_T^\infty f(t)dt.$$

Similarly, the component unreliability $Q(T)$ is the probability that the component fails by time T, and

$$Q(T) = \int_0^T f(t)dt.$$

Consistent with Note 2 above,

$$R(T) + Q(T) = 1$$

<u>Example 1</u>

One thousand light bulbs were installed at $t = 0$. After 5000 hours' continuous service, 153 bulbs have burned out, and bulbs are failing at the rate of 1.8 per day. What is the bulb reliability for a 5000 hour mission? What is the value of the failure distribution function at $t = 5000$?

<u>Solution</u>

$$R(t) = \frac{N(t)}{N_o}$$

$$\therefore R(5000) = \frac{N(5000)}{N_o}$$

$$= \frac{1000 - 153}{1000} = \underline{\underline{0.847}}$$

ie, the bulb reliability for a 5000 hour mission is 0.847.

$$f(t) = -\frac{\dot{N}(t)}{N_o}$$

$$\therefore \quad f(5000) = -\frac{\dot{N}(5000)}{N_o}$$

$$= -\frac{-1.8/24}{1000}$$

$$= \underline{\underline{7.5 \times 10^{-5}}} \text{ per hour}$$

ie, the value of the failure distribution function at

$t = 5000$ h is 7.5×10^{-5} h^{-1}

———— " ————

The probability that any surviving component fails during unit time at time t, sometimes called the "instantaneous hazard rate", or simply the "failure rate", is

$$\lambda(t) = -\frac{\dot{N}(t)}{N(t)}$$

$$= -\frac{\dot{N}(t)/N_o}{N(t)/N_o}$$

$$= -\frac{\dot{R}(t)}{R(t)}$$

Integrating both sides of this equation over the interval (o,t) gives

$$\int_o^t \lambda(t)dt = -\int_{R(o)}^{R(t)} \frac{dR}{R}$$

$$= -\ln R(t) + \ln R(o)$$

$$= -\ln R(t) + \ln 1$$

$$= -\ln R(t)$$

Exponentiating both sides with base "e" gives

$$\boxed{R(t) = e^{-\int_o^t \lambda(t')dt'}}$$

This is the *general reliability function*.

II RELIABILITY FOR 'USEFUL LIFE' MISSIONS

The $\lambda(t)$ versus t curve is often called the "Bathtub Curve" because of its characteristic shape as seen in Figure 2. Note that each curve in Figure 2 is divided into three sections. Section I, where the failure rate is decreasing, is called the *"infant mortality era"*, or *"burn in era"*. Here failures are predominantly due to manufacturing defects. Section II in the life history of a component is called the *"useful life era"*. Here the failure rate is minimum and constant with time, ie, failures are random in time. Section III is called the *"wear out era"*. Here the failure rate rises as components fail due to wear or fatigue. Figure 2 shows that electronic components typically have lengthier, better-defined useful lives than mechanical components.

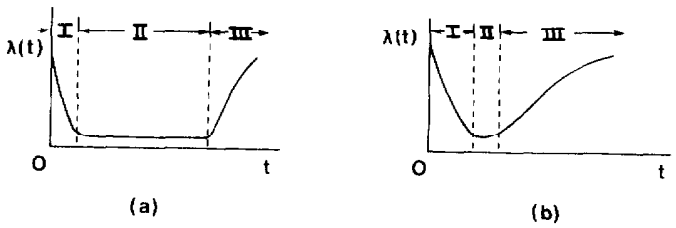


Figure 2: Failure Rate Curves Typical of (a) Electronic Components and (b) Mechanical Components

Clearly, it is advantageous to operate equipment during its useful life era because the failure rate is least, ie, the availability of the equipment is greater because the fraction of time on forced outage is reduced. Useful life operation is achieved in practice by placing only burned in components in service, and by either replacing or overhauling components before they reach the wear out era, ie, by following the so-called *Golden Rule of Reliability*.

The Golden Rule of Reliability

Replace components as they fail within their useful lives, and replace components preventatively, even if they have not failed, no later than by the end of their useful lives.

If operation is restricted to the useful life of a component or system, then the failure rate is constant and the "general reliability function" derived in section I simplifies to

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

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

and $Q(t) = 1 - e^{-\lambda t}$

The relationships amongst R(t), f(t) and Q(t) are shown in Figures 3 and 4.

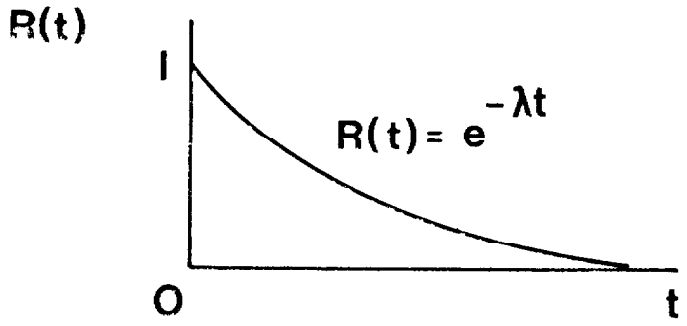


Figure 3: Useful Life Reliability Function

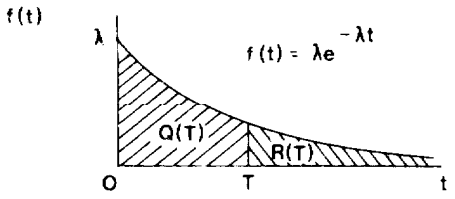


Figure 4: Useful Life Failure Distribution Function

Consider two missions of equal duration t - mission A early in the useful life and mission B late in the useful life of a component - see Figure 5.

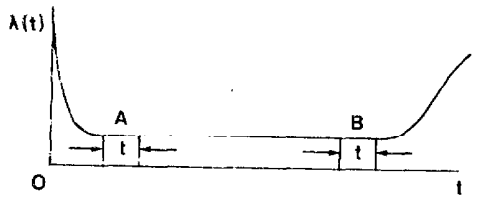


Figure 5: Hypothetical Missions A and B

Question: How does the reliability for mission B compare with that for mission A?

Answer: The reliabilities for the two missions are exactly the same. The reliability of useful life missions depends only on the *mission time t*, since the failure rate is constant.

Proof: Consider a mission which begins T units into the useful life of a component, and concludes t units later - see Figure 6.

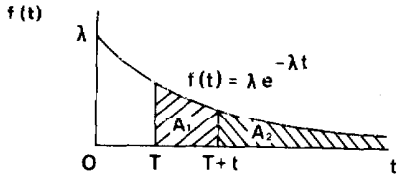


Figure 6: Failure Distribution Function for Useful Life Mission over Interval (T, T + t)

Let S_T, S_{T+t} denote component survival to time T, time T + t, respectively. Then the mission reliability is the conditional probability,

$$P(S_{T+t}|S_T) = \frac{P(S_{T+t} \cap S_T)}{P(S_T)} \qquad \text{by PR6}$$

$$= \frac{P(S_{T+t})}{P(S_T)}$$

$$= \frac{\int_{T+t}^{\infty} \lambda e^{-\lambda t} dt}{\int_{T}^{\infty} \lambda e^{-\lambda t} dt}$$

$$= \frac{A_2}{A_1 + A_2} \qquad \text{(see Figure 6)}$$

$$= e^{-\lambda t}$$

Note that the mission reliability is utterly independent of T and depends only on λ and t.

III MEAN TIME TO FAILURE

DEFINITION: The *Mean Time to Failure* (MTTF) of a component is the average time it would operate under useful life conditions before failing.

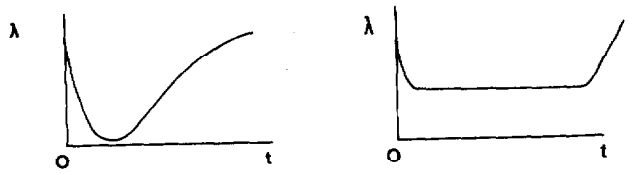
By PR9 adapted for the case of a continuous probability distribution function,

$$MTTF \equiv E(t) = \int_0^{\infty} tf(t)dt$$

$$= \int_0^{\infty} t\lambda e^{-\lambda t} dt$$

ie, $$\boxed{MTTF = \frac{1}{\lambda}}$$

Note that there is no mathematical relationship between the MTTF and the useful life (UL) of a component. For example, Figure 7(a) depicts a short UL and long MTTF (small λ => large $1/\lambda$), whereas Figure 7(b) depicts a long UL and relatively short MTTF (large λ => $1/\lambda$).



(a) Short UL; long MTTF (b) Long UL; short MTTF

Figure 7

Note that the MTTF is often much longer than the useful life. For example, for a human in the prime of life the failure rate may be of the order of 10^{-3} per annum, corresponding to a MTTF of 1000 years. What this means is that people would live an average of 1000 years if they could 'operate' continuously under 'useful life' conditions. In reality, of course, an individual enters the 'wear out region' long before the 1000 years expire, and failure is due to aging rather than to random statistical failures (eg, accidents, terminal illnesses) characteristic of prime of life operation.

Another example of these concepts - one which may, perhaps, be analyzed with a little more objectivity - is the life history of automobile tires. The useful life failure rate of a tire might be 2.5×10^{-6} per km, corresponding to a 'MTTF' of 400,000 km. In reality, of course, the tire goes bald long before the 400,000 km is up, and fails due to wear rather than due to the random statistical failures (eg, punctures, overheating) characteristic of useful life operation.

Example 1

A component has a MTTF of 10,000 hours and a useful life of 1000 hours. Find the reliability for (a) a 10 hour mission (b) the entire useful life.

Solution

(a) $R(t) = e^{-\lambda t}$ where $\lambda = \frac{1}{MTTF}$

$= 10^{-4}\ h^{-1}$

$R(10) = e^{-10^{-4} \times 10}$

$= \underline{\underline{0.9990}}$

ie, the reliability for a 10 hour mission is 0.9990.

(b) $R(1000) = e^{-10^{-4} \times 10^{3}}$

$= \underline{\underline{0.9048}}$

ie, the reliability for the useful life is 0.9048.

Example 2

If a system is required to have a reliability of at least 99.9% for a 100 hour, useful life mission, find the minimum tolerable MTTF.

Solution

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

$R(100) \geq 0.999 \Rightarrow e^{-100\lambda} \geq 0.999$

ie, $-100\lambda \geq \ln 0.999$

ie, $\lambda \leq 1.00 \times 10^{-5}\ h^{-1}$

$\therefore$ $MTTF \geq 1.00 \times 10^{5}$ hours

ie, the minimum tolerable MTTF is 1.00×10^{5} hours.

IV RELIABILITY OF NETWORKS OF COMPONENTS

(i) Series Network

Suppose that n components are connected in series, see Figure 8, and that system operation requires all n components:

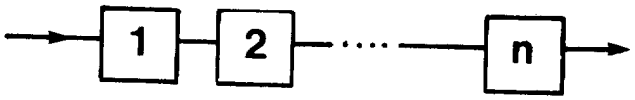


Figure 8: n Components in Series

Then system reliability Rs is the probability that all n components survive, ie, if R_i represents the ith component reliability,

$$R_s = R_1 R_2 \ldots\ldots R_n \qquad \text{by PR1}$$

$$= \prod_{i=1}^{n} R_i$$

Assuming useful life operation of all components,

$$R_i(t) = e^{-\lambda_i t}$$

and $$R_s(t) = \prod_{i=1}^{n} e^{-\lambda_i t}$$

ie, $$\boxed{R_s(t) = e^{-\left(\sum_{i=1}^{n} \lambda_i\right)t}}$$

(ii) Parallel Network

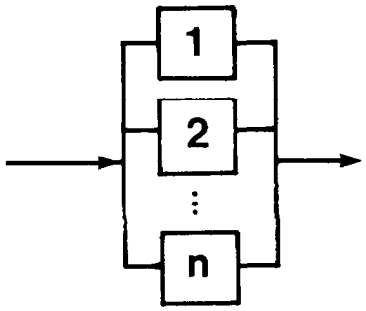


Figure 9: n Components in Parallel

Suppose that n redundant components are connected in parallel. Then system unreliability Q_S is the probability that all n components fail:

$$Q_s = \prod_{i=1}^{n} Qi \qquad \text{by PR1}$$

Assuming useful life operation of components,

$$Q_i(t) = 1 - R_i(t) = 1 - e^{-\lambda_i t}$$

and $$\boxed{Q_s(t) = \prod_{i=1}^{n} (1 - e^{-\lambda_i t})}$$

Note: All components essential to system operation, whether physically connected in series or not, are effectively in series as far as system reliability is concerned. The reader may assume that all block diagrams given in examples, assignments, and check-outs are *reliability block diagrams*, ie, that components shown in series are all necessary to the integrity of that series path, whereas components or branches of components shown in parallel are redundant.

Example 1

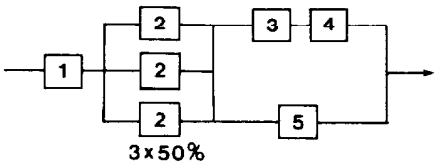


Figure 10

(a) Derive an expression for the reliability R_S of the system of Figure 10, in terms of component reliabilities R_1, R_2,.....,R_5.

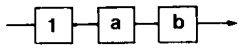
(b) Calculate the numerical value of R_S if

$R_1 = R_2 = R_3 = R_4 = R_5 = 0.900000$

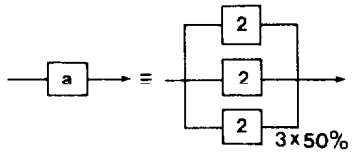
(c) Calculate the numerical value of R_S for a 5000 hour mission if $\lambda_1 = 10^{-5}$ f/h, $\lambda_2 = \lambda_3 = 8 \times 10^{-5}$ f/h, and $\lambda_4 = \lambda_5 = 5 \times 10^{-6}$ f/h.

Solution

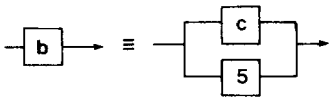
The given system is neither simple series nor simple parallel, but it is series-parallel in nature, ie, it is readily analyzed as a composite of simple series and simple parallel configurations. The given system is equivalent to the following simple series system:



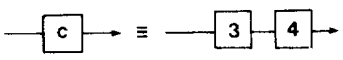
where



and



where



Now $R_s = R_1 R_a R_b$

where R_a = P(2 or 3 "2's" survive)

$= {}_3C_2 R_2^2 Q_2 + {}_3C_3 R_2^3$ by PR4

$= 3R_2^2(1-R_2) + R_2^3$

Note that there are ${}_3C_2 = 3$ ways for exactly two of the three "2's" to survive, and only ${}_3C_3 = 1$ way for all three "2's" to survive.

$R_b = 1 - Q_b$

$= 1 - Q_c Q_5$

$= 1 - (1 - R_c)(1 - R_5)$

where $R_c = R_3 R_4$

Substituting for R_a, R_b and R_c gives

$R_s = R_1[3R_2^2(1-R_2)+R_2^3][1-(1-R_3R_4)(1-R_5)]$

(b) $R_s = 0.9[3(.9)^2(.1)+(.9)^3][1-(1-.9x.9)(1-.9)]$

$= \underline{0.858179}$

(c) $R_1(t) = e^{-\lambda_1 t}$

$\therefore R_1(5000) = e^{-10^{-5} \times 5000}$

$= 0.951229$

Similarly $R_2(5000) = R_3(5000) = 0.670320$

and $R_4(5000) = R_5(5000) = 0.975310$

Substituting for Ri in the expression for R_s derived in (a) gives

$\underline{R_s = 0.703172}$

iii Use of Baye's Theorem to Analyze Non Series-Parallel Networks

Some reliability block diagrams are not readily broken down into simple series and parallel subsystems. A conditional probability approach can be useful in analyzing the reliability of such systems. Consider the schematic reliability block diagram of Figure 11. Suppose that the calculation of system reliability could be simplified substantially if the status of component x were known.

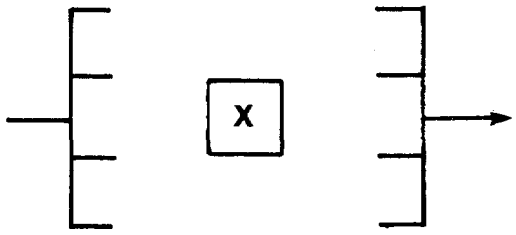


Figure 11: Schematic Representation of a Network Containing Component x

Recall from 121.00-3, Baye's Theorem, which states that if event A can occur only in conjunction with one of two mutually exclusive events, B_1 and B_2, then

$$P(A) = P(A|B_1)P(B_1) + P(A|B_2)P(B_2)$$

This equation can be interpreted with reference to the system of Figure 11 as follows:

A ≡ system survives

B_1 ≡ component x survives

B_2 ≡ component x fails

The above equation can then be rewritten as follows:

$$P_{(\text{system survives})} = P(\text{system survives}|x \text{ survives})\, P(x \text{ survives} + P(\text{system survives}|\, x \text{ fails})P(x \text{ fails})$$

The following short-hand notation will be used in this text:

$R_s^x \equiv P(\text{system survives}|x \text{ survives})$

$R_s^{\bar{x}} \equiv P(\text{system survives}|x \text{ fails})$

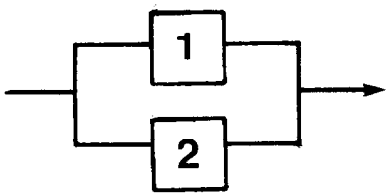
The preceding statement of Baye's Theorem is then written

$$\boxed{R_s = R_s^x R_x + R_s^{\bar{x}} Q_x}$$

where R_x, Q_x represent component x reliability, unreliability, respectively.

Example 2:

Calculate the reliability of the following simple parallel system using Baye's Theorem:



Solution:

Choose component 1 as component x

Then $R_S = R_S^1 R_1 + R_S^{\overline{1}} Q_1$

$= (1)\ R_1 + R_2(1-R_1)$

$= R_1 + R_2 - R_1R_2$

Note that this is readily identified as the correct answer by applying PR3 to the following:

P(system survives) = P("1" survives $\cup$ "2" survives).

This answer is also derived readily from the expression developed for parallel networks in section IV(ii) above:

$$Q_S = Q_1Q_2$$

ie, $R_S = 1-Q_S$

$= 1 - Q_1Q_2$

$= 1 - (1-R_1)(1-R_2)$

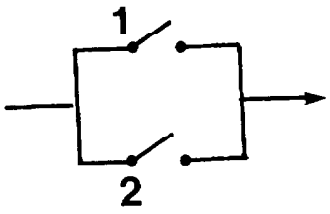
$= R_1 + R_2 - R_1R_2$ as above.

Example 2:

Calculate the reliability of a system of two identical switches in parallel. A switch can fail open or short and has failure rate

$$\lambda = \lambda_o + \lambda_s$$

where λ_o is the rate of failing open, and
λ_s is the rate of failing short.



Solution:

Expanding about switch #1 using Baye's Theorem,

$$P(S) = P(S|1G)P(1G) + P(S|1FO)P(1FO) + P(S|1FS)P(1FS)$$

where S ≡ system survives
1G ≡ switch #1 survives
1FO ≡ switch #1 fails open
1FS ≡ switch #1 fails short

Using analogous notation for switch #2,

$$P(S|1G) = P(2G \cup 2FO)$$

$$= P(2G) + P(2FO) \qquad \text{by PR4}$$

ie, if switch #1 survives the system survives providing switch #2 either survives or fails open. Note that the system fails if either switch fails short, regardless of the status of the other switch, because the system loses the ability to open the circuit.

Also, $P(S|1FO) = P(2G)$, and
$P(S|1FS) = 0$

$$\therefore \quad P(S) = [P(2G) + P(2FO)]P(1G) + P(2G)P(1FO)$$

If r and q represent switch reliability and unreliability, respectively, then

$$P(1G) = P(2G) = r,$$

$$P(1FO) = P(2FO) = \frac{\lambda_o}{\lambda} q, \text{ and}$$

$$P(1FS) = P(2FS) = \frac{\lambda_s}{\lambda} q$$

Then $P(S) = [r + \frac{\lambda_o}{\lambda} q]r + r \frac{\lambda_o}{\lambda} q$

ie, a little algebraic manipulation gives system reliability $R_s = P(S)$ as

$$\boxed{R_s = \frac{2\lambda_o}{\lambda} r + \frac{\lambda_s - \lambda_o}{\lambda} r^2}$$

Analysis of Solution

Case 1: $\lambda_o = \lambda_s \Rightarrow R_s = r$

In this case system reliability is unaffected by adding switch #2 in parallel with switch #1.

Case 2: $\lambda_o = 0 \Rightarrow R_s = r^2$

In this case, system reliability is reduced by connecting the second switch in parallel. (This is true as long as $\lambda_o < \lambda_s$ because switch #2 is more likely to fail the system by failing short, than it is to save the system when switch #1 fails open.)

Case 3: $\lambda_s = 0 \Rightarrow R_s = 2r - r^2$

In this case system reliability is improved by connecting the second switch in parallel. (This is true as long as $\lambda_o > \lambda_s$ because switch #2 is more likely to save the system when switch #1 fails than to fail the system by failing short.)

This example is instructive: it shows that installing redundant components may improve, not affect, or even reduce reliability, depending on the possible failure modes of the redundant components, and on the relative probabilities of such failure modes.

It also shows very clearly the distinction between the way in which the components are connected physically and the way in which they are connected in the reliability block diagram. The Case II expression, $R_S = r^2$, is the expression for two components in series, ie, when switches which can only fail short are physically connected in parallel, they are effectively connected in series as far as system reliability is concerned. In contrast, the Case III expression, $R_S = 2r - r^2$, is the expression for two components in parallel, ie, when switches which can only fail open are physically connected in parallel, they appear in parallel on the reliability block diagram as well.

Example 3

Calculate the reliability of the system of Figure 12 assuming that the reliability of all components is 0.9000000.

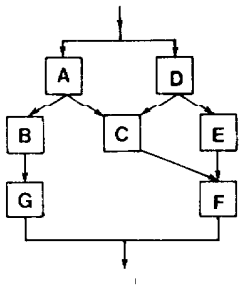


Figure 12

Solution

Applying Baye's Theorem using component A, and resorting to notation introduced earlier in section IV(iii),

$$R_S = R_S^A R_A + R_S^{\overline{A}} Q_A$$

Since R_S^A, $R_S^{\overline{A}}$ are still not very easy to calculate, Baye's Theorem is reapplied using component C:

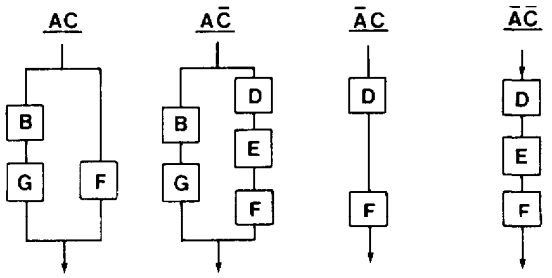
$$R_S^A = R_S^{AC}R_C + R_S^{A\bar{C}}Q_C, \text{ and}$$

$$R_S^{\bar{A}} = R_S^{\bar{A}C}R_C + R_S^{\bar{A}\bar{C}}Q_C$$

$$\therefore \quad R_S = R_A R_C R_S^{AC} + R_A Q_C R_S^{A\bar{C}} + Q_A R_C R_S^{\bar{A}C} + Q_A Q_C R_S^{\bar{A}\bar{C}}$$

(Note that this line could have been written down at the outset since AC, $A\bar{C}$, $\bar{A}C$ and $\bar{A}\bar{C}$ constitute a set of four mutually exclusive events suitable for use as "B-events" in PR8).

To aid in expanding R_S^{AC}, $R_S^{A\bar{C}}$, $R_S^{\bar{A}C}$ and $R_S^{\bar{A}\bar{C}}$, the system of Figure 12 is redrawn for each alternative:



Thus $R_S^{AC} = 1-(1-R_B R_G)(1-R_F)$,

$$R_S^{A\bar{C}} = 1-(1-R_B R_G)(1-R_D R_E R_F),$$

$$R_S^{\bar{A}C} = R_D R_F, \text{ and}$$

$$R_S^{\bar{A}\bar{C}} = R_D R_E R_F$$

Substitution of these four expressions into the above expression for R_S, and substituting 0.9000000 for all component reliabilities gives

$$R_S = 0.9601659$$

ASSIGNMENT

1. A system consists of three black boxes A, B and C. These may be arranged in any one of the four following configurations.

   The individual component reliabilities are:

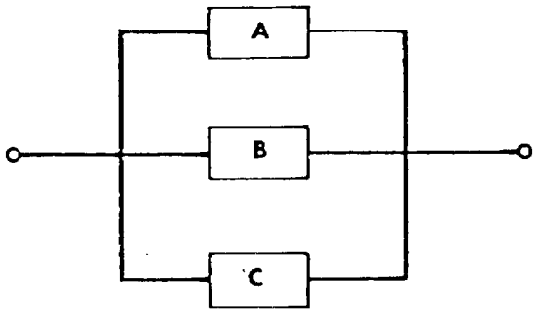
   $$R_A(t) = e^{-\alpha t}$$

   $$R_B(t) = e^{-\beta t}$$

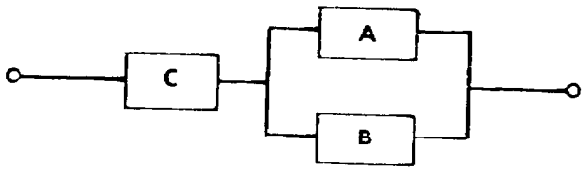
   $$R_C(t) = e^{-\gamma t}$$

   Write an expression for the system reliability in each of the four cases below:

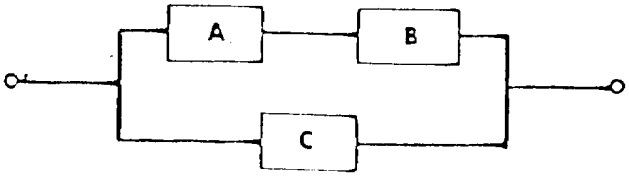
(a)



(b)



(c)

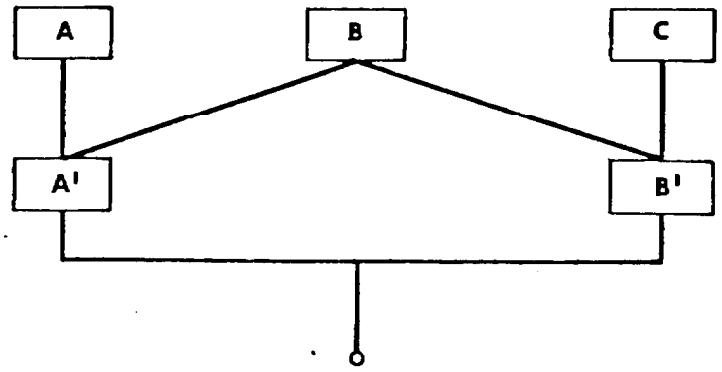


(d)

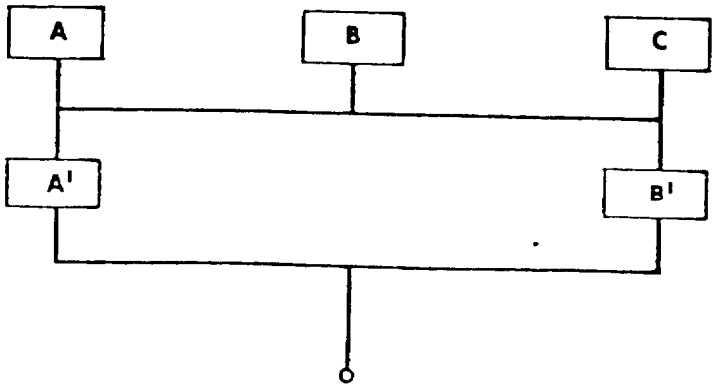
2. A component operating during its useful life has a reliability of 90% for a mission of 50 hours. What would the component reliability be for a mission of 100 hours?

3. A system consists of four components in parallel. System success requires that at least three of these components must function. What is the probability of system success if the component reliability is 0.9? What is the system reliability if five components are placed in parallel to perform the same function?

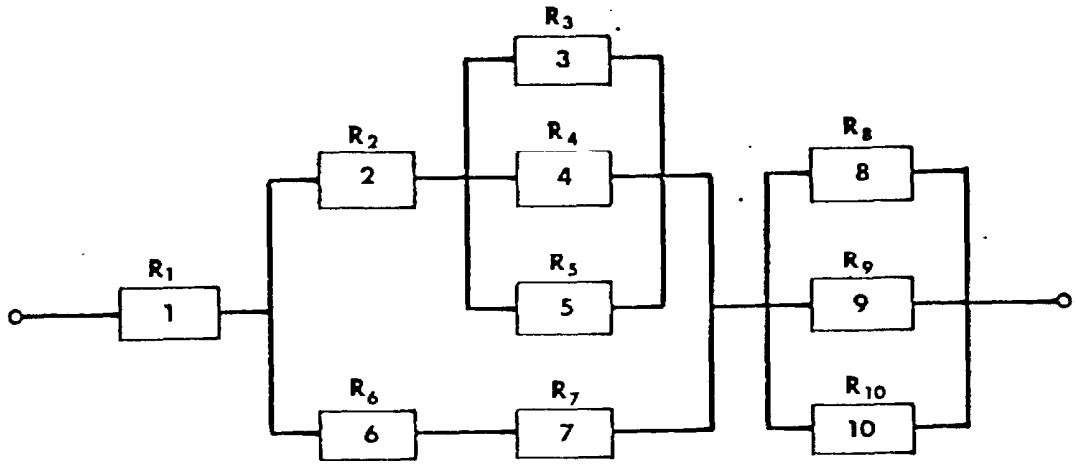
4. In the system shown below, system success requires that one of the following paths must be available A-A', B-A', C-B', B-B'. Write an expression for the reliability of this system. If all the components have a reliability of 0.9, what is the system reliability?



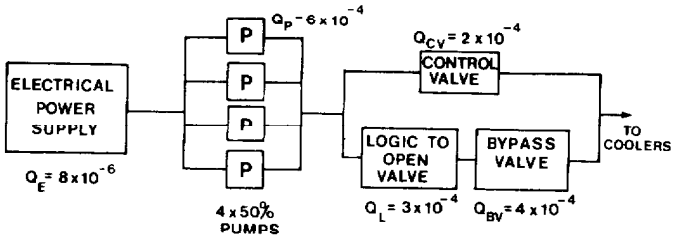
Compare this with the reliability of the following system.



5. The system shown below is made up of ten components. Components 3, 4 and 5 are not identical and at least one component of this group must be available for system success. Components 8, 9 and 10 are identical and for this particular group it is necessary that two out of the three components function satisfactorily for system success. Write an expression for the system reliability in terms of the R values given.

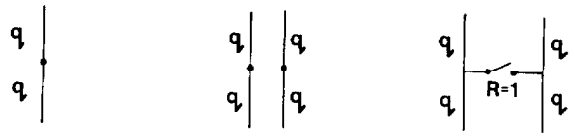


6. Calculate the unavailability of service water supply to the vault coolers using the following reliability model:

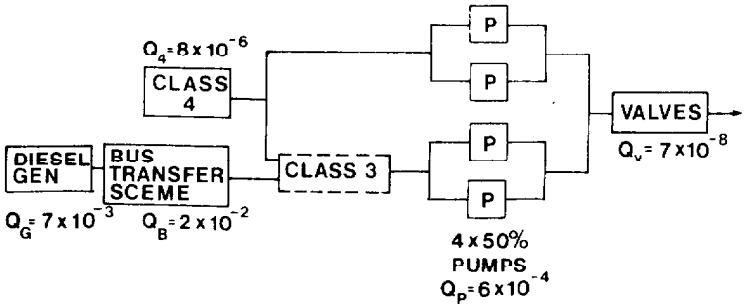


The control valve is normally open; the bypass valve opens on high vault pressure. Either valve delivers sufficient flow.

7. Compare the unreliabilities of the following transmission facilities: ($q = 10^{-2}$).



8. Calculate the unreliability of service water using the following reliability model:



Note that class 4 normally supplies class 3. On failure of class 4, the diesel generator starts and the bus transfer scheme transfers class 3 loads to the generator.

9. Example 2, section IV(iii) of this lesson analyzes the reliability of a system of two switches connected in parallel. Show that the reliability of a <u>series</u> system of two such switches is given by

$$R_S = 2\frac{\lambda_S}{\lambda} r + \frac{\lambda_o - \lambda_S}{\lambda} r^2$$

Under what circumstances does connecting the second switch in series with the first

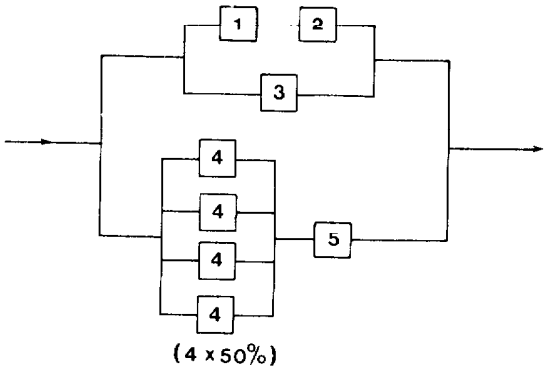
(a) improve
(b) have no effect on
(c) reduce

system reliability?

10. Repeat Example 3, section IV(iii) but expanding about components

(a) D and C
(b) A and D

11.



(a) Derive an expression for system unreliability Q_S in terms of component unreliabilities Q_1, Q_2, Q_3, Q_4, Q_5.

(b) If $Q_1 = Q_2 = Q_3 = Q_4 = Q_5 = 0.100000$, calculate the value of Q_S.

12. (a) Calculate the unreliability of a system of two diodes connected in parallel if diode unreliability

$$Q = Q_O + Q_S,$$

where $Q_O = 0.02$ is the probability of failing open-circuit, and $Q_S = 0.01$ is the probability of failing short-circuit.

(b) Calculate the Unreliability Improvement Ratio (UIR) over a single diode system. (The UIR in this case is the ratio of single-diode unreliability to the unreliability of the 2-diode system.)

(c) Repeat (a) and (b) using the values $Q_O = 0.01$ and $Q_S = 0.02$. Rationalize the result.

This Appendix tidies up two points which were left open earlier in the course.

I Annual Risk

Problem

The following formulas were used in 121.00-5:

$$ARPE = \lambda_R Q_P$$

$$ARNA = \lambda_R Q_P Q_{CT}$$

where ARPE is the "Annual Risk of Power Excursions", ie the probability of at least one power excursion per annum,
λ_R is the number of unsafe losses of power regulation (LOR's) per annum,
Q_P is the unavailability of the protective (shutdown) system,
ARNA is the "Annual Risk of Nuclear Accidents", ie the probability of at least one nuclear accident per annum, and
Q_{CT} is the unavailability of the containment system.

The RHS's of these equations represent the numbers of failures per annum due to power excursions and nuclear accidents, respectively, whereas the LHS's represent dimensionless probabilities. The problem is to justify these formulas.

Solution

Suppose that a unit is placed in service at t = 0 and that the number of failures per annum due to power excursions is $\lambda_R Q_P$ (this is the number of LOR's for which the protective system is unavailable to trip off the unit). If $Q_e(t)$ represents unit unreliability due to power excursions, then the annual risk of power excursions is $Q_e(1)$. The standard exponential distribution for useful life failures gives

$$Q_e(t) = 1 - R_e(t)$$

$$= 1 - e^{-\lambda_R Q_P t}$$

Thus the annual risk of power excursions is

$$Q_e(1) = 1 - e^{-\lambda_R Q_P}$$

The McLaurin Series expansion of e^x (derived in most elementary calculus texts) is

$$e^x = 1 + x + \frac{x^2}{2!} + \frac{x^3}{3!} + \ldots$$

Thus

$$e^{-\lambda_R Q_P} = 1 - \lambda_R Q_P + \frac{(-\lambda_R Q_P)^2}{2!} + \frac{(-\lambda_R Q_P)^3}{3!} + \ldots$$

Substituting this expression in the expression for $Q_e(1)$ gives

$$Qe(1) = \lambda_R Q_P - \frac{(\lambda_R Q_P)^2}{2!} + \frac{(\lambda_R Q_P)^3}{3!} - \ldots$$

If $\lambda_R Q_P << 1$, and of course it must be, then to an excellent approximation,

$$Q_e(1) \equiv \text{ARPE} = \lambda_R Q_P$$

Note, incidentally, that the RHS really is dimensionless after all because of the implicit factor of t = 1 year:

$$\text{RHS} = (\lambda_r \text{ year}^{-1})(Q_P)(t = 1 \text{ year})$$

The argument to vindicate the formula for ARNA is completely analogous to the above.

II Unavailability of a Tested Safety System

Problem

The problem here is to vindicate the claim made in 121.00-5 that the formula for safety system unavailability, namely,

$$Q = \lambda \frac{T}{2},$$

gives the average unreliability, neglecting repair time.

Solution

Figure A1 shows the reliability cycle for a tested safety system, neglecting repair time. Every T years the system is tested, repaired if necessary, and placed back in service. Each time the integrity of the system is ascertained, the reliability returns to 1, and then decays exponentially during the test interval.

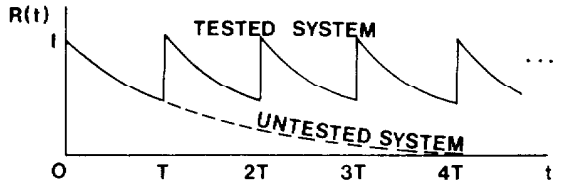


Figure A1: Reliability Cycle of a Tested Safety System

One cycle only of this pattern is shown in Figure A2. The average reliability for this cycle will be the average reliability of the system since all cycles are identical under the assumption of negligigle repair time.

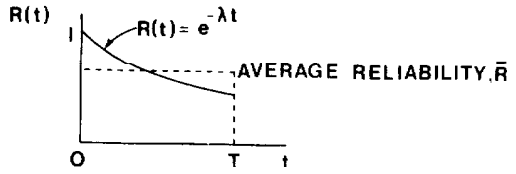


Figure A2: Reliability of a Safety System Between Consecutive Tests

The average reliability $\bar{R}$ is then given by

$$\bar{R} = \frac{1}{T}\int_0^T e^{-\lambda t}dt$$

$$= -\frac{1}{\lambda T}\int_0^T de^{-\lambda t}$$

$$= \frac{1 - e^{-\lambda T}}{\lambda T}$$

Expanding $e^{-\lambda T}$ via the McLaurin Series (see section AI of this Appendix) gives:

$$\bar{R} = \frac{1 - [1 - \lambda T + \frac{(-\lambda T)^2}{2!} + \frac{(-\lambda T)^3}{3!} + \ldots]}{\lambda T}$$

$$= 1 - \frac{\lambda T}{2} + \frac{(\lambda T)^2}{6} - \ldots$$

Since $\lambda T << 1$ in practice in order to maintain high reliability, to a very good approximation,

$$\bar{R} = 1 - \frac{\lambda T}{2}$$

Hence the average unreliability is given by

$$\bar{Q} = \frac{\lambda T}{2}$$

which is the formula used in section 121.00-5.

L. Haacke