Mathematics - Course 221

BASIC RELIABILITY CONCEPTS

The material in this lesson is intended to provide the basic probability and reliability concepts required in the reliability evaluation of nuclear power station systems. The emphasis is on the analysis of safety systems, eg, ECC, shutdown systems, containment.

I. BASIC PROBABILITY

The word *probability* is often used very loosely, and it is important that it is recognized as a technical word implying "a measure of chance".

Probability is expressed over a scale of 0 to 1 as shown in Figure 1.

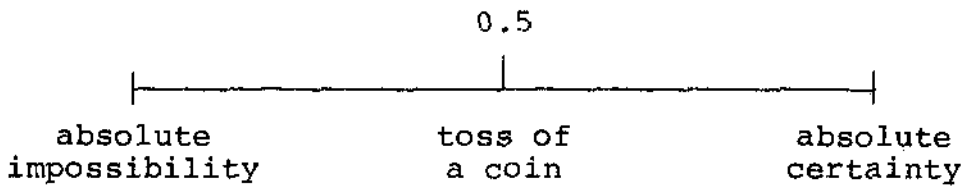


Figure 1

Probability Scale

Example 1

Roll a die. What is the probability that a two appears? There are only six possible outcomes to the experiment and only one of them gives a two.

The probability of a two appearing is 1/6. Symbolically:

$$P(2) = 1/6$$

The proability of a two not appearing $P(\bar{2})$ is 5/6. Symbolically:

$$P(\bar{2}) = 5/6$$

If p is the proability that an event occurs and q is the probability that the event does not occur, then:

$$p + q = 1$$

In engineering applications, component success or failure probabilities cannot usually be determined by their geometries as in the case of a coin, a die, a roulette wheel, a deck of cards, etc. A *frequency interpretation of probability* must be used.

If n is the number of times an experiment is repeated and f is the number of occurrences of a particular event E, then the probability of E's occurring,

$$P(E) = \lim_{n \to \infty} \left(\frac{f}{n}\right)$$

Independent Events

Consider two events: if the outcome of one cannot be affected by the outcome of the other, they are said to be independent.

If there are two independent events, Event A and Event B, the probability of both Event A and Event B happening equals the product of the probabilities of each happening. The combined event is designated Event AB.

$$P(AB) = P(A) \times P(B)$$

Generalizing to n independent events:

$$P(A_1A_2 \ldots A_n) = P(A_1)P(A_2) \ldots P(A_n)$$

This relation is of utmost importance in reliability work. For example, consider an electronic system which is composed of 5 components: the probability that component No. 1 survives $P(A_1)$ is some value p_1; for component No. 2 $P(A_2) = p_2$ and so on. The system will survive (ie, maintain the ability to perform its task) only if all its components survive. The probability of this event is:

$$P(\text{system survives}) = p_1 \cdot p_2 \cdot p_3 \cdot p_4 \cdot p_5$$

In words, the probability that the system survives is the product of the survival probabilities of its components.

Where do the p_i's come from? They are based on empirically (based on practical experience rather than theory) determined failure rates. For systems in the design stage, one uses historical data collected from tests under simulated operating conditions or from items used in similar duty. For operating equipment, this data can be refined using actual experience; in this way, the effects of any "local" or individual conditions can be included.

II. BASIC RELIABILITY

Reliability (R) is the probability, at any given instant, that a component or system will be available to perform its intended function. *Unreliability* (Q) is just the opposite of reliability, ie, the probability of being unavailable at any given instant. Both are dimensionless quantities and represent the fraction of total time spent in either condition. R + Q must always equal 1; ie, if a component is out of service 2% of the time, it means the component must be in-service 98% of the time. Hence, R = 0.98 and Q = 0.02 and R + Q = 1.

In safety system analysis, we generally speak of unreliability (Q). This is purely for arithmetical convenience; ie, it is easier to write an unreliability of 10^{-5} than a reliability of 0.99999.

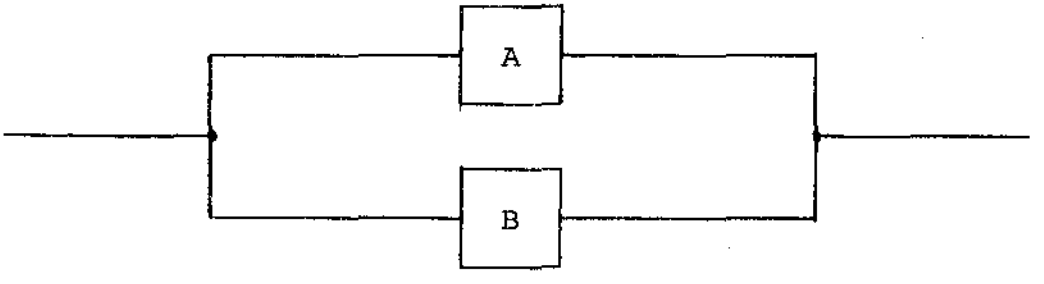
Redundancy

In some instances requirements are beyond the inherent reliability of the equipment. To meet the requirements, one can employ redundant components. The justification for redundancy is simply that multiple random failures are less likely than single ones.

There are two types of redundancy - active and standby. In active redundancy, all components operate simultaneously, while in standby redundancy, the components operate in solo and require a switching operation to change from an operating one to a standby one.

Example of Active Redundancy

The simplest form has only two components, eg, two 100% control valves. If one or both of them survive (operate as required), the system is said to be 'successful'.



'Success Modes'

Both operate as required (each allowing 50% flow)

$$P(A) \times P(B)$$

A operates allowing 100% flow, B failed

$$P(A) \times [1-P(B)]$$

A failed, B operates allowing 100% flow

$$[1-P(A)] \times P(B)$$

The probability of the system success (required operation) is equal to the sum of all success modes:

$$P = P(A) \times P(B) + P(A)\ [1-P(B)] + [1-P(A)] \times P(B)$$

$$= P(A) + P(B) - P(A) \times P(B)$$

If $P(A) = P(B)$, it is easily shown that:

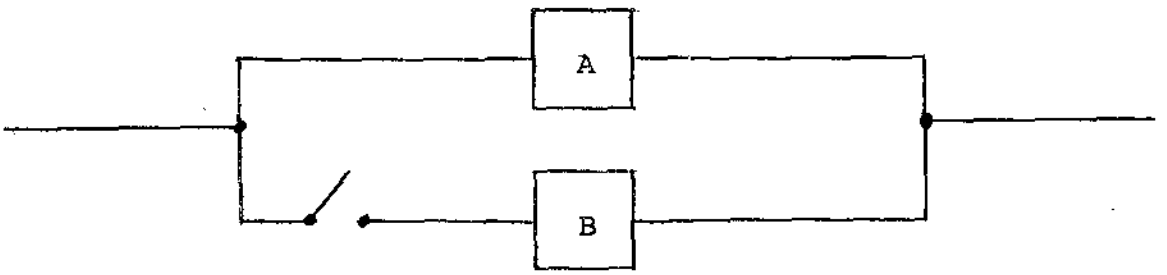
$$P = 2P(A) - P^2(A)$$

$$= 1 - Q^2(A) \qquad \text{when } P(A) + Q(A) = 1$$

The probability of at least one component success is equal to 1 minus the probability that both components fail.

Example of Standby Redundancy

A similar approach can be taken with standby redundancy (eg, 2 x 100% pumps, when one fails the other is switched on).



Two approaches are common: one which assumes failure free switching and the other which considers that switching may fail.

III. SAFETY SYSTEMS UNRELIABILITY

Safety systems are standby, 'guardian angel' systems - they normally operate only when process equipment fails. For example, the reactor *protective system* trips off the reactor only when the *regulating system* fails; otherwise the protective system does nothing. Similarly, the *containment system* operates to confine the spread of radioactivity within plant boundaries only in the event that both regulating and protective systems fail simultaneously.

For safety systems, the unreliability is numerically equivalent to the *unavailability*.

Definition

The unavailability Q of a component or system is the fraction of time during which it would not function as required.

Thus: $$Q = \lambda t,$$

where λ is the *failure rate* in failures per year, and
t is the *average fault duration* in years.

Failure rates can be calculated on the basis of operating experience.

Example 2

Calculate the failure rate of a component, given that 6 component failures occurred during 4 years' operation of 12 such components.

Solution

$$\lambda = \frac{\text{No. of component failures}}{\text{No. component-years of operation}}$$

$$= \frac{6}{4 \times 12}$$

$$= 0.125 \text{ failures/year.}$$

Since safety systems are passive until hazardous circumstances arise, and since it is unwise to wait for such circumstances to arise before finding out whether the safety systems are still operative, the systems are *tested* periodically. For reliability evaluation purposes, the system is assumed to be in a failed state for one-half the *test period* each time it fails. This is obviously the long-term average fault duration, although the actual fault duration on any particular occasion can be anything from 0 (ie, component fails just as test occurs) to one test period (ie, component failed at conclusion of previous test).

The fault duration, $t = \frac{T}{2} + r$,

where T is the test period in years, and r is the repair time in years.

Normally r<<T, and is neglected in reliability calculations. Accordingly, the usual formula for unreliability of safety systems is:

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

Example 3

Pickering Pressure Relief Valves are tested at a rate of 1 per month. Since there are 12 valves the test interval for each is one year, and hence:

$$t = \frac{T}{2} + r$$

$$= \frac{1}{2} \text{ year} + \text{few days}$$

$$\cong \frac{1}{2} \text{ year}$$

Example 4

During six years of operation, a power reactor experienced the following independent faults:

- two faults in the regulating system which rapidly increased the power to such an extent that the reactor was shut down by the protective system,
- three faults which would have prevented operation of the protective system if it had been called on to act, were detected by routine daily testing of the protective system.

Assuming the faults were repaired within minutes of being discovered, calculate the annual risk of a run-away accident in this reactor (ie, the average annual frequency of such accidents).

Solution

The annual risk A.R. of a run-away accident equals the regulation system failure rate λ_R times the fraction of time the protective system is unavailable, Q_p,

ie, $$A.R. = \lambda_R Q_p$$

$$= \lambda_R \lambda_p \frac{Tp}{2} \qquad (\because Q_p = \lambda_p \frac{Tp}{2})$$

$$= \left(\frac{2 \text{ failures}}{6 \text{ years}}\right) \left(\frac{3 \text{ faults}}{6 \text{ years}}\right) \left(\frac{\frac{1}{365} \text{ years}}{2}\right)$$

$$= 2 \times 10^{-4} \text{ accidents/year.}$$

ASSIGNMENT

1. In 12 years of operation of 30 pressure detection instrument lines in the containment system, 5 failures were detected. The instrumentation is tested semi-annually. What is the unreliability of a pressure detection line?

2. In 12 years of operation of 6 dump valves, 3 failures were found. The dump valves are tested twice weekly. Determine the valve unreliability.

3. Assume that the expected frequency of a complete unsafe failure of the NPD regulating system is once every 2 years. What is the annual risk of power excursions if the failure rate of the protective system is:

   (a) Complete system failure occurs once each year and the system remains in the failed state for 1 day.

   (b) Complete system failure occurs 6 times each year and failures are detected and corrected at the beginning of each shift.

4. Two pumps P_1 and P_2 operate in series. P_1 raises line pressure to meet P_2's intake requirements. The system will fail if either pump fails. If P_1 and P_2 have unreliabilities of 1.2×10^{-2} and 5×10^{-3}, respectively, calculate system unreliability.

5. Two identical pumps, each with unavailability of 2×10^{-2} are operated in a 2 x 100% arrangement. Calculate the unavailability of the system.

6. Weekly testing of a system of 15 switches has revealed 50 switch failures in 10 years' operation. Calculate the unreliability of a switch.

7. How often should a system of 12 dousing valves be tested in order to meet an unreliability target of 1.0×10^{-2}, if 15 valve failures have occurred during the past 5 years?

L.C. Haacke