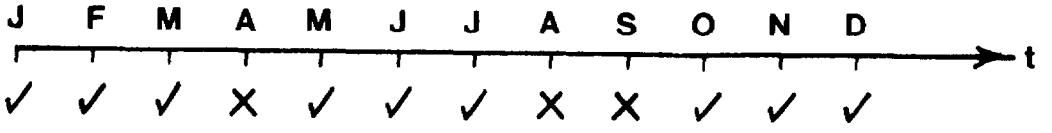
Mathematics - Course 121

SAFETY SYSTEMS ANALYSIS - SOLUTIONS TO SAMPLE PROBLEMS

Example 1

A passive safety system is tested on the first of each month. If a test reveals that the component has failed, it can be repaired within a few minutes and returned to service. The performance for one year is summarized on the time line below, where "x" denotes "component failed", and "✓" denotes "component operates satisfactorily".



Question

What is the *unavailability* of this component?

Definition

The unavailability of a component is the fraction of time the component is unable to perform its intended purpose.

Logically, the probability that a component is unavailable at any randomly chosen instant equals the component's unavailability. For example, if a component is unavailable 2% of the time, the probability is 2% that it will not perform its intended purpose if called upon at any randomly chosen instant. The distinction between the unavailability and unreliability of a component was drawn in lesson 121.00-4. For the moment, suffice it to say that the unavailability of a component may be regarded as the average value (expectation) of the time-dependent unreliability, provided that unavailability due to the testing process itself and due to repair time is negligible.

Based on the preceding definition and the scant data in this example, the component unavailability, Q, is defined as:

Q = fraction of time component unavailable

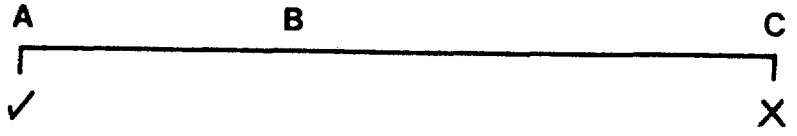
= (number of failures/year)(downtime in years per failure)

= (3 failures/y)(1/2 x 1/12 y/failure)

= 1/8

Notes

1. The downtime per failure is taken as one-half the test interval, not the whole test interval. The rationale for this is as follows: with reference to the following diagram showing the time interval between consecutive tests, the component failure detected at C could have taken place immediately following the previous test at A, just prior to test C, or at any instant B between A and C:



Thus, the time interval during which the component was actually unavailable could have been anything from zero up to the full test interval, T, but the average downtime per failure should be T/2. Hence, the component unavailability can be calculated via the formula:

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

where Q is the component unavailability (no units)
λ is the failure rate in failures per component-year, and
T is the test interval in years.

2. More accurately, the downtime per failure should include the average repair time, r, so that

$$Q = \lambda\left(\frac{T}{2} + r\right)$$

However, if $r << \frac{T}{2}$, which is often the case, r may be neglected. Trainees should assume r can be neglected unless told otherwise in course assignments and check-out questions.

---

* In fact, because the failure distribution function falls exponentially over the test interval (see lesson 121.00-8), the average downtime per failure is not exactly T/2. However, as shown in 121.00-8, Appendix, this formula is an excellent approximation providing $\lambda T << 1$.

3. The question naturally arises as to how confident one can be that the unavailability in this example is less than or equal to 1/8, especially in view of the very scant data base available. Obviously, one could be far more confident in this result if it were based on observing, say, 30 failures over a ten year interval rather than on just 3 failures over a one year interval. The question of *confidence limits* is treated briefly in Appendix 1, lesson 121.10-1.

Example 2

Calculate the unavailability of the protective system of a reactor if 22 failures have been detected during 4 years operation. Failures are detected and corrected at the beginning of each shift.

Solution

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

$$= \frac{22}{4} \times \frac{\frac{1}{3} \times \frac{1}{365}}{2}$$

$$= 3 \times 10^{-3}$$

Note that unavailabilities based on such poor statistical bases are seldom quoted to more than one or two significant failures.

Example 3

A safety system containing 12 identical components is tested weekly. Eleven component failures have been discovered during 7 years operation. Calculate the component unavailability.

Solution

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

$$= \frac{11}{12 \times 7} \times \frac{\frac{1}{52}}{2}$$

$$= 1.3 \times 10^{-3}$$

Example 4

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.

Solution

a) The annual risk of a power excursion (ARPE) is the probability of at least one excursion during one year. This is numerically nearly equal to the expected annual frequency of excursions (see lesson 121.00-8, Appendix, Section I).

ARPE = annual number of losses of regulation (LOR's) for which the protective system is unavailable

$= \lambda_R Q_P$,

where λ_R = number LOR's/year

= 1/2 per year

and Q_P = unavailability of protective system

= 1/365 year

$\therefore$ ARPE = 1/2 (1/365)

$= 1.4 \times 10^{-3}$

b) Using $Q_P = \lambda_P \frac{T_P}{2}$ for the unavailability of the protective system,

$$\text{ARPE} = \lambda_R \lambda_P \frac{T_P}{2}$$

$$= \frac{1}{2} \times 6 \times \frac{\frac{1}{3} \times \frac{1}{365}}{2}$$

$$= 1.4 \times 10^{-3}$$

Example 5

Information

Assume the following results were obtained in NPD Safety system tests over a 5 year period.

a) 13 protective system single channel failures - each channel tested every 2 days.

b) 12 Reactor Vault dousing valve failures - each valve tested once per month.

c) 12 Reactor Vault containment damper failures - each damper tested twice per year.

Unsafe failure of safety systems are defined as the events:

- Protective system - E_1: 2 or more of the 3 independent channels in a failed condition simultaneously.

- Reactor Vault containment system - E_2: 1 or more of the 2 dousing valves in a failed condition or E_3: both of the double containment dampers in either the inlet or outlet ducting in a failed condition.

Problem

If the expected frequency of unsafe regulating system failures is 10^{-1} per year what is the annual probability of:

a) A nuclear incident resulting from coincident failure of the regulating and protective system.

b) A nuclear accident resulting from coincident failure of the regulating, protective and Reactor Vault containment systems.

Solution

a) As in Example 4, the annual risk of a power excursion (ARPE) due to coincident failure of regulating and protective systems is given by:

$$ARPE = \lambda_R Q_P, \tag{1}$$

where $Q_P = P(E_1)$

$$= {}_3C_2 Q_c{}^2 R_c + {}_3C_3 Q_c{}^3, \tag{2}$$

where the unavailability of a channel,

$$Q_c = \lambda_c \frac{T_c}{2}$$

$$= \frac{13}{3 \times 5} \times \frac{\frac{2}{365}}{2}$$

$$= 2.4 \times 10^{-3} \qquad (3)$$

(The channel availability $R_c = 1-Q_c$

Note that the binomial coefficients ${}_3C_2$ and ${}_3C_3$ in equation (2) account for the numbers of possible combinations of 2 failed channels and 3 failed channels, respectively, from 3 channels. Substituting (3) in (2) gives

$$Q_P = 1.7 \times 10^{-5} \qquad (4)$$

Substituting (4) in (1) gives

$$\underline{\underline{\text{ARPE} = 1.7 \times 10^{-6}}} \qquad (5)$$

b) The annual risk of a nuclear accident (ARNA) is found as follows:

ARNA = annual number of LOR's for which <u>both</u> Protective and Containment systems are unavailable*

$$= \lambda_R Q_P Q_{CT}, \qquad (6)$$

where λ_R = annual frequency of LOR's

Q_P = unavailability of protective system, and

Q_{CT} = unavailability of containment system.

---

* Again, the RHS of this expression is actually the expected annual <u>frequency</u> of nuclear accidents, but this is <u>numerically</u> nearly <u>equal to the probability</u> of one or more accidents per annum, providing $\lambda_R Q_P Q_{CT} \ll 1$ (see 121.00-8, Appendix, Section I).

Now $Q_{CT} = P(E_2 \cup E_3)$

$$= P(E_2) + P(E_3) - P(E_2)P(E_3) \quad \ldots PR3 \tag{7}$$

Let Q_V, Q_D represent unavailabilities of a dousing valve, and a containment damper, respectively.

Then $P(E_2) = {}_2C_1 Q_V R_V + {}_2C_2 Q_V^2$ (8)

where $Q_V = \lambda_V \frac{T_V}{2}$

$$= \frac{12}{2 \times 5} \times \frac{\frac{1}{12}}{2}$$

$$= 0.05 \tag{9}$$

$\therefore P(E_2) = 0.098$ (from (9) in (8)) (10)

And $P(E_3) = Q_D^2 + Q_D^2 - Q_D^4$ (11)

where $Q_D = \lambda_D \frac{T_D}{2}$

$$= \frac{12}{4 \times 5} \times \frac{\frac{1}{2}}{2}$$

$$= 0.15 \tag{12}$$

$\therefore P(E_3) = 0.044$ ((12) in (11)) (13)

$\therefore Q_{CT} = 0.14$ ((10) and (13) in (7)) (14)

$\therefore$ ARNA $= 2 \times 10^{-7}$ ((4) and (14) in (6))

Example 6

Information

The target or maximum permitted unavailability for the NPD Reactor Vault containment provisions is 10^{-2}. Assume only the following groups of components can cause unsafe system failure and that the expected unavailability of each group is as indicated:

- Dousing tank and lines - $1 \times 10^{-3} = Q_a$
- Control circuits - $4 \times 10^{-4} = Q_b$
- Exhaust damper - $1 \times 10^{-3} = Q_c$
- Isolation dampers - $3 \times 10^{-3} = Q_d$
- Dousing valves - unknown $= Q_e$

Two dousing valves are provided, both of which must operate to prevent a nuclear accident.

Problem

If experience shows that each dousing valve will fail unsafely once every 20 years, how often should the valves be tested?

Solution

$$Q_a + Q_b + Q_c + Q_d + Q_e = 10^{-2}$$

Substituting given values of Q_a, Q_b, Q_c, Q_d gives

$$Q_e = 4.6 \times 10^{-3}$$

But Q_3 = P(at least one dousing valve fails)

= 1 - P(both valves survive)

$$= 1 - (1 - Q_V)2$$

where Q_V = dousing valve unavailability

Substituting (1) in (2) gives

$$Q_V - 2.3 \times 10^{-3}$$

ie, $\lambda_V \frac{T_V}{2} = 2.3 \times 10^{-3}$ $(\lambda_V = \frac{1}{20}$ f/y)

$\therefore T_V = 0.092$ years

$\therefore$ a suitable test frequency is once per month.

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 unavailability 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 unavailability.

3. 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.

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

5. Weekly testing of a system of 15 switches has revealed 50 switch failures in 10 years operation. Calculate the unavailability of a switch.

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

7. A system of 12 dousing valves, tested monthly, has developed 10 failures of individual valves in 8 years operation. Calculate the unavailability of an individual valve.

8. Calculate the annual risk of a nuclear accident at a reactor, which, during 9 years operation, developed the following faults:

   3 unsafe failures of the regulating system, and

   50 complete failures of the protective system, failures of which are detected and corrected at the beginning of each shift.

9. At a certain nuclear generating station, three independent divisions of equipment protect against nuclear accidents:

   (i) process equipment with a failure frequency of 0.3 per annum,

   (ii) protective equipment with unavailability of 2×10^{-3}, and

   (iii) containment equipment with unavailability of 5×10^{-3}

   Calculate the annual risk (frequency of)

   a) an incident consisting of process failure combined with simultaneous failure of either protective or containment systems.

   b) simultaneous failure of all three systems.

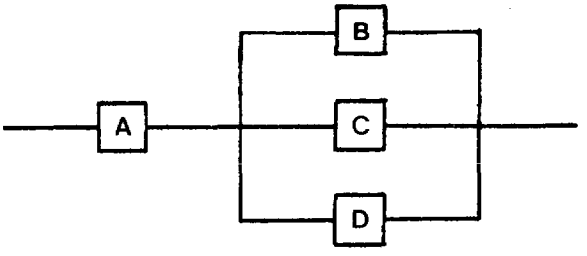
10. Monthly testing of 6 safety switches has revealed 8 failures of individual switches during 15 years operation.

   a) Calculate the unavailability of a switch.

   b) How, without altering the equipment, could the unavailability in (a) be decreased by a factor of about 30?

   c) How often should the switches be tested if the permitted unavailability of a switch is 10^{-2}?

11.



In the above system, a system failure consists of a failure of either component A, or a failure of at least two of B, C, D.

Calculate the unreliability of the system, given component unreliabilities,

$Q_A = 0.05$, and
$Q_B = Q_C = Q_D = 0.1$.

12. A pump designed for continuous operation has failed 6 times in 5 years operation, with total down time of 124 hours. Calculate the unavailability of

    a) the pump

    b) a system of three such pumps in a 3 x 50% parallel arrangement.

13. Information

The permitted unavailability of the Douglas Point light water injection system is defined as 10^{-2} in accordance with predictions made in Appendix I of the Safety Report. Before this system will provide injection flow, the following components must actuate:

a) A level switch in either inlet header to indicate the need for injection.

b) A pressure switch across appropriate headers to indicate the direction of injection.

c) At least 5 isolating valves open to pass injection flow.

l) Assume that the expected unavailability of the injection system is

$Q_T = Q_{LS}^2 + Q_{PS} + 5Q_{PV}$ where Q_T = expected system unavailability

Q_{LS} = expected level switch unavailability

Q_{PS} = expected pressure switch unavailability

Q_{PV} = expected isolating valve unavailability

2) Assume that injection system component failure rates are predicted to be

Level switch failure rate $\lambda_{LS} = 0.02$ per year

Pressure switch failure rate $\lambda_{PS} = 0.02$ per year

Isolating valve failure rate $\lambda_{PV} = 0.05$ per year

Problem

a) What is the expected system unavailability if all components are tested once per month and failure rates are as predicted?

b) What is the expected system unavailability if all components are tested once per month, and failure rates of valves and pressure switches are as predicted, but failure rates of level switches are double predicted rates?

NB The remainder of this assignment consists of questions abstracted verbatim from recent AECB Nuclear General Examinations (Shift Supervisors').

14. Question #9, February 1976

Suppose that over a period of four years, daily testing of a safety system has revealed twenty faults which would have prevented operation of the system if it had been called upon to act. Assuming the faults were repaired within a short time of being discovered, show that this testing gives reasonable assurance that there was no greater than a 1% probability of the fault existing at any given time. Qualitatively explain why the demonstrated reliability of the system would be less if the same number of faults were found by weekly testing.

15. Question #8, October 1976

a) 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 probability of a runaway accident in this reactor.

b) During the same six years of operation, faults occurred in the containment system as follows:

- several incidents of inoperative air lock seals, totalling 40 hours of loss of containment due to defective air locks.

- four faults in the containment logic system which would have prevented effective containment in the event of an accident. These faults were detected in routine weekly testing and each time were repaired within minutes of being discovered.

Calculate the probability for this reactor of a runaway accident accompanied by release of radioactivity to the environment.

16. Question #6(a), February 1977

Although safety systems must be extremely reliable, they generally contain switches, relays, valves, etc., that are relatively unreliable. Explain how an extremely reliable system can be obtained and maintained when it is composed of relatively unreliable components.

17. Question #7, June 1977

Give and explain three reasons why reactor safety systems should be tested routinely.

18. Question #9, February 1978

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

- three faults in the regulating system which rapidly increased the power to such an extent that the reactor was shut down by the protective system.

- two 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.

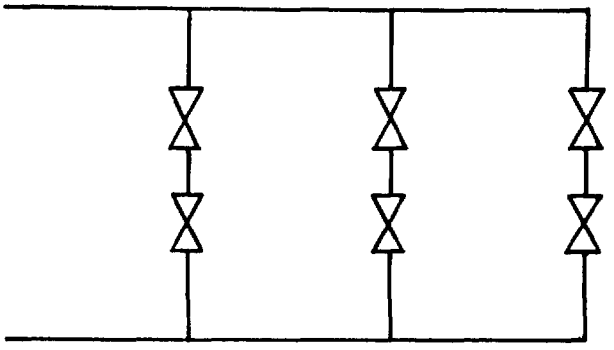
Assuming the faults were repaired within minutes of being discovered:

a) calculate the expected frequency of runaway accidents in this reactor,

b) calculate the probability of having, during one year, one or more faults in the regulating system which rapidly increase the power.

A partial table of exponential functions is attached for your optional reference.

19. Question #5, June 1978



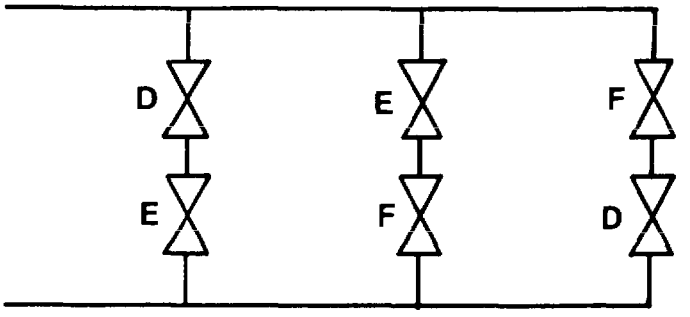
The above diagram is a schematic representation of the typical dump valve arrangement for a reactor with moderator dump. In 5 years of operation of this reactor, 6 failures (to open) of individual dump valves were found. The dump valves are tested twice a week.

a) Calculate the unreliability of:

   i) a dump valve
   ii) a dump line.

b) If the correct operation of 1 dump line is sufficient to achieve an efficient dump, calculate the unreliability of the dump system due to dump valve failures.

20. Question #6, October 1978



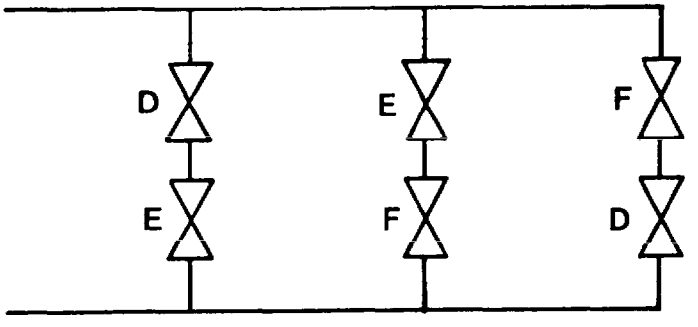
The above diagram is a schematic representation of the typical dump valve arrangement for a reactor with moderator dump. The opening and closing of valves D, E and F are controlled by channels D, E and F respectively. During 5 years of reactor operation, the electronics of channels D, E and F were tested three times a week and 4 unsafe failures of individual channels were found.

a) Calculate the unreliability of a dump channel.

b) If the correct operation of 1 dump line is sufficient to achieve an efficient dump, calculate the unreliability of the dump system due to dump channel failures. (Show your reasoning.)

c) Suppose that during a test, channel F fails to operate. Calculate the unreliability of the dump system due to dump channel failures, if reactor operation were to be maintained in spite of channel F failure.

21. Question #7, February 1979



The above diagram is a schematic representation of the typical dump valve arrangement for a reactor with moderator dump. The opening and closing of valves D, E and F are controlled by channels D, E and F respectively. The

correct operation of any one pair of dump valves in series is sufficient to achieve an efficient dump.

During 5 years of reactor operation, the control circuits of channels D, E and F were each tested three times a week and a total of 4 unsafe failures of individual channels were found. Over the same period, the dump valves were mechanically tested twice a week and a total of 7 failures of individual dump valves to open were found.

a) Calculate:

   i) the unreliability of the control circuit of a dump channel;

   ii) the mechanical unreliability of a dump valve.

b) Suppose that the control circuit of one channel fails to operate during a test. The reactor continues operation with the defect uncorrected and, due to operator error, the two dump valves associated with the defective channel are left in the closed position.

   i) Calculate the resulting unreliability of the dump system.

   ii) Suppose that the shift supervisor notices the error and the defective channel is rejected correctly, ie, the two dump valves associated with the defective channel are opened. Calculate the resulting unreliability of the dump system.

L. Haacke