PI 21.04

AVAILABILITY OF SAFETY SYSTEMS

OBJECTIVES

4.1 Define and give an example of the following terms:

a) A Safety Related System
b) A Poised System
c) A Standby Safety Support System
d) A Special Safety System
e) An Active System

4.2 a) Describe in words, or mathematically, the relationship among failure rate, test interval and unavailability.

b) Explain how the availability of a passive system can be increased without any physical changes to the system.

4.3 Calculate the unavailability of a tested component.

4.4 a) List and explain four reasons for testing safety systems.

b) List and explain four reasons for limiting testing of safety systems.

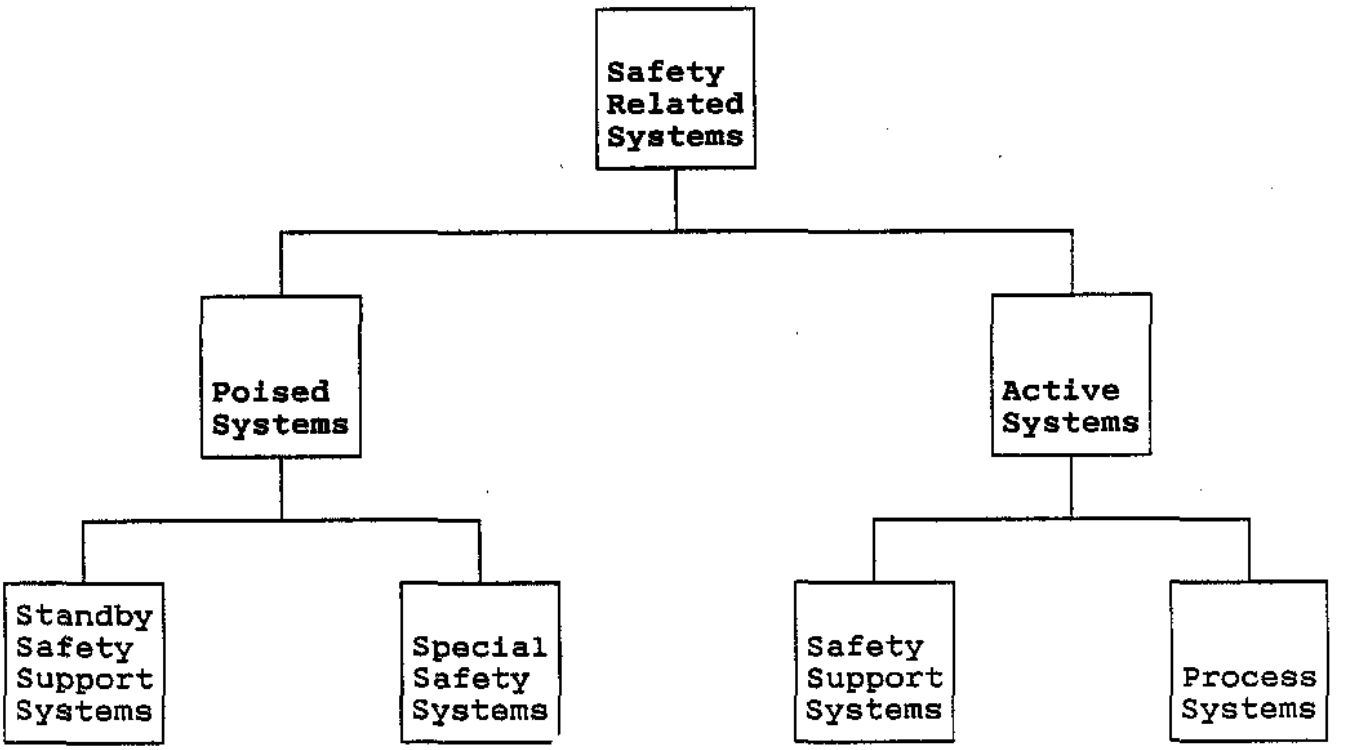
4.5 Calculate the probability of single and dual failures involving process and safety systems.

4.6 Describe and give an example of a Level I impairment of a Safety System.

COURSE NOTES

In this module, we will be looking at the reliability of Safety Systems, so it is important to take a few minutes up front to go over some of the terminology used when describing them. There are many definitions of the various classifications of systems but the ones given here are those generally used in station technical reports.

For the purpose of assessing failures which could lead to the escape of radioactivity, station systems which provide a safety function are classified as **Safety Related Systems.** They are then subdivided into the classifications shown on the next page.



Safety Related Systems

Those systems which are intended to:

a) Control

Regulate the reactor under all normal plant and anticipated transient conditions and to maintain the reactor core in a safe state for an extended period.

b) Cool

Cool the reactor core under all normal plant and anticipated transient conditions and to maintain the reactor core cooling for an extended shutdown period under such conditions.

c) Contain

Limit the release of radioactive materials to meet the criteria established by the licensing authority, with respect to radiation exposure.

Poised Systems

The term poised is applied to those systems which usually play no part in the normal production process but remain available, ready to operate to minimize the consequences of a process system failure. All special safety systems and standby safety support systems are classified as poised.

Component failures on poised systems tend not to be revealed immediately and routine testing is the principal method of fault detection.

Examples of poised systems are Emergency Power System, the dousing water system and the auxiliary boiler feed system.

Standby Safety Support Systems

A standby safety support system is a poised system which will prevent the occurrence, or mitigate the consequences, of a serious process failure. However, it may perform other normal operating functions in addition to its safety support role.

Examples of standby safety systems are Instrument Air System, service water, Emergency Power System and emergency air.

Special Safety Systems

A system designed specifically to prevent significant releases of radioactivity to the public in the event of a serious process failure. There are three types of special safety systems.

a) Shutdown Systems
b) Emergency Coolant Injection Systems
c) Containment Systems

A Special Safety System has no purpose other than to Control the reactor, Cool the fuel and Contain any releases of radioactive material. It is not used in day-to-day operation and usually has its own detectors, trip logic and equipment so that it is independent of any failures of normal process systems.

Active Systems

A term applied to those safety-related systems which are an integral part of the normal production process. Component failure on active systems tends to be revealed immediately. The impact of the failure is usually immediately obvious and the Operator can initiate prompt corrective action.

Active safety-related systems are broken down into two groups, Safety Support Systems and Process Systems.

Safety Support Systems

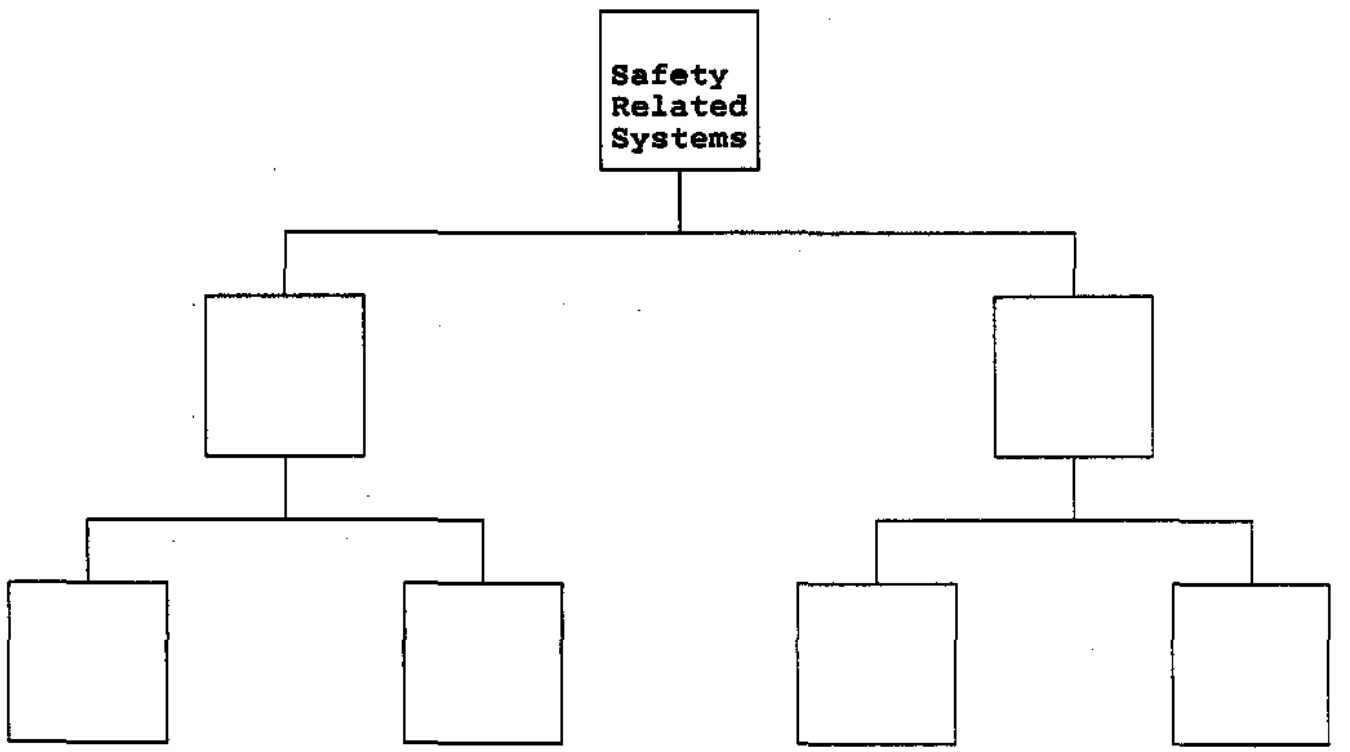
These are those systems which are active and support or are a part of the Special Safety systems described earlier. Examples of this type of system are the Low Pressure Service Water System (which provides cooling water to many heat exchangers) and the Instrument Air System (which is used to open and close valves).

Process Systems

In Module 3, we looked at process systems as those systems which are involved in the "process" of the conversion of fission heat to electricity. Some of these systems, although normally active and used in normal operation also can play a safety-related role in the event of an accident. This can be by acting as a heat sink (service water for example) or a heat transfer medium (primary heat transport coolant) or by providing control to instruments and equipment (Class II electrical power, instrument air).

EXERCISE

1. **Fill in the following diagram showing the subdivisions of safety related systems:**



Unavailability

As you with great memories no doubt recall, in Module 1 we gave a definition of Availability. For those whose memories are good but just short, we'll review it here. The availability of a component is that fraction of time that it is able to perform its intended purpose. It then follows that unavailability (Q) is that fraction of time that a component is not able to perform its intended purpose. This is equal to the probability that a component is unavailable at any randomly chosen instant.

So how do we find out the fraction of time that a component is unavailable? Well, it's definitely unavailable when it's broken and while it's being fixed, so we get: Q = [number of times it is broken] x [how long it is unavailable each time it is broken]. For systems which are active, it is easy to determine these figures because when something fails, you know about it right away. For systems which are poised, the only way we can find out about failures in some components is by testing.

Now suppose that we've been testing something once a week and the last time we checked, it was working fine. However, this week when we test it, we find that it has failed. How long has it been unavailable? It could be anything from the entire time since the last test to just a few moments before we tested it this week. For our calculations we take the average and assume that it has been in a failed mode for one half of the time since the last test. This then gives us the equation for the calculation of unavailability of tested components or systems:

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

Where T is the test interval or time between tests in years
r is the repair time in years
λ is the failure rate in failures per component year

If the repair time is small compared to the test interval, we can simplify the equation to:

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

The following examples illustrate how this is used.

EXAMPLE ONE

For a component which is tested weekly, it was discovered that there were 5 failures in the last 7 years of operation. What was the unavailability of the component during this time?

Solution

Using the equation, we have a test interval of one week or 1/52 years, a failure rate of 5/7 failures per year. If we assume that the repair time is negligible, then the unavailability is:

$$Q = 5 \frac{\text{failures}}{7 \text{ years}} \times \left(\frac{\frac{1}{52} \text{ years}}{2}\right)$$

$$= 7.0 \times 10^{-3} \text{ years/year}$$

EXAMPLE TWO

Calculate the unavailability of the protective system of a reactor if 22 failures have been detected during 4 years of operation. Failures are detected and corrected at the beginning of each 12 hour shift.

Solution

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

$$= \frac{22 \text{ failures}}{4 \text{ years}} \times \frac{\left(\frac{12}{24} \times \frac{1}{365}\right) \text{years}}{2}$$

$$= 4.5 \times 10^{-3} \text{ years/year}$$

NOTE: The units of Unavailability have been expressed as years per year here but can also be and often are, expressed as hours per year, days per year or some other units of time per time.

For the Special Safety Systems, the target unavailability is 10^{-3} years per year or about 8 hours per year.

EXERCISES

2. Why are poised safety-related systems tested?

3. 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?

Looking at the equation for calculating unavailability, a little algebraic examination will tell you that the unavailability of a component or system can be altered by merely changing the test frequency.

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

Although this may seem like lying with statistics, it actually is quite legitimate. If you test something more often, you have a better idea of whether or not it is working. Taken to the extreme, if we keep the component in operation continuously, you can be sure that it is always available. In fact, we do this with the standby generators when we want to ensure that we have backup power available in situations where some of the units in a station are shutdown or otherwise unable to supply backup power to a unit that is running.

Testing of Safety Systems

So, you can see from the above discussions that it is important to test safety systems. Specifically there are a number of reasons that this should be done. These are:

1) To discover failed components so that they can be repaired or replaced.

2) To maintain system unavailability below a specified maximum value (proactive). In other words, reduce the time that the system is unavailable.

3) To check whether or not unavailability targets are being met (reactive), so that corrective action such as upgrading the system and/or more frequent testing can be taken if the targets are not met. This also satisfies the conditions of the AECB operating license.

4) To build up a data bank of component failure rates for use by designers in either modifying existing systems or designing future systems.

However, in spite of all these reasons for testing safety systems, there are a few good reasons for limiting the frequency of testing.

1) Excessive testing can cause excessive wear on the system or components.

2) The testing process itself can contribute to system unavailability. Some tests involve removing the component from service which means that for the duration of the test, it is unavailable.

3) The more human intervention, the greater the risk of inadvertently leaving the system in a downgraded state.

4) If the systems are tested too often, it can increase the risk of unplanned outages. If during a test, human error or random failures results in shutting down the reactor when it doesn't need to be shut down, there is an economic penalty.

Combinations of Failures

Up to now, we have been looking at failures of Process Systems in Module 3 and Safety Systems in this module. Back in Module 2, we looked at the probability of combinations of events, which are applicable in situations where we are interested in the probability of one thing happening AND/OR another thing happening. In the discussion of unavailability, we often need to consider those combinations of events. For example "what is the probability of the Reactor Regulating System failing and the Shutdown Systems being unavailable?" "What is the probability of a Shutdown System and the Containment System being unavailable at the same time?" The answer to these and other questions are usually calculated using some of the same techniques that you have used up to now.

There's really nothing too difficult about these calculations. In most cases, it is simply the AND relationship which means that we multiply the probabilities together. So, if we want the probability that the Regulating System will fail **AND** the Shutdown System will be unavailable, we simply multiply the failure rate of the Regulating System by the Unavailability of the Shutdown System. This type of failure is referred to as a Dual failure where a Process System fails along with the Safety System required to act in that event. The following example will illustrate how these are done. Warning: Do not attempt to do this at home. These examples have been done by trained professionals (and after this, you'll be trained professionals)!

EXAMPLE THREE

Assume that the Reactor Regulating System for a large nuclear unit has failed 3 times in 7 years of operation. The shutdown system, which is tested once per shift, has had 16 failures in the same 7 years. These failures were detected and corrected very quickly at the beginning of each 12 hour shift. What is the probability of the regulating system failing at the same time that the shutdown system is unavailable?

Solution

Probability of Dual Failure = Probability of Regulating System Failure **AND** Shutdown System being unavailable

$$= \lambda_{Reg} \times Q_{Shutdown}$$

$$= \lambda_{Reg} \times (\lambda_{Reg} \times \frac{T}{2})$$

$$= \frac{3 \text{ failures}}{7 \text{ years}} \times (\frac{16 \text{ failures}}{7 \text{ years}} \times \frac{(\frac{12}{24} \times \frac{1}{365})}{2})$$

$$= 6.7 \times 10^{-4} \text{ failures/year}$$

Safety System Impairments

At times, it is possible for safety systems to be impaired (no, this doesn't mean that someone put alcohol in the poison injection tanks). It means that the system cannot perform its function totally as intended. The seriousness of this is classified according to Impairment Levels which provide Operator action guidelines and objectives for a variety of safety system faults. The levels range from the most serious, Level 0, to the least serious, Level 3.

Level 0: The system is totally incapacitated such that it would not have provided any protection under any circumstances.

Level 1: The system effectiveness is significantly reduced such that it would have been of little or no benefit if any possible process system failure had occurred which required that system. The system is not effective in keeping releases below allowable limits for either the worst case or lesser events.

Level 2: The system effectiveness is marginally reduced to below the design intent. The system is effective for keeping releases below allowable limits for lesser events but not the worst case.

Level 3: There is a reduction in system redundancy or margin of safety (however, design intent can still be fulfilled).

SUMMARY

In this module, we have discussed:

- Definitions and examples of:
  - A Poised System
  - An Active System
  - A Safety Related System
  - A Special Safety System
  - A Standby Safety System
- The relationship among failure rate, test interval and unavailability.
- Calculations of unavailability.
- Reasons for testing Safety Systems and reasons for limiting the amount of testing.
- Calculations of dual and triple failures.
- Impairments of Safety Systems.
- Significant Events as they pertain to an NGS.

ASSIGNMENT

1) For the following examples of systems, identify whether they are:

A - An Active Safety Related System
B - A Special Safety System, or
C - A Standby Safety Support System

_____ i) Shutdown System One

_____ ii) The Reactor Regulating System which is used during normal operation

_____ iii) Emergency Boiler Cooling

_____ iv) Containment System

_____ v) Emergency Water System

_____ vi) Standby Generators

2) How is the unavailability of a tested component determined?

3) Give four reasons for testing Safety Systems.

i)

ii)

iii)

iv) _____

4) Give four reasons for limiting the testing of Safety Systems.

i) _____

ii) _____

iii) _____

iv) _____

5) In five years of operation, there were two faults on the Reactor Regulating System which would have allowed the reactor power to increase uncontrolled if the Shutdown Systems were not available. During this same time, the Shutdown System was tested daily and two faults were discovered. In all cases, the failures were repaired in a very short time. Based on this data, what is the probability of the regulating system failing at the same time that the Shutdown System is unavailable?

This Module Prepared By: Richard Yun, WNTC