Reactor Boiler and Auxiliaries - Course 133

SAFETY SYSTEM PERFORMANCE

The development of a safety standard, for nuclear power stations was discussed in a previous lesson. The standard applied to NPD was that the annual risk of a nuclear accident should be less than 10^{-5}.

This lesson considers some of the techniques being developed, at NPD and more recent stations, to measure the effectiveness of safety systems against this safety standard.

The Probability of Nuclear Accidents

Nuclear accidents may be defined as circumstances during which sufficient quantities of fission products escape from the fuel to populated areas to cause injuries or deaths.

The escape of fission products is prevented by the various containment barriers, each of which must fail before an accident can occur. If all barriers were completely independent so that no fault could affect more than one barrier then the annual accident probability could be calculated by taking the annual probability of failure of each barrier and obtaining the product of all terms. Thus, if the annual probability of failure of each of 5 containment barriers was 1/10 then the annual accident probability would be $(1/10)^5$ or 10^{-5}, the required standard. If on the other hand a single fault could cause failure of all containment barriers, then the annual accident probability would become the annual probability of the fault.

The faults which can potentially effect more than one containment barrier are less probable than other faults, but they are, nevertheless, of greatest concern in the design and operation of nuclear power stations. The safety systems, as discussed in the previous lesson, reduce the probability of such faults by independently protecting the containment barriers. Thus, nuclear accidents can not occur unless there are simultaneous failures of the following equipment:

(a) The process equipment which normally prevents fuel failures by restricting power production in the fuel and maintaining adequate heat removal from the fuel. Fuel failures are possible if the fuel temperature increases because of failure of this equipment, either as a result of mechanical faults or human error.

(b) The protective equipment fails to limit fuel temperatures either by rapid shutdown of the reactor or by emergency injection. Fuel and fuel sheath failures then occur.

(c) The containment equipment fails to prevent the escape of fission products, which were released into the heat transport system, to inhabited areas.

If the protective equipment and containment equipment are constructed and maintained independent of each other and the process equipment, so that they are not affected by the same faults then the annual accident probability is reduced to the product of the annual probability of failure of each group of equipment. Thus, if an analysis of process equipment indicated that the probable frequency of faults which may cause fuel failures is once per year, then our safety standard would indicate that the annual probability of failure of both the protective and containment equipment should be less than 10^{-5} per year or typically an annual failure probability of 3×10^{-3} for the protective equipment and 3×10^{-3} for the containment equipment.

Safety System Performance

Increased favourable operating experience in nuclear power stations will lead to an increased confidence that a nuclear accident will never occur, as a result of simultaneous failures of process, protective and containment equipment. The safety standard can, however, be used to set an acceptable failure rate for individual process or safety systems and to judge the required effectiveness of the safety systems.

A tentative Reactor Siting and Design Guide, prepared by the Atomic Energy Control Board of Canada sets the following limits for equipment failures:

1. Single Failures - failures of process equipment which could lead to fuel failures but are safely terminated by protective and containment equipment should not exceed 1/3 per year.

2. Dual Failures - failures of process equipment potentially leading to fuel failures combined with failures of either protective or containment equipment should not exceed 1 in 1000 years or an annual risk of 10^{-3}. Dual failures are terminated by correct operation of the remaining containment or protective equipment.

The Siting Guide, which is discussed in Course 131, sets standards for the maximum allowable fission product release following single and dual failures. The allowable releases are limited both by an allowable individual and an allowable integrated population dose. Process failures only are assumed to be frequent enough to form part of the normal operating effluent

and the release is limited by the allowable annual exposure of the general public. The release following dual failures is limited below the allowable once per lifetime exposure of the the general public since these would not occur more often than once per 1000 years.

These standards set limits for the required effectiveness of safety systems, (eg, leak tightness of building containment), and for the allowable annual failure probability of the safety systems.

Safety System Unreliability

Safety systems are normally inactive and are only required to operate if there is some process equipment failure. Thus, faults which incapacitate the system may develop and go unnoticed until operation is attempted. To avoid this, safety systems are tested regularly and all observed faults promptly recorded, corrected and their duration estimated.

An estimate of the system reliability can be calculated as the proportion of total time during which the system would have operated correctly if called upon. However, this normally results in numbers which are awkward to use, such as 99.999. To simplify the mathematics the proportion of total time during which the system would have failed to operate is calculated resulting in a number such as .001 or 1×10^{-3}. This portion of total time, during which it was in a failed condition, or the probability of failure, is identified as the system unreliability.

The duration of a fault is frequently difficult to estimate so it is usually assumed that it occurred at the mid point between discovery and the last successful test. Thus, if a system is tested daily and one fault is discovered, during a year, which causes system failure then the system unreliability can be calculated as follows:

$$P = \frac{\text{Duration of Failed Condition}}{\text{Total Time}} = \frac{FT}{2}$$

where P is the system unreliability, F the number of faults per year and T the test interval in years.

In the case quoted; $F = 1$ and $T = 1/365$

$$\text{Therefore, } P = \frac{1 \times 1}{2 \times 365} \approx 0.001$$

Component Unreliability

It may be impractical to completely test all the safety systems after a nuclear power station is operating. It may also be that system failures are so rare that it would take too long to accumulate valid statistics on system unreliability. If the components of each safety system are carefully tested, it is possible to obtain an accurate estimate of the system unreliability from an analysis of the observed component faults.

If the indicated unreliability of a component is too high it may be improved either by reducing the test interval or by reducing the failure frequency.

For a reduction in test interval it is usually necessary that facilities for remote on power tests be available since many components are located in areas that are accessible only during shutdown and shutdowns must occur with a minimum of frequency in base loaded nuclear power stations.

If the component failure frequency cannot be reduced by replacement or maintenance then redundant components should be provided so that system failures do not occur unless there are multiple component faults. If these components are <u>independently</u> arranged so that they are not affected by the same fault then the system unreliability is a function of the <u>product</u> of their individual failure rates.

Suppose, for example, that 3 independent pumps are available for adding injection water following a process failure and that any one pump will provide sufficient flow to prevent fuel failures. If the pumps are tested once each year and records indicate that on the average one pump fails every 3 years then the unreliability of each pump can be calculated as follows:

$$P = \frac{\text{Duration of Failed Condition}}{\text{Total Time}} = \frac{F}{n} \times \frac{T}{2}$$

where P is the unreliability of each pump, F is the average failures per year for all pumps, n is the total number of pumps and T is the test interval in years.

In the example, $F = 1/3$, $n = 3$ and $T = 1$

Therefore, $P = \frac{1}{3} \times \frac{1}{3} \times \frac{1}{2} \approx 0.06$

The unreliability of all three pumps, (ie, the probability that they will all fail at the same time), is approximately P^3 or 0.0002. This is the safety system unreliability due to the pumps.

The analysis of each safety system will show that it may fail for any one of several reasons. Thus, an emergency injection system may fail if pumps fail, or if valves do not open, or

if a water supply is not available. The calculated unreliability of the safety system is the sum of the unreliabilities of each of these groups of components. Therefore, the unreliability of each group must be less than the required unreliability of the system.

Operating Considerations

Experience at NPD has indicated that the deterioration of components, which sit idle and unattended for long periods of time in inaccessible areas, tends to be higher than predicted. This applies to both moveable components, such as valves and dampers, and static components such as lines containing stagnant water. On the other hand the performance of components which can be tested frequently has been better than predicted and so provision should be made for remote component tests wherever possible.

If facilities are available for on power safety system component tests, then the facilities must provide either for continued availability of the system during the test or for its rapid return to service. For routine testing these facilities must not interfere with normal operation of the station. Thus, if dousing components are tested, all lines must be drained remotely to avoid spilling of dousing water into the reactor area.

ASSIGNMENT

1. (a) Which faults are of greatest concern in the design and operation of nuclear power stations?

   (b) How do the safety systems reduce the probability of such faults?

2. What limits for equipment failures are set by the AECB Reactor Siting and Design Guide?

3. (a) Why is it desirable to test safety systems regularly?

   (b) A safety system is tested once every six months and one fault was discovered in 4 years. What is the apparent system unreliability?

   (c) Why would the unreliability, as calculated in 3(b), not be too valid?

4. How can component testing provide an estimate of the system reliability and what previous experience suggests that provisions should be made for remote component tests whenever possible?

R. Kelly