Mathematics - Course 121

SAFETY SYSTEMS ANALYSIS

I NUCLEAR PLANT SYSTEMS

Nuclear Plant systems may be classified into two major categories - Process systems and Safety systems.

Process Systems

Process systems are systems active in the normal functioning of the plant, ie, all the systems involved in the "process" of converting fission heat to electrical energy.

Examples:
- Heat Transport Circulating System and Auxiliaries
- Steam-feedwater System and Auxiliaries
- Turbine Lube Oil System
- Heat Transport Pressure Control System
- Reactor Regulating System

Safety Systems

Safety systems are passive during normal plant operation, but act following process failures to prevent fuel damage and escape of radioactivity to the environment. The Safety systems are, specifically,

(1) *Shutdown Systems #1 and #2 (SDS1 and SDS2)*, which automatically trip (shutdown) the reactor on process upsets such as high coolant pressure, low coolant flow, high neutron power, etc.

(2) *Emergency Core Injection System (ECIS)*, which supplies coolant to the core following a *Loss of Coolant Accident (LOCA)*. The ECIS is triggered on low coolant pressure.

(3) *Containment System*, which acts to contain radioactivity within certain areas of the plant. This system consists of the following:

- dampers and valves (for sealing off ducts and pipes which penetrate the containment boundary.
- dousing equipment, and at the multi-unit plants, a vacuum building, for minimizing the pressure rise within the Containment boundary following a LOCA.

Protective System

The Protective System consists of those systems which act to prevent fuel damage following process failures, namely, the Shutdown Systems SDS1 and SDS2 and the ECIS.

To summarize, there are three independent divisions of equipment which protect against nuclear accidents at CANDU stations:

(1) Process
(2) Protective
(3) Containment

Note that the safety systems are designed to protect against "nuclear", not conventional accidents.

DEFINITION: A *conventional accident* is an event resulting in death or injury due to causes other than exposure to radiation, eg, electric shock, falling off a scaffold, slipping on an oily surface, etc.

DEFINITION: A *nuclear accident* is an event resulting in death or injury due to contact with radioactive material.

The CANDU design provides five barriers between radioactive fission products and members of the public.

(1) Ceramic fuel pellets (which entrap fission products)
(2) Fuel Sheath
(3) Heat Transport Boundary
(4) Containment Boundary
(5) Exclusion area around the plant.

The most dangerous possible causes of nuclear accidents are those Process failures which could cause several of these barriers to fail at once, namely

- a Loss of Coolant Accident (LOCA)
- a power excursion due to a Loss of Regulation (LOR)

However, neither of these accidents would result in public injuries or deaths unless both Protective and Containment systems also failed.

Note also that the Process, Protective, and Containment systems are deliberately designed to be independent so as to minimize the probability of losing more than one system at once, and hence to minimize the probability of nuclear accidents. For example, if the Shutdown System were using the same neutron flux detector as the Regulating System, then a failure of that one detector would impair both Process and Protective systems at once.

II UNAVAILABILITY OF SAFETY SYSTEMS

DEFINITION: The *unavailability* of a safety system is the fraction of time that the system in unavailable to perform its intended purpose.

For example, if a system spends 2% of its time in a failed state, then system unavailability Q = 0.02, and system availability R = 1 - Q = 0.98. In other words, at any randomly chosen instant of time, the probability that the system is unavailable is 0.02.

Recall that system *unreliability* is defined somewhat differently, namely, as the probability that the system will fail to perform its intended purpose during a specified time interval. Thus unreliability is a time-dependent quantity, whereas unavailability is time-independent. In order to calculate the unreliability at any particular instant of time, one must know when last the system was ascertained to be working properly - see 121.00-8.

In spite of this distinction between the meanings of unreliability and unavailability, the two terms are often used interchangeably in reports. In fact, it is easily shown that the unavailability is nearly equal, numerically, to the average unreliability of a tested safety system, providing repair time is negligible - see 121.00-8, Appendix, section II.

III SAFETY SYSTEM TESTING

Because a Safety system is passive except during process upsets, the only way to ascertain its status during normal plant operation is by testing, ie, by simulating the signals characteristic of the various possible upsets, and observing whether or not the Safety system reacts properly. If a Safety system cannot be tested as a whole, then its components must be tested in groups, and system unavailability is then determined from the unavailabilities of these component groups.

The unavailability Q of a tested safety system is given by the formula

$$Q = \lambda \frac{T}{2} , \qquad (1)$$

where λ is the system failure rate in failure per year, and
T is the *test interval* (time between consecutive tests) in years.

The RHS of this equation represents the fraction of time the system is unavailable, assuming T/2 is the average downtime per failure. (The derivation of this formula is discussed again in Example 1, lesson 121.00-5). In fact, the average downtime per failure is not T/2 but T/2 + r, where r is the *average repair time*, but usually $r << T/2$, and therefore Equation (1) is usually sufficently accurate.

Demonstrated Unavailability

The *Demonstrated Unavailability* of a Safety system is the value of unavailability determined from equation (1), using a failure rate λ determined from operating experience by testing every T years.

Expected Unavailability

The *Expected Unavailability* of a system is the value of system unavailability predicted for the future. It is based on the Demonstrated Unreliability and adjusted as necessary for modifications to test frequency and component hardware.

Permitted Unavailability

The *Permitted Unavailability* of a Safety system is an upper limit on the system unavailability, which exists to keep the risk of nuclear accidents below a specified maximum, and which provides a standard for measuring performance.

In practice, if the system Demonstrated Unavailability is comfortably below the Permitted Unavailability, the system hardware and test interval are likely to remain unaltered, in which case the Expected Unavailability will equal the Demonstrated Unavailability (barring changes in operating conditions, of course). However, if the Demonstrated Unavailability were greater than the Permitted Unavailability, the Expected Unavailability would be reduced by either upgrading system hardware or by increasing the test frequency, or both. If the Demonstrated Unavailability

were far below the permitted value, then the test frequency might be reduced and/or cheaper components might be purchased for replacements. The incentives for reducing test frequency are as follows:

- to improve station efficiency. Testing is time-consuming, and tends to risk unplanned outages.
- to avoid excessive component wear due to the testing process, eg, diesels.
- the testing process itself contributes to system unavailability.
- the more human intervention, the greater the risk of inadvertently leaving a safety system in a degraded state.

This section on safety system testing concludes with the following list of reasons for periodic testing:

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

(2) To maintain system unavailability below a specified value which is proportional to the test interval (see Equation (1).

(3) To ascertain whether unavailability targets are being met, so that corrective action - upgrading system and/or more frequent testing - can be taken if they are not.

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

(5) To satisfy the conditions of the AECB operating license, ie, to obey the law.

In connection with (3), (4) and (5) the importance of documenting failures cannot be overstated. When components fail there are two things which must be done:

(1) repair or replace bad component

(2) document the failure.

IV SAFETY STANDARD

It is impossible to guarantee absolutely the safety of a nuclear plant, because it is inherently impossible to design equipment which cannot fail, or to recruit staff who cannot make mistakes. In fact, there is some risk of death or injury associated with all human activity. The decision to proceed with such activities as driving cars or operating nuclear plants is based on an assessment of the risks versus the benefits of such activities. If the risk outweighs the benefit, additional safety measures may be adopted to reduce the risk to an acceptable level, or the activity may be outlawed.

For rational decisions on nuclear generation, society needs quantitative (numerical) values of the risks. These should be evaluated in the context of the risks attending many widely accepted human activities. Table 1 from "A Catalog of Risks" by Cohen and Lee[1] is instructive in this regard.

Table 1

Loss of Life Expectancy Due to Various Causes

CAUSE	DAYS	CAUSE	DAYS
Being unmarried-male	3500	Drowning	41
Cigarette smoking-male	2250	Job with radiation exposure	40
Heart disease	2100	Falls	39
Being unmarried-female	1600	Accidents to pedestrians	37
Being 30% overweight	1300	Safety jobs - accidents	30
Being a coal miner	1100	Fire - burns	27
Cancer	980	Generation of energy	24
20% overweight	900	Illicit drugs (U.S. average)	18
<8th grade education	850	Poison (solid, liquid)	17
Cigarette smoking-female	800	Suffocation	13
Low socio-economic status	700	Firearms accidents	11
Stroke	520	Natural radiation (BEIR)	8
Living in unfavorable state	500	Medical X-rays	6
Army in Vietnam	400	Poisonous gases	7
Cigar smoking	330	Coffee	6
Dangerous job-accidents	300	Oral contraceptives	5
Pipe smoking	220	Accidents to pedalcycles	5
Increasing food intake 100 cal/day	210	All catastrophes combined	3.5
Motor vehicle accidents	207	Diet drinks	2
Pneumonia - influenza	141	Reactor accidents - UCS	2*
Alcohol (U.S. average)	130	Reactor accidents-Resources	.02*
Accidents in home	95	Radiation from nuc.industry	.02*
Suicide	95	PAP test	-4
Being murdered (homicide)	90	Smoke alarm in home	-10
Legal drug misuse	90	Air bags in car	-50
Average job-accidents	74	Mobile coronary care units	-125
		Safety improvements 1966-76	-110

*These items assume that all U.S. power is nuclear. UCS is Union of Concerned Scientists, the most prominent group of nuclear critics.

Note that while the estimates of risk due to reactor accidents vary from 0.02 days to 2 days, even the most pessimistic estimate (produced by an antinuclear group) is still insignificant compared to the risk of such commonly accepted activities as being single, smoking, being overweight, driving an automobile, or even working for a living.

The basic *Safety Standard* for Canadian nuclear power stations is that the risk shall be no greater than that resulting from other industries of equal economic importance, in particular, that from equivalent-sized, coal fired stations.

Historical Sketch - NPD Safety Standard

The justification for proceding with NPD ran as follows[2]:

1. Since NPD represented an important technological advance, it was considered to have the same economic worth as a 200 MWe coal fired plant.

2. The annual savings in lives due to mining and transportation of nuclear fuel rather than coal for a 200 MWe plant was estimated to be 0.82.

3. Assuming equivalent risks due to conventional accidents from equivalent-sized nuclear and coal fired stations, this annual savings of 0.82 lives could be traded off against the risk due to nuclear accidents at NPD.

4. A safety factor of 5 was introduced to allow for early life problems and a further factor of 10 since a new technology should be safer than that which it replaces. Thus the safety standard for NPD was adopted as a risk of 0.01 lives per annum due to nuclear accidents.

5. Analysis of potential accidents at NPD showed that the maximum death toll under the most severe conditions would not exceed 1000. Thus the maximum permitted *annual risk of nuclear accidents* is 10^{-5}.

DEFINITION: The *annual risk of a nuclear accident* is the probability of at least one accident during one year.

Thus the safety standard for NPD was based on an allowable risk of deaths due to nuclear accidents.

Douglas Point Safety Standard

The nuclear safety standard at DPNGS was based on the economic worth of the plant. The risk due to nuclear accidents was set at 10% of that expected over the life of a 'typical' industrial project of equal worth, namely, at 1 death over the life of the plant.

This standard was translated into the following maximum permitted annual risks of nuclear accidents at DPNGS:

- 10^{-6} for accidents causing public deaths
- 10^{-5} for accidents causing public injury only
- 10^{-4} for accidents causing death of plant staff.

Pickering Safety Standard

The AECB Reactor Siting and Design Guide was used as a standard for PNGS. The Siting Guide risk analysis is based on the principle that at all nuclear stations 3 independent divisions of equipment protect against nuclear accidents, namely, Process, Protective, and Containment equipment (see section I of this lesson).

Nuclear accidents, as defined here, cannot occur unless these three systems fail simultaneously. Growing experience indicates that the probability of this happening is so small that nuclear accidents can be considered as incredible. As a result, the Siting Guide does not define a permitted annual nuclear accident risk, but it does specify a permitted annual risk for each of the following:

- *Single Failures* - Process failures which could lead to fuel failures if they were not terminated by operation of the safety systems.
- *Dual Failures* - combined failures of both Process and Protective, or both Process and Containment systems, which could lead to a nuclear accident if they were not safely terminated by the third remaining system.

The Siting Guide imposes limits also on the radiological dose which may be given to the public as a result of either single or dual equipment failures. The limits represent a restriction on the permitted fission product escape during these incidents. Thus the Siting Guide provides standards not only for the permitted rate of equipment failure, but also for the permitted severity of equipment failures.

The Siting Guide follows the principle that restrictions should be placed not only on the dose received by any individual but also on the total number of persons that receive significant exposure. Thus, limits are shown both for the individual dose and the population dose. The population dose is obtained by multiplying individual dose by population density and integrating over the exposed population.

Table 2 summarizes the maximum permitted frequencies* of single and dual failures.

An appreciation of the significance of these population limits may be obtained from studies which indicate that 10^6 man rem can lead to 10 to 20 cases of leukaemia and 10^6 thyroid rem can lead to 20 to 30 cases of thyroid carcinoma. Hence, the chosen dose limits would lead to a very small increase over the natural incidence of leukaemia of about 60 per 10^6 people per year and of thyroid carcinoma of about 10 to 20 per 10^6 people per year.

Table 2

Permitted Annual Frequencies and Dose Limits for Single and Dual Failures

Situation	Assumed Maximum Frequency	Maximum Individual Dose Limits	Maximum Total Population Dose Limits
Normal Operation	100%	0.5 rem/yr whole body	10^4 man rem/yr
Process Equipment Failure	0.33 per yr	3 rem/yr thyroid	10^4 thyroid rem/yr
Process and Protective or Process and Containment Failure	1×10^{-3} per year	25 rem whole body 250 rem thyroid	10^6 man rem 10^6 thyroid rem

*The reader may be wondering about the connection between the "permitted annual risk" and the "permitted annual frequency". This is discussed again in Examples 4 and 5 of lesson 121.00-5, and dealt with fully in 121.00-8 Appendix, section I.

The corresponding Table for BNGS is similar except that the dual failure frequency is restricted to 3×10^{-4} per annum.

References

1. B.L. Cohen and I - Sing Lee, A Catalog of Risks, Health Physics 36, 707 (June, 1979).

2. R.J. Kelly and A.M. Lopez, Safety System Analysis Report CNO-IR-11 (Ontario Hydro internal report).

ASSIGNMENT

1. Distinguish between:

   (a) nuclear Safety systems and Process systems

   (b) Protective and Containment systems

   (c) conventional and nuclear accidents.

2. List the two most dangerous possible causes of nuclear accidents and explain why they are so dangerous.

3. Explain why it is desirable to have completely independent systems for Process, Protection and Containment.

4. Define unavailability of a Safety system and distinguish between unavailability and unreliability of a Safety system.

5. Define and distinguish amongst:

   (a) Demonstrated Unavailability

   (b) Expected Unavailability

   (c) Permitted Unavailability

6. List and explain four reasons for testing Safety systems.

7. Explain why it is impossible to guarantee the safety of a nuclear generating station, ie, to guarantee that there will never be any nuclear accidents.

8. State the accepted Safety Standard for CANDU stations.

9. Define Annual Risk of a Nuclear Accident.

L. Haacke