Module 6

RELIABILITY CONCEPTS

OBJECTIVES:

After completing this module you will be able to:

6.1 Sketch the bathtub curve showing the typical variation of component failure rate with time. Label the three distinctive regions of the curve. ⇔ *Page 3*

6.2 Relate the concept of useful life to the station preventive maintenance program, and explain why it is important to station reliability that specified preventive maintenance schedules are followed. ⇔ *Page 4*

6.3 Define the terms Reliability and Availability, and state their applicability with respect to poised and active systems. ⇔ *Page 4*

CRO 6.4 State with respect to Special Safety Systems:

a) one OP&P requirement pertinent to each: availability, testing, and on-line maintenance ⇔ *Page 5*

b) numerical unavailability targets ⇔ *Page 7*

c) Nuclear safety consequences of exceeding unavailability targets ⇔ *Page 7*

CRO 6.5 Explain two strategies used to increase the reliability of each of the following systems:

a) instrument air ⇔ *Page 8*

b) process (service) water ⇔ *Page 8*

NOTES AND REFERENCES

Page 8 ⇔ **CRO** 6.6 Describe the hierarchy of station electrical power supplies--Class IV, Class III, Class II, Class I and EPS, and state the minimum power supply requirements to:

a) operate the reactor at power,

b) remove decay heat,

c) maintain indication, control and protection

Page 10 ⇔ **CRO** 6.7 Explain why maintenance on Class III, II and I supplies, and on equipment powered by these supplies, requires Shift Supervisor approval.

CRO 6.8 Define the following reliability strategies, explain their impact on equipment reliability, and give one application in a CANDU plant:

Page 12 ⇔ a) redundancy

Page 14 ⇔ b) diversity

Page 15 ⇔ c) independence

Page 15 ⇔ d) fail safe

Page 15 ⇔ **CRO** 6.9 Define *common cause failures*, and give three examples.

Page 16 ⇔ **CRO** 6.10 Explain one possible limitation of the fail safe design strategy, and illustrate with two examples.

Page 16 ⇔ **CRO** 6.11 Explain why rejection of one channel in a 2-out-of-3 trip system improves system availability.

CRO 6.12 Explain how each of the following design strategies contributes to equipment or system independence, and give one example of the application of each concept:

Page 16 ⇔ a) physical separation

Page 17 ⇔ b) Odd/even equipment

Page 17 ⇔ c) Seismic qualification

Page 17 ⇔ d) Environmental qualification

Page 18 ⇔ e) Group I/group II systems

NOTES AND REFERENCES

f) Channelization. ⇔ *Page 18*

6.13 State three advantages of channelization in safety system design. ⇔ *Page 19*

6.14 Poised safety systems in a CANDU plant are routinely tested according to a schedule issued by Technical Support staff.

a) State the effect on availability of increasing or decreasing test frequency. ⇔ *Page 21*

b) State the effect on system availability of not following the specified schedule. ⇔ *Page 22*

c) Give four reasons for doing this testing. ⇔ *Page 23*

d) Give five reasons for limiting the testing frequency. ⇔ *Page 23*

USEFUL LIFE AND PREVENTIVE MAINTENANCE

The failure rate of most components varies with time in a familiar pattern known as the *bathtub curve* of Figure 6.1. ⇔ *Obj. 6.1*

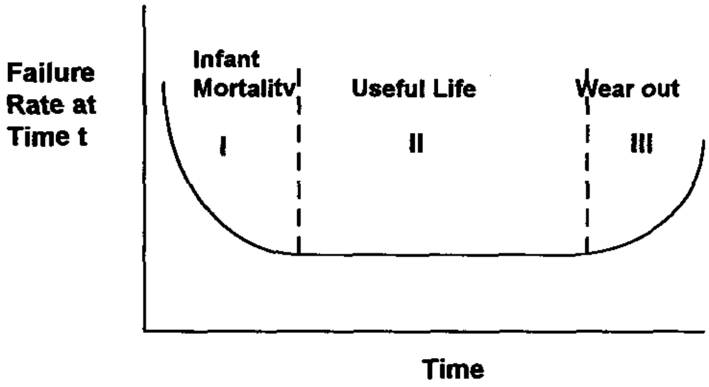


Figure 6.1: Bathtub Curve

Region I in the diagram shows a rapidly decreasing failure rate, and is known as the *Burn-In* or *Infant Mortality* period. Failures in region I are due mainly to manufacturing defects or burn-in failures. Early failures due to manufacturing defects can be avoided by burning in (test running) components on the bench prior to placing them in service.

Obj. 6.2 ⇔

Region II features a low, constant failure rate, and is known as the *useful life* period. Failures in this region are random and relatively infrequent. Region III shows an increasing failure rate, and is known as the *wear out* period. For maximum system reliability, components must be operated only during their *useful life* periods. Thus components are replaced *before* the end of their useful lives through preventive maintenance programs, even though they have not failed yet! If such preventive replacements are *not* performed, production is continually disrupted by emergency repairs, with breakdown maintenance pre-empting planned maintenance.

RELIABILITY VERSUS AVAILABILITY

Obj. 6.3 ⇔

Definition: ***Reliability*** is the probability that a component or system will perform its design function for a specified mission time, under specified operating conditions.

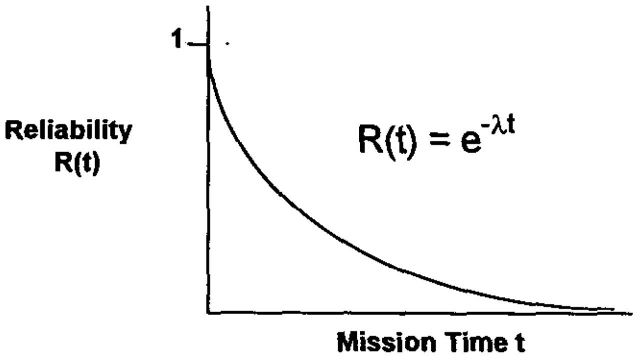


Figure 6.2: General Reliability Function *

* Use of the general reliability function is beyond the scope of this course.

For useful life operation, where the failure rate is constant with time and failures are random, reliability decays exponentially with time, analogous to a nuclear decay curve—see Figure 6.2. The concepts of mission time and Reliability are appropriate to active (continuously operating) systems.

Definition: ***Availability*** is the fraction of time that a component or system is available to perform its intended purpose. *Unavailability* is the fraction of time that a component or system is unavailable to perform its intended function. Since a component or system is either available or unavailable, therefore

Unavailability = 1 - Availability

The concept of *availability* is appropriate to *poised* systems. The unavailability of a poised system is measured by testing it periodically (see later).

Both reliability and availability are calculated (predicted) using historical failure rate data, which is obtained by documenting component failures.

OP&P REQUIREMENTS PERTAINING TO SPECIAL SAFETY SYSTEMS

⇔ *Obj. 6.4 a)*

The sole purpose of the special safety systems is to mitigate the consequences of serious process failures—they have no role whatsoever in the nuclear electric generation process. In fact, they are deliberately designed to be independent of the process systems, so that process failures cannot cause related failures in the special safety systems, thereby disabling both process and safety systems at once. The special safety systems must therefore be available whenever there is a need for their emergency control, cooling and containment functions.

The Operating Policies and Principles (OP&Ps) define minimum conditions for each of the special safety systems to be considered available--eg, that the shutdown system reactivity depth and insertion rate are as claimed in the safety report. If these minimum conditions are not met, then the reactor must be shut down and placed in a state in which the safety system is not required.

Shutdown System Availability

All CANDU units subsequent to Pickering-A were designed with two independent and diverse shutdown systems.* In order to ensure that failure to shutdown on a serious process failure is an incredible event, no credit is taken for shutdown system redundancy—ie, <u>both</u> shutdown systems must be continuously available, unless the reactor is in the GSS.

* Meanwhile, the SDSE retrofit planned for 1997 and following will increase shutdown reliability for Pickering-A units.

The shutdown systems must be available whenever equipment or procedural faults could lead to an uncontrolled power increase. Since this could happen at any power level, OP&Ps require that both shutdown systems be available before removal of the shutdown guarantee. Furthermore, if either shutdown system becomes unavailable, regardless of power level, the reactor must be placed in the GSS (unless repairs can be completed within the grace period specified in operating instructions for the relevant impairment level). A shutdown system can be made unavailable for maintenance once the reactor has been placed in a guaranteed shutdown state. Normally, only one shutdown system at a time is made unavailable, even with the reactor in the GSS.

NOTES AND REFERENCES

Emergency Coolant Injection System Availability

The Emergency Coolant Injection System (ECIS)* must be available whenever the coolant temperature is high enough that boiling could occur with the PHT coolant depressurized. Depressurization would then result in core voiding and degraded fuel cooling. Therefore, whenever the PHT temperature is at or above typically 90°C, ECIS must be available. The specific temperatures for blocking and restoring the ECIS logic are chosen so as not to fire ECIS as the PHT system is depressurized, while still providing adequate protection. When the ECIS is isolated, it must be recallable in case a loss of HTS inventory occurs. The longer the time after shutdown, the lower the decay heat rate, and the longer the permissible recall time.

* This system is called the Emergency Core Cooling System (ECCS) at some stations. For the purposes of this course, the two terms may be used

Containment System Availability

The containment system must be available whenever radioactive material could be released into the reactor building from the heat transport system or fuel handling system, as a result of a LOCA. Thus, the containment system must be available whenever the primary coolant temperature is greater than 90°C, or there is irradiated fuel in a fueling machine.

Testing

OP&Ps require that special safety systems be tested at a frequency sufficient to demonstrate compliance with the unavailability targets assumed in the safety analysis and specified in licensing documents.

On-line Maintenance

The following typically worded OP&P ensures that special safety systems remain available during on-line maintenance:

> ***The method of performing maintenance, which shall be used unless Operations Manager approval is given for an alternative method, is to put in a safe state, where such a state exists, repair, test, and return one channel to service prior to working on another channel.***

Safety system unavailability is minimized by placing a channel in its safe state (ie, by "rejecting" the channel), as soon as practicable after discovery of a fault.

Before rejecting a special safety system channel for discretionary maintenance, the channel is tested in order to confirm its availability. If the channel then fails to operate properly after the maintenance, the fault can be traced to the maintenance itself, and the unavailability is limited to the period subsequent to the last successful test.

TYPICAL UNAVAILABILITY TARGETS

The target unavailability for special safety systems is less than 10^{-3} years per year. This target is a licensing requirement for the design and operation of special safety systems.

⇔ *Obj. 6.4 b)*

Standby safety support systems do not have specific availability requirements established by the AECB, but these systems must be operated and maintained such that their unavailabilities are within values assumed in the plant safety assessment. The general principle of maximizing availability also applies to these systems.

Unavailability targets for standby safety support systems are typically ~ 10^{-2} years/year.

Consequences of Exceeding Safety System Unavailability Targets

⇔ *Obj. 6.4 c)*

When a safety system exceeds its unavailability target, nuclear safety is less than intended—ie, the risk to the public is greater than that claimed in the safety report. In such cases, prompt action must be taken to reduce the risk to acceptable limits.

The Reactor Operating Licence requires that prompt reports be made to the AECB in the following situations among others:

1. Any degradation of a special safety system which could substantially prevent it from performing as described in the Safety Report and documents listed in the licence application;

2. Information in the Safety Report or licensing support documents is discovered to be inaccurate or incomplete.

In the case of a prompt report, the AECB is normally informed by the Operations Manager the next business day. This prompt report is followed up by a written report describing the incident and remedial actions to be taken.

RELIABILITY OF AIR, WATER AND POWER

Air, water and power supplies are essential to support the process, even with the reactor shutdown. Since the water and power requirements with the reactor at power can always be reduce to the lesser decay heat sink requirements simply by shutting down the reactor, therefore the decay heat sink water and power supplies are designed to have greater reliability. Some of the reliability design features of these systems are discussed below.

Instrument Air

Obj. 6.5 a) ⇔ To enhance the reliability of the instrument air supply to control valves, the instrument air compressors are powered by class III power. Another reliability enhancement stratagem is the use of redundant air distribution headers, with roughly half the similar loads supplied from each header. A failed header can be isolated, while the functional header continues to supply its loads, thus avoiding total loss of control. On loss of instrument air compressors, instrument air receivers continue to supply vital control valves for a few minutes, providing some response time before process control is lost. Also, many key control valves operate in a fail safe mode upon loss of instrument air.

Process (Service) Water

Obj. 6.5 b) ⇔ Process water (called *service water* at some stations) provides cooling for the fuel (indirectly), and for various electrical and mechanical equipment. For enhanced reliability, enough process water pump motors are powered by class III to provide cooling requirements with the reactor shut down. A seismically qualified emergency water system, powered by the Emergency Power System, is also available at stations built after Bruce-A.

Electrical Power

Obj. 6.6 ⇔ Consistent with the *defense in depth* philosophy, equipment power supplies are classified, and their reliability requirements assessed according to the equipment's importance to nuclear safety. Five sources of electrical power are provided for reactor operation, control, monitoring and protection functions--class IV, class III, class II, class I and emergency power, as described below.

NOTES AND REFERENCES

Class IV Power

Class IV supplies loads which are necessary to maintain the full power heat removal chain. These loads include*:

- Primary heat transport pump motors
- Main boiler feed pump motors
- Main condensate extraction pump motors
- Main process (service) water pump motors
- Condenser circulating water pump motors

A loss of Class IV power results in automatic protective action to reduce reactor power to a level that can be handled by a class III heat removal chain.

Class IV power supplies the other three classes of power under normal operating conditions; it supplies Class III directly, and Classes II and I indirectly, via Class III.

Class III Power

When class IV power is lost, class III is also lost temporarily, until restored via the standby generators. On loss of class IV power, class III standby power is required to supply decay heat removal loads, including the following:

- auxiliary boiler feed pump motor
- auxiliary condensate extraction pump motor
- shutdown or maintenance cooling pump motors (as applicable)
- PHT feed (pressurizing) pump motors
- Emergency LP and HP service water pump motors
- end shield cooling pump motors
- auxiliary moderator pump motors (where applicable)

* Except at Pickering the main moderator pump motors are also supplied by class IV

Class III standby power is also required to supply the following loads, which are essential to maintain process monitoring, control and protection:

- class I and II power
- Instrument air compressors

Were class III standby power unavailable on loss of class IV power, not only would the class III decay heat sinks be disabled, but thermosyphoning would gradually become ineffective due to loss of HT pressure control. In the absence of further intervention, this would result in fuel overheating, and possibly fuel failures.

With the reactor shut down and cooled down, there is no immediate need for class III standby power as the decay heat production decays rapidly with time after shutdown, and the initial fuel temperature is low to begin with. This provides time to complete repairs before the fuel is at risk. However, class III would still have to be restored urgently as fuel cooling is still required, and class I and II batteries will run out in about 40 minutes.

Obj. 6.7 ⇔ If a load is powered by Class III, it is safe to assume that the load is important to nuclear safety. For this reason, the Shift Supervisor's approval is required to remove either a class III supply or load from service for discretionary maintenance. Operations Manager approval may also be required.

Class II and Class I Power

All instrumentation associated with monitoring, control and protection of plant systems is supplied by class II or Class I electrical power. Since continuous monitoring, control and protection are vital to safety and production, Class II or I repairs must receive high priority. Again, maintenance on class II and class I supplies and loads requires Shift Supervisor approval.

The Emergency Power Supply

All stations built after Bruce NGS-A have an Emergency Power Supply (EPS) that powers the Emergency Water System (EWS). The EPS also supplies other critical loads, including certain class III pump motors and motorized valves. The EPS caters to the effects of simultaneous loss of Class III and IV power.

NOTES AND REFERENCES

Interruptability of Class I, II and III Power Supplies

Table 6.1 summarizes the interruptability criteria of the class I, II and III power supplies and the reasons for these criteria:

Class	Interruptability Criteria	Reasons
1	DC power can never be interrupted without affecting worker, public and environmental safety.	Class I Loads are vital to equipment monitoring, control and protection, including the turbine-generator and circuit breakers. Failure of this equipment could result in massive plant damage.
2	AC power, can be interrupted for only a few power cycles without affecting the safety of station equipment or personnel.	Class 2 loads are considered uninterruptible and are critical for monitoring, controlling and protecting the reactor.
3	AC power, can be interrupted with the unit on load for up to about 3 minutes without affecting the safety of station equipment or personnel	Loads are essential to maintain fuel cooling with the reactor in a low power state when class IV power is not available. Also, class III supplies class I and II power; therefore, a sustained loss of class III for more than about 40 minutes (back-up battery life) results in a loss of class I and II as well.

Table 6.1: Interruptability Criteria for Various Classes of Electrical Power

NOTES AND REFERENCES

DESIGN STRATEGIES FOR IMPROVING RELIABILITY

Obj. 6.8 a) ⇔

Redundancy

Definition: *Redundancy* is the provision of components or capacity in excess of 100% of system requirements, such that failures of excess components or capacity do not disable the system function.

Example: Two 100 percent capacity pumps placed in parallel are *redundant*, since either can deliver the design flow.

Figure 6.3 shows two pump configurations, one with a single pump, and the second with two 100% duty pumps in parallel. Assume that all pumps are identical and the reliability of each pump is 0.95. In the case of the single pump system, the system reliability is the same as the reliability of the pump, ie, 0.95.

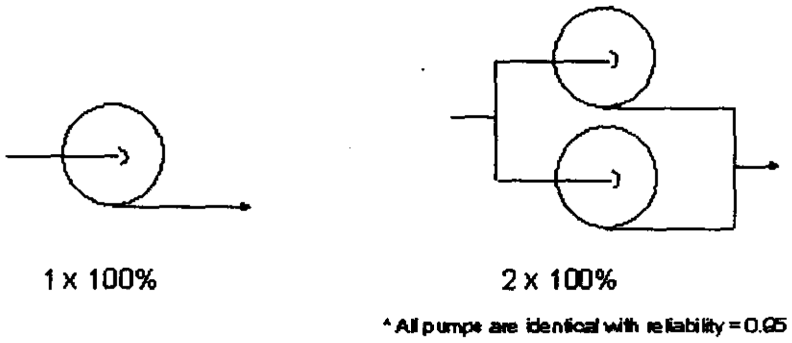


Figure 6.3: Pump configurations

In the case of the two pump system, if one pump fails, the second pump continues to provide the design flow. The system fails only when both pumps fail simultaneously. The probability of both pumps failing at the same time* is equal to 0.05 x 0.05 = 0.0025. Therefore, the system reliability is 1 - 0.0025 = 0.9975, significantly higher than the reliability of the single pump configuration.

* The probability of two or more independent events occurring at once is the product of the probabilities of the individual events.

NOTES AND REFERENCES

Redundancy may be achieved by adding components in either a series or parallel configuration, depending upon the system function. For example, two identical valves in *series* are redundant if their function is to close and stop flow under certain conditions. Figure 6.4 shows single and dual valve configurations.

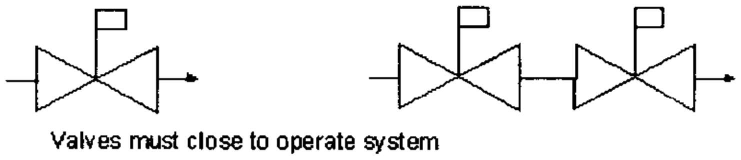
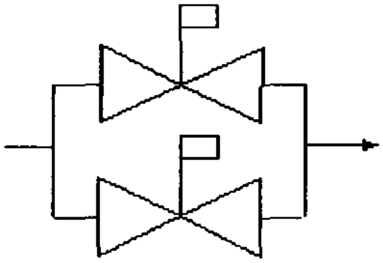


Figure 6.4: Valve configurations

In the single valve configuration, the system reliability is equal to the reliability of the valve. In the two valve configuration, only one of the two valves must close to stop flow, not necessarily both. In this case, the system fails only if both valves fail to close. Since the probability of both valves failing at the same time is lower than the probability of one valve failing, the reliability of the dual valve system is greater than that of the single valve system.

If the second valve is placed in *parallel* with the first valve, as shown in Figure 6.5, then *both* valves must close to stop flow. If either or both valve(s) fail, the system fails. Since the probability of either one of two valves failing is greater than the probability of one valve failing, the system reliability *decreases* in this case.

These examples show the difference one redundant component can make on the reliability of a system.



For this arrangement, both valves must close to be successful.
Either valve remaining open will cause system failure.

Figure 6.5: Two valves in parallel

Obj. 6.8 b) ⇔

Diversity

Definition: *Diversity* of design, manufacture, operation and maintenance of redundant components or systems is a strategy for reducing unavailability due to *common cause effects*, such as design or manufacturing flaws, and operational or maintenance errors.

For example, SDS1 achieves reactor shutdown by dropping neutron absorbing rods under gravity, while SDS2 injects a neutron absorbing liquid under pressure. The diversity of SDS1 and SDS2 designs decreases the risk of losing both shutdown systems as once due to some unforeseen failure mode. For example, if in an accident sequence some unforeseen mechanism prevented the shutoff rods from falling into the core, it is unlikely that the same mechanism could also prevent the liquid poison from being injected.

Other examples of diversity in safety system design include the following:

- Diverse trip parameter instrumentation for each shutdown system
- Diverse actuation power supplies--electrical and pneumatic
- Two diverse trip parameters on each SDS for each credible accident (see R-10 requirements, Module 7)
- Diverse manufacturers of ion chambers

Diversity in system design can be enhanced by such measures as:

- Using different Designers for redundant systems

- Purchasing components for redundant systems from different manufacturers
- Using different maintenance crews to support the operation of redundant systems.

Independence

⇔ *Obj. 6.8 c)*

Redundancy provides protection from the consequences of random isolated failures of individual system components. However, redundancy by itself does not protect against multiple component failures caused by common cause effects.

Definition: *Common cause failures* (also called *common mode failures*) are failures in more than one piece of equipment or structure due to the same cause. Examples of *common causes* are aircraft crashes, earthquakes, tornadoes, fires, floods, sabotage, high temperature environment, high radiation environment, steam environment, common design flaws, and common fabrication, installation, operation, or maintenance errors.

⇔ *Obj. 6.9*

Definition: Systems are said to be ***independent*** if a failure in one cannot cause related failures in the others. ***Independence*** is achieved by having no shared components or common services (functional separation), and by physical separation.

It is important to realize when a single fault or event can disable otherwise independent components or systems, and to minimize the risk of such failures. For example, the standby generator fuel system is common to more than one standby generator (SG). Therefore, contaminants entering the SG fuel supply can cause failures of more than one SG. Lack of independence (shared fuel supply) makes the SGs vulnerable to *common cause failures*. The risk can be minimized by using fuel handling cleanliness procedures, and the use of fuel filters.

As another example of a *common cause failure*, suppose that an alarm unit on Channel A is improperly calibrated during a call-up, so that the unit functions at the wrong parameter value. If the same Maintainer proceeded to make the same error on Channel B, then both channels would be impaired. To avoid such *common cause failures*, wherever practical, tests and call-ups are staggered so that different people from different crews work on different channels.

Fail Safe

Definition: A component or system *fails safe* if it performs its design function immediately and automatically as a result of the failure--ie, the failure does not contribute to unavailability.

⇔ *Obj. 6.8 d)*

For example the shutoff rods fail safe on loss of electrical power to the electromagnetic clutches holding the rods above the core. When power to the clutches is lost, they de-energize and the rods fall into the core, shutting down the reactor. Another example of fail safe design is valves that are designed to fail in the safe position (either open or closed, depending upon the process function) upon losing control power.

Note that a component designed to fail safe, sometimes fails unsafe—eg, shutoff rods failing to drop fully due to cable snarling. Unsafe failures of fail safe components do, of course, contribute to component unavailability.

Obj. 6.10 ⇔ In some cases, there is no fail safe state--eg, if the PHTS fully instrumented liquid relief valves fail open, coolant pressure drops, and fuel cooling is impaired due to core voiding. But if they fail closed, HT pressure relief capability is lost. Another example is a check valve which disrupts needed flow if it fails closed, but permits unacceptable bypass flow if it fails open. A circuit breaker is yet another component which may not have a fail safe state. If a circuit breaker fails open, power to a safety related component may be disrupted; but if it fails closed, an electrical fault may propagate, resulting in a more widespread power outage affecting multiple components. Where a fail safe state does not exist, components are often designed to fail "as is".

Special safety system channels are designed to fail safe whenever possible--eg, component failure, sub-system malfunction, and power loss normally cause a channel to go to the safe (trip) state.

Obj. 6.11 ⇔ In practice, it is not feasible to design a trip channel which is fail safe in all eventualities. It is therefore an OP&P requirement that, upon detection of an inoperable or out-of-specification trip function, the channel or parameter concerned is placed in the safe state (ie, "rejected"). This results in an *increase* in the predicted availability of the safety system, since now only one channel of two must trip rather than two of three. The probability of one channel of two tripping on a genuine fault is greater than the probability of two channels of three tripping.

Physical and Functional Separation

Obj. 6.12 a) ⇔ Vulnerability of redundant systems to many *common cause failures* is eliminated by physical and functional separation. For example, physical separation of special safety system channels protects against multiple channel failures due to a localized fire or impact by a falling object. *Functional separation* (no shared components or common services) protects against multiple channel failures due to single component failure or loss of a power supply.

NOTES AND REFERENCES

Odd/Even Equipment

⇔ *Obj. 6.12 b)*

One possible common cause failure mode is the loss of an electrical supply. To reduce the impact of an electrical power failure, supplies are designated as *odd* or *even*. Typically half the equipment performing a given function receives power from an *odd* supply, and half from an *even* one.

For example, 2 x 100% capacity pumps would normally be fed one from an *odd* supply and one from an *even* supply. Thus design flow is still possible despite a failure of either the *odd* or *even* supply. Equipment is commonly referenced by designated power supply—eg, as the "*odd* pump" or the "*even* pump".

Seismic Qualification

⇔ *Obj. 6.12 c)*

An earthquake could induce site-wide *common cause failures*. Thus mere separation of redundant systems does not protect against an earthquake, as it does against some other common cause events, such as turbine missiles or localized fire. The approach used at plants built after Bruce A is to seismically qualify sufficient safety-related systems that a LOCA will not occur due to seismically induced stresses in the PHT system, and *control, cool and contain* capabilities survive a design basis earthquake:

Environmental Qualification (EQ)

⇔ *Obj. 6.12 d)*

Some design basis accidents impose a harsh operating environment on affected equipment - eg, a LOCA, feedwater break, or main steam line break could subject equipment to such conditions as high temperature, high radiation fields, steam jets, and flooding. Safety related equipment required to mitigate the impact of such accidents must be environmentally qualified to survive the harsh environment imposed by the accident itself. Otherwise, the harsh environment could induce common cause failures which would escalate the impact of the initiating incident.

Maintenance performed on environmentally qualified equipment must not degrade this qualification, which typically depends on the integrity of seals or other protective physical barriers. Sometimes the environmental qualification is obtained by locating the equipment in a protected room. When doors, typically labelled *STEAM PROOF DOOR, KEEP CLOSED,* are left open, it invalidates the EQ assumptions in the Safety Analysis. Note that a failed environmental qualification would not normally be discovered during routine safety system testing. Rather, the integrity of equipment EQ depends on staff following good operating and maintenance practices.

NOTES AND REFERENCES

Obj. 6.12 e) ⇔

Group I/Group II Systems

To protect against such common cause incidents as plane crash, earthquake, fire, and flood, systems are separated at some stations into two groups--*Group I* and *Group II*.

Each group provides the capability to do the following:

1. Shut down the reactor and maintain the shutdown status
2. Remove decay heat and thus prevent fuel damage
3. Prevent radioactive releases from containment
4. Monitor and control post-accident plant conditions.

This separation means that even wide spread failures in one group do not cause failures in the other group. At Pickering-B, Bruce-B, Point Lepreau, Gentilly 2 and Darlington, the *Group II* systems are seismically qualified to ensure their operation in the event of an earthquake, and have their own seismically qualified water and power supplies. Furthermore, the *Group II* systems can be operated from a remote, seismically qualified location (Unit Emergency Control Center or Secondary Control Area), in case the Main Control Room becomes incapacitated or uninhabitable.

Obj. 6.12 f) ⇔

Channelization

Definition: *Channelization* is the provision of more than one independent means of transmitting energy or signals.

Example: Redundant and identical sets of instrument loops are provided to actuate setback, stepback and special safety systems.

In 2-out-of-3 channel majority voting logic, system actuation occurs when any 2 of the 3 channels are in the trip condition. 3-out-of-4 logic is sometimes used where there is a major economic penalty due to system operation, because it reduces the risk of spurious system operation.* 1-out-of-2 logic is used where the system can be actuated without economic penalty. Note that when one channel is rejected for test or maintenance in 1-out-of-2 logic, the system actuates. Also, 2-out-of-3 logic becomes 1-out-of-2, and 3-out-of-4 logic becomes 2-out-of-3, when one channel is rejected for testing or maintenance.

* As in the case of the ECIS at PND

Channelization provides the following advantages in safety system design:

⇔ *Obj. 6.13*

1. Channel redundancy increases system availability. 1-out-of-2, 2-out-of-3 and 3-out-of-4 systems all have greater availability than a single channel system.
2. 2-out-of-3 and 3-out-of-4 initiation logic permits rejecting one channel at a time for test or repair while the system remains poised. System availability actually increases with one channel rejected, but vulnerability to spurious system operation also increases.
3. A spurious single channel trip in a 2-out-of-3 or 3-out-of-4 system will not actuate the safety system.

In summary, channelization provides for increased system availability, on-line testing and maintenance, and reduced vulnerability to spurious system operation.

SUMMARY OF KEY CONCEPTS

- The variation of failure rate with time for most components follows a predictable pattern, known as the *bathtub curve*.
- Preventive maintenance schedules should be followed to keep reliability high, and to avoid production losses due to equipment breakdowns.
- Both shutdown systems must be poised unless the reactor is in the GSS.
- Both ECI and containment systems must be available whenever the PHT temperature is above 90°C.
- OP&Ps require testing of special safety systems at a frequency sufficient to demonstrate that they meet the unavailability target mandated in licensing documents and assumed in the Safety Report.
- The unavailability target for special safety systems is less than 10^{-3}. Standby safety support systems' unavailability targets are typically ~ 10^{-2}.
- When safety system unavailability targets are exceeded, prompt corrective action is required to reduce public nuclear safety risk to the range claimed in the safety report. Also, the reactor operating licence requires prompt notification of the AECB.

- *Redundant* components must be returned to service as soon as possible after maintenance, to restore reliability to design values.

- *Diversity* of design, manufacture, operation and maintenance reduces vulnerability of redundant systems and components to *common cause failures.*

- Redundant equipment is often powered by separate *odd* and *even* electrical supplies. Thus, on loss of *odd* power supply, the *even*-supplied equipment remains available, and conversely.

- In case *group I* equipment is lost due to a common cause event, such as an earthquake, vital *control, cool and contain* functions can be maintained using *group II*, seismically qualified equipment. Group II equipment can be operated from a seismically qualified, auxiliary control center, physically separated from the main control room.

- *Channelization* is the provision of more than one independent means of transmitting energy or signals. Channels are independent, since they share no components or common services, and are physically separated. Channelization of special safety systems is used to:

  — increase system availability

  — permit on-line testing or maintenance, one channel at a time, with the channel rejected to the safe (trip) state

  — prevent spurious system trips.

- A component or system *fails safe* if it performs its design function immediately and automatically as a result of the failure. Component failures to the safe state do not contribute to unavailability. Where there is no well-defined safe state, the *fail safe* design strategy cannot be used.

ROUTINE TESTING OF POISED SYSTEMS

A NPP's testing and surveillance program includes tests designed to demonstrate that the availability and capability of poised equipment meet the claims made in licensing documentation. Such tests are undertaken to a defined schedule, and detected failures are corrected promptly. Waiting until a poised system is called to mitigate a process upset to detect and correct failures, is clearly an unacceptable alternative to detecting and correcting failures by routine testing.

NOTES AND REFERENCES

Test Frequencies and Unavailability

⇔ *Obj. 6.14 a)*

Suppose a component failure is discovered during a test. The component could have failed immediately after the last test, or immediately prior to the present test, or at any time in between. Assuming that failures are random in time, and that the failure rate is constant, then on average, a failed component has been unavailable for one-half of the time since the last test, ie, for one-half the test interval. Thus the equation for calculating the predicted unavailability of tested components is:

$$Q = \lambda\left(\frac{T}{2} + r\right) \qquad (1)$$

where T = the test interval (time between tests) in years;

r = the repair time in years;

λ = the failure rate in failures per component year;

Q = the unavailability (the fraction of time that a component is not able to perform its intended purpose).

If the repair time is negligible compared to the test interval, ie, if $r \ll T$, then the equation simplifies to:

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

Example: A component which is tested weekly has failed five times during the last seven years of operation. What is the predicted component unavailability?

Solution: Substituting a test interval **T** of 1/52 years, and a failure rate **λ** of 5/7 failures per year into equation (2), and assuming negligible repair time, the unavailability is:

$$Q = \frac{5\ \text{failures}}{7\ \text{years}} \times \frac{1/52\ \text{years}}{2}$$

$$= 6.9 \times 10^{-3}\ \text{years/year}$$

In equation (2), system unavailability is proportional to the test interval for failures random in time. That is, the predicted system unavailability can be decreased by reducing the test interval. For example, if the actual failure rate of a safety system component exceeded the failure rate assumed by the system Designer, the system target unavailability might still be met by increasing the test frequency. Conversely, *in*creasing the test interval *in*creases the predicted system unavailability, potentially beyond licence limits.

How can system unavailability be decreased merely by increasing test frequency? Intuitively, one might think that some physical change to the system should be required to decrease its unavailability. In fact, a physical change *is* taking place—the more frequently a system is tested, the sooner system failures are detected and corrected. Hence the smaller the fraction of time the system spends in the failed state. In the extreme case, keeping the system in operation continuously, as in the case of an active system, is analogous to testing infinitely often, and failures are instantaneously detectable.

Again, all of the above assumes that failures are random in time, and that the failure rate is constant. But in the event that failures are cycle-based--eg, the failures are induced by the testing process itself, then Q becomes a constant independent of the test interval. For cycle-based failures, more frequent testing does not decrease the value of Q.

Obj. 6.14 b) ⇔

Compliance With Test Schedule

Testing most effectively reduces system unavailability when the tests are done at uniform intervals. To understand why, consider case A in which a system is tested on the last day of each month throughout the calendar year, and case B, where the twelve tests are all deferred to December 31st. Suppose that a failure occurs in July. In case A, the failure is detected and corrected on July 31st, and the unavailability reckoned at one-half month. In case B, the failure is detected and corrected on December 31st, and the unavailability reckoned at 6 months, ie, 12 times longer than for case A. This example shows the importance of conducting tests promptly as scheduled.

Compliance with the start-up test schedule is especially important. Many routine tests are not scheduled during outages, because they cannot be done under shutdown conditions such as negligible neutron flux, or depressurized HT coolant. There is no problem with this as long as the system is not required to be available. However, undetected failures can still occur during the outage, and the probability of there being failed components in a system could be many times higher than normal. For example, in the case of a component normally tested once per week, after a two month outage, the probability of its being in a failed state could be as much as about eight times the normal maximum. Hence the importance of doing start-up tests as soon as unit conditions permit.

Occasionally, scheduled tests are deferred legitimately--for example, when operating in quiet mode to reduce the probability of a plant upset. For instance, SDS testing might be postponed at the System Control Center's request, when available generation barely meets grid demand. However, the tests would be done with priority once the grid supply shortage were resolved, so as to avoid exceeding SDS unavailability limits.

In the case of tests deferred beyond the window specified in the published test schedule, calculations are required to determine the effect on system availability. In the extreme case, deferred or missed tests could result in violating safety system unavailability targets.

Reasons to Test Poised Safety Related Systems

⇔ *Obj. 6.14 c)*

1. To discover failed components so that they can be repaired/replaced, and thus to limit system unavailability.
2. To obtain failure rate data required to optimize the preventive maintenance program.
3. To demonstrate that the special safety systems meet licensing unavailability targets. In the event that these targets are threatened, corrective action must be taken, such as upgrading the system and/or more frequent testing.
4. To obtain site specific failure rate data for accurate reliability predictions, and for use by Designers in modifying existing systems or designing new ones.

Reasons To Limit Test Frequency

⇔ *Obj. 6.14 d)*

1. Excessive testing can cause unnecessary *wear out* failures (components reach wear out region of the *bathtub curve* sooner).
2. If a component cannot be put into its safe state during the test, then the testing process itself contributes to the component's unavailability.
3. Each test carries a small but finite probability of leaving the tested system in a compromised state due to human error in executing the test procedure.
4. Since each test carries a small but finite probability of causing a unit outage due to either human error or random equipment failure, excessive testing therefore results in lost production. (Recall that multi-channel majority voting logic is more vulnerable to spurious actuation with one channel rejected.)

5. Testing is a manpower intensive activity. Therefore, unnecessary tests divert operating staff from other surveillance activities important to nuclear safety.

Changes To Test Frequency

The impact of proposed safety system design and operational changes on test frequency and system availability must be assessed prior to implementation. A Nuclear Generating Station has a regulatory commitment to ensure that system unavailability targets will be met despite changes to system design, operation, test procedures, or test frequency. While authorized staff do not determine the test frequencies, as the final line of defense in implementing changes, they should be aware of the basis on which test frequencies are determined by technical support staff.

As noted earlier, system test frequencies may need to be increased to meet unavailability targets. On the other hand, where unavailability targets are met with a wide margin to spare, the possibility of reducing the test frequency will be considered.

An example of a reactive change to testing frequency occurred when, following a maintenance outage, monthly tests revealed unexpected problems with sticking trip plungers on the turbine governor trip system. The testing frequency was initially increased to once per shift, and then as the sticking problem diminished, the test interval was increased to daily, then to twice weekly, then to weekly, and ultimately to two weeks.

SUMMARY OF THE KEY CONCEPTS

- Safety system testing is done to limit unavailability and to demonstrate that availability and capability are as claimed in licensing documents.

- Test frequencies are chosen so that the length of time a failure can exist is acceptably small. System unavailability is proportional to the test interval, providing failures are random in time, and the failure rate is constant. Predicted system unavailability can be decreased by reducing the test interval.

- Test frequencies may be increased to meet the target unavailability. Tests deferred past the scheduled window of opportunity are treated as missed, and the impact on system availability must be calculated.

- Four reasons to test safety systems, and five reasons to limit the test frequency were given.

NOTES AND REFERENCES

- When an inoperable or out-of-specification trip function is detected, the channel concerned is placed in the trip condition. It is now impossible for this channel to fail, and only one of the two remaining channels need work to trip the system; therefore system availability increases.

- *Common cause failures* are failures of more than one piece of equipment or structure resulting from the same cause.

- *Seismic qualifications* ensure that sufficient process and safety systems will operate to *control, cool, and contain* during and following a design basis earthquake.

- *Environmental qualification* ensures safety related equipment is available to function in the harsh operating environment created by accidents such as LOCAs and main steam line breaks where high temperatures, high radiation fields, and steam wetting can cause related equipment failures.

ASSIGNMENT

1. Carefully prepare detailed answers to the Module 6 learning objectives.

2. Distinguish between the terms ***reliability*** and ***availability***. Explain the relevance of these terms to active versus poised systems, and to nuclear safety.

3. Describe three major advantages of using 2-out-of-3 channel trip logic in a Shutdown System. Illustrate the validity of your answer numerically, assuming a channel unavailability of 0.01. Include an explanation of why system unavailability decreases when one channel is open.

4. Explain the advantage of 3-out-of-4 rather than 2-out-of-3 majority voting logic to trigger a poised safety system (eg, ECIS), whose action might result in severe economic penalty. Illustrate your answer with numerical calculations.

5. At CANDU plants, class III standby power is required to be available at all times during the operation of the reactor, and if it becomes unavailable, the reactor must be shut down and cooled down within a specified time period.

   Explain why it is considered necessary to shut down and cool down the reactor if the class III standby power supplies are not available. Your answer should include, but not be limited to, the following:

   a) purpose of the class III standby system, including *five* examples of important loads that it supplies

   b) the likely consequences of class III standby power not being available when needed

   c) an explanation of why having the reactor in a shutdown and cooled down state has significantly reduced the concern for the availability of class III standby power.

6. Systems and components are expected to have a defined (low) failure rate. What is the Nuclear safety significance of frequent failure of a component before the expected wear-out period, and how can such failures be compensated?

7. What should the CRO do if, while one SDS channel is rejected for testing, a second channel is discovered to be impaired?

8. Under what circumstances should safety system testing be deferred?