NOTES AND REFERENCES

Module 3

DEFENCE IN DEPTH

OBJECTIVES

After completing this module you will be able to:

CRO 3.1 Define the *Defence in Depth* operating philosophy, and state the three basic assumptions inherent in this philosophy. ⇔ *Page 3*

CRO 3.2 The *Defence in Depth* model of nuclear safety features many overlapping barriers protecting workers, the public and the environment from large releases of fission products. Explain how each of the following physical or administrative barriers impacts on nuclear safety, and give three elements of the application of this barrier in a NPP:

NOTES AND REFERENCES

Page 13 ⇔ **CRO** 3.3 Give and explain the three aspects of a *Defence in Depth* approach to managing reactor accidents.

Page 14 ⇔ **CRO** 3.4 Explain how *Defence in Depth* is maintained when a safety related system is impaired or removed from service for maintenance.

Page 14 ⇔ **CRO** 3.5 Explain how the *Defence in Depth* philosophy applies to the diagnosis of *abnormal incidents.*

Page 15 ⇔ 3.6 Explain how an SS ensures *Defence in Depth* is maintained when an automated control system is placed on manual control.

Page 15 ⇔ **CRO** 3.7 Describe the five physical barriers between radioactive fission products and the public.

Page 16 ⇔ **CRO** 3.8 Describe the effect of large scale fuel failures on the physical barriers to environmental releases, and the impact on the protection of the public and environment.

Page 17 ⇔ **CRO** 3.9 Distinguish between, and give two examples of each:

a) Process Systems

b) Safety Support Systems

c) Special Safety Systems

d) Standby Safety Support Systems

Page 18 ⇔ **CRO** 3.10 Distinguish between, and give two examples of each:

a) Active Systems

b) Poised Systems

Page 19 ⇔ **CRO** 3.11 Define *margin of safety* and *margin to trip* and give two examples of each. Explain the important relationship that must exist between a *margin of safety* and a *margin to trip* in order for adequate trip coverage to exist.

NOTES AND REFERENCES

DEFENCE IN DEPTH

Defence in Depth is an important and fundamental principle in the safe operation of nuclear generating stations. It underlies all safety aspects of nuclear power.

Definition: *Defence in Depth* is the principle that multiple methods of high quality assurance are required in NPP design, construction, operation and maintenance.

⇔ *Obj. 3.1*

Nuclear safety provisions can be thought of as barriers to radioactive releases to the environment. These barriers may be engineered (ie, hardware or software-based) administrative, or people-based in nature. The *Defence in Depth* philosophy calls for multiple overlapping barriers (multiple methods of assurance), such that an environmental release can occur only if several barriers fail at once.

The defense-in-depth philosophy asserts that each method of assurance must be of high quality, but nevertheless is assumed to be imperfect. The classical approach to defense-in-depth involves excellence in the activities of design, construction, operation and maintenance backed up by safety equipment, procedures and training, multiple physical barriers, and multiple levels of defense of both safety and quality.

The following realistic assumptions are inherent in the *Defence in Depth* philosophy:

⇔ *Obj. 3.1*

1. NPP operating personnel will occasionally make mistakes.

2. NPP equipment will occasionally fail.

3. NPP design will have occasional imperfections.

The *Defence in Depth* approach to nuclear safety compensates for occasional personnel errors, equipment failures and design flaws, by ensuring that redundant barriers exist to prevent accidents when these things occur. Once these barriers have been put in place, it is important to keep them in place. Therefore, all *changes* to plant equipment, procedures and staffing must be scrutinized to ensure that they don't inadvertently weaken *Defence in Depth* barriers to accidents. One module of this course is devoted exclusively to the subject of *change control*.

NOTES AND REFERENCES

Defence In Depth Model Of Nuclear Safety

Described below and illustrated in Figure 3.1 is a *Defence in Depth* model consisting of 12 layers of defence, or barriers, against nuclear accidents. Most of these barriers are addressed in greater detail in other modules of this course. These barriers are not independent of one another--a failure of one can sometimes affect the integrity of others. This model provides a convenient method of conceptualizing the many physical and administrative barriers to protect workers, the public and the environment from radiological hazards associated with NPP operation.

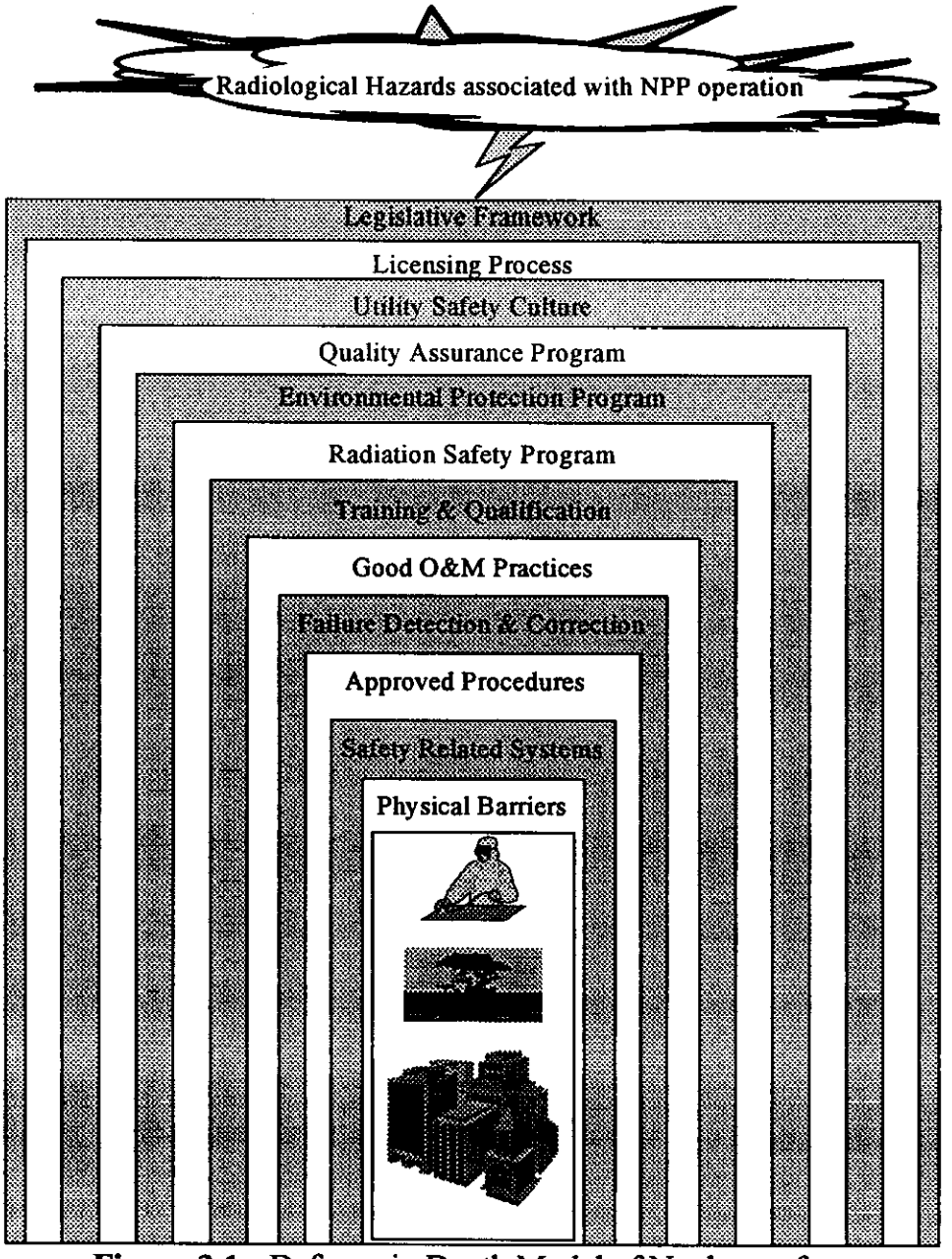

Figure 3.1: Defence in Depth Model of Nuclear safety

NOTES AND REFERENCES

Obj. 3.2 a) ⇔

1. **Legislative Framework.** The following legislative Acts provide the public policy basis for nuclear safety. These Acts oblige Canadian nuclear Utilities to operate in such a way as to limit public and environmental risk, and they establish agencies to regulate various aspects of NPP operation.

   a) Atomic Energy Control Act

   b) Nuclear Liability Act

   c) Transportation of Dangerous Goods Act

   d) Environmental Protection Act

   e) Provincial Acts

Obj. 3.2 b) ⇔

2. **Licensing Process.** The following elements of the licensing process ensure a high standard of NPP design, construction, operation, maintenance and staffing, and hence a high standard of nuclear safety:

   a) Siting Guide (Consultative Document C6 for DNGD)

   b) Safety Analysis and Safety Report

   c) Operating Policies & Procedures

   d) Power Reactor Operating Licence

   e) Quarterly Technical Report

   f) Ongoing performance auditing by Regulator

   g) AECB actions on Utility to remedy deficiencies

   h) Authorization of key positions

3. **Utility Safety Culture.** The following elements of a well-managed nuclear safety program, all of which have an obvious, positive impact on nuclear safety, demonstrate a Utility's commitment to fostering a good safety culture:

⇔ *Obj. 3.2 c)*

a) clear policy commitment--eg, that safety takes precedence over production

b) adequate funding of the nuclear safety program

c) dedicated organizational unit(s) (eg, Division, Department) to manage nuclear safety

d) well-defined nuclear safety roles and responsibilities

e) practising self-regulation

f) nuclear safety performance monitoring and reporting versus established measures

g) Nuclear Review Committee to oversee Corporate nuclear safety

h) Regulatory relations

i) motivation by Management leadership and example

j) conservative decision making

k) employee commitment--eg, to personnel error reduction work practices

NOTES AND REFERENCES

Obj. 3.2 d) ⇔

4. **Quality Assurance Program.** The quality of plant components and systems, management functions and work practices is assured by the following elements of a Utility's QA program:

   a) quality principles

   b) legislation, codes and CSA standards for design, procurement, construction, commissioning and operation of NPP equipment and systems

   c) life cycle QA program for plant

   d) quality audits and corrective action follow-up

Obj. 3.2 e) ⇔

5. **Environmental Protection Program.** Compliance with public dose limits is demonstrated, and environmental impact of NPP operation is minimized by the following program elements:

   a) Derived emission limits on radioactive contaminants in liquid and airborne effluents

   b) Environmental monitoring sites

   c) Water, vegetation, precipitation, fish and milk sampling program

   d) Active Liquid Waste Management System and authorized pump-outs

   e) Airborne effluent sampling via Stack Monitors

   f) Liquid effluent sampling (Service Water and Condenser Circulating Water)

   g) MISA program

   h) Spills reporting

   i) Radioactive waste management and volume reduction program

   j) Intermediate term storage of irradiated fuel--IFB, dry storage modules

   k) Long-term radioactive waste disposal project

NOTES AND REFERENCES

6 **Radiation Safety Program.** The focus of this program is to minimize the impact of radiological hazards on NPP workers. The program includes the following elements:

⇔ *Obj. 3.2 f)*

a) Radiation Protection Policies and Procedures, Regulations, and station Procedures

b) Radiation Protection Training & qualification program

c) Radiation instruments

d) Health Physics program

e) Dose reporting, planning and control

f) ALARA program (dose targets, performance reporting, dose equalization,...)

g) Root cause investigation and reporting of incidents, and corrective action follow-up

h) High hazard procedures and radiological work planning

i) Contamination control--plant zoning

j) Radiological surveys and reporting via radiological log and signs

k) Access control to high radiation areas

l) Whole body counting

m) Radiation protective equipment

7. **Training and Qualification.** Only highly trained, competent staff can perform the following functions and tasks critical to nuclear safety:

⇔ *Obj. 3.2 g)*

a) recognize when a layer of defence is threatened by proposed actions, or changes to equipment, procedures or staffing,

b) monitor, operate and maintain safety related systems (eg, calibrate instrument loops, perform safety system tests, perform welds on nuclear class 1 systems,...),

NOTES AND REFERENCES

c) identify incipient equipment failures, so that corrective action can be taken before catastrophic failures occur, and

d) properly execute emergency response procedures to mitigate and accommodate accident consequences.

The following are elements of the NPP staff training & qualification program:

a) work group training & qualification programs--Operators, Mechanical/Control/Civil Maintainers, Chemical Technicians, Technical Support staff,

b) initial training, progression training, continuing training

c) classroom, simulator, laboratory, shop, and on-the-job training, as required

d) conventional and radiation safety training

e) authorization training for key positions

f) emergency response training

g) special duty qualification--eg, crane operator, Media Briefer in Emergency Operations Center, confined space gas Tester, magnetic particle QC inspector, ...

Obj. 3.2 h) ⇔

8. **Good Operating and Maintenance Practices.** The integrity of the analyzed state is preserved, the plant material condition maintained in good repair, and the risk of unnecessary upset is minimized through such practices as the following:

a) the exercise of *due diligence*

b) procedural compliance

c) good housekeeping

d) configuration management and change control

e) pre- and post-maintenance testing

f) foreign material exclusion

g) personnel error reduction programs--self-checking, independent verification

NOTES AND REFERENCES

h) Supervision (pre-job briefing, coaching, job surveillance, job quality review)

i) Guaranteed Shutdown State

j) Work Authorization and work protection process

9. **Detection and Correction of Failures.** The integrity of the analyzed state and of the various *Defence in Depth* barriers is preserved by vigilantly seeking out failures, and taking corrective action. Strategies for doing this include the following:

⇔ *Obj. 3.2 i)*

a) surveillance and inspection of plant components and systems

b) Deficiency Report process and Daily Work Plan

c) root cause investigations of incidents and corrective action follow-up

d) application of lessons learned from industry *Operating Experience*

e) routine testing and repair of faults discovered in poised safety systems

f) audits (internal, PEER, QA, AECB, IAEA, WANO ...) and corrective action follow-up

g) corrective action initiated when safety performance does not meet standards

10 **Approved Procedures.** The use of approved procedures during both routine and upset conditions ensures adequate review for legislative, technical and operational constraints. The review and approval process ensures that system interactions, and impact on integrity of physical barriers to fission product release, are considered. In the case of abnormal incident procedures, the review and approval process ensures that the system or unit is placed in a safe state. Approval may be in writing by the appropriate level of management, or verbal from the SS or Station Manager. Examples of approved procedures include the following:

⇔ *Obj. 3.2 j)*

a) Operating Manuals

b) Radiation Protection Procedures

NOTES AND REFERENCES

c) Emergency Response Procedures (abnormal incidents, radiation emergency, fire and rescue, contaminated casualty treatment, breach of security, spill response, and transportation accident involving radioactive shipment)

d) Mechanical, Control and Civil Maintenance Procedures

e) Chemical Laboratory Procedures

Obj. 3.2 k) ⇔

11. **Reliable Safety Related Systems.** Each time a serious process failure occurs, the safety systems are challenged to mitigate the consequences. Each time they are called upon, there is a small but finite probability that they will fail, resulting in a release. The more reliable the process systems, the less frequently the safety systems are challenged, and the more reliable the safety systems, the less likely they are to fail when called upon. *Defence in depth* elements to maintain reliable safety related systems include the following:

a) design codes and standards--eg, CSA standards, ASME code

b) preventive and predictive maintenance

c) reliability design strategies--redundancy, independence, diversity, fail-safe

d) limit on serious process failure frequency, demonstrated via operating experience

e) limit on special safety system unavailability, demonstrated via periodic testing

f) probabilistic risk assessment (PND-A, DNGD)

g) inspection programs for HTS boundary (e.g. boiler and pressure tubes) and for containment boundary (e.g. quarterly leak rate test)

h) automatic protection via special safety systems and standby safety support systems

i) adequate trip coverage for all design basis accidents

j) independence of special safety system (SSS) channels

k) two-out-of-three or three-out-of-four majority voting logic to initiate SSS action

NOTES AND REFERENCES

12. **The Five Physical Barriers.** In order for radioactive fission products to reach the public, they must first escape from the ceramic fuel pellets, then penetrate the fuel sheath, the heat transport boundary, the Containment boundary, and the exclusion zone. The integrity of these barriers is maintained using the following strategies:

⇔ *Obj. 3.2 l)*

    a) ensuring that reactor power is controlled, and fuel cooling maintained

    b) similar strategies as those to maintain reliable safety related systems, listed above

    c) HT boundary inspections--feeders, pressure tubes, boiler tubes

    d) Containment boundary leak rate tests

Additional Examples Of The Defence In Depth Philosophy:

The balance of this module is devoted to discussing additional examples of the *Defence in Depth* philosophy in NPP operations.

Defence In Depth Approach To Reactor Accidents

A *Defence in Depth* approach to reactor accidents includes the following three aspects:

1. **Accident prevention.** Accidents are prevented to the extent possible using the strategies of the above *Defence in Depth model*. Accidents are prevented by high quality design, construction, operation and regulatory control of the plant, consistent with the safety analysis. Systems are tested, inspected, operated and maintained according to approved procedures, by trained and skilled personnel, with an appropriate level of supervision. When faults are detected, they are corrected, or if repairs cannot be made, the plant is placed in a safe state. Automatic system responses, and use of approved procedures prevent process upsets from escalating into accidents.

⇔ *Obj. 3.3*

2. **Accident mitigation.** We cannot rely on accident prevention alone. Even with high quality design, operation and maintenance, accidents are still possible, and so we require high quality strategies for accident mitigation and management . In accident mitigation, the overall strategy is to shut down the reactor, maintain fuel cooling, and contain radioactivity. These functions are accomplished by qualified staff using accident *mitigation (Abnormal Incidents)* procedures, with the aid of safety systems designed especially for accident mitigation. The availability of poised systems to perform their mitigating functions is ensured by periodic testing.

NOTES AND REFERENCES

3. **Accident management.** The residual consequences of a mitigated accident are managed with the aid of emergency response procedures. These procedures include provisions for personnel assembly and accounting, search and rescue, off-site notifications, radiological surveys, public dose projection, public protective actions (banning food and water consumption, sheltering or evacuating the affected population, minimizing thyroid dose by distribution of KI pills), and communications with the media and local governments. Emergency response drills are run periodically to ensure availability of emergency response facilities, and to enhance staff response capability.

Maintenance on Safety Related Systems

Obj. 3.4 ⇔

Operation and maintenance activities on safety related systems can impair *Defence in Depth* provisions. As a result there is a need to ensure that adequate *Defence in Depth* is maintained. When a safety related system is impaired, or removed from service to complete maintenance, compensating action is taken to decrease risk--eg. to lower the risk of upsets, to verify the availability of back-ups, to minimize the outage duration, etc., or the plant is placed in a state where the safety system is not required.

Diagnosis of Events

Obj. 3.5 ⇔

The Control Room Operator (CRO) is trained to diagnose process failures using diagnostic aids. The SS independently verifies the CRO's diagnosis, providing a layer of *Defence in Depth* on the diagnosis. If the critical safety parameters (CSPs) remain within limits during the event-based recovery procedure, this is a good indication that the original diagnosis was appropriate--ie, that the correct procedure is being used. But even if the event were misdiagnosed, monitoring critical safety parameters and reacting according to plant restoration guides should return the plant to a safe state. **The CSP monitoring and restoration procedure is thus a *Defence in Depth* back-up in case the diagnosis is wrong, or the event-based procedure fails to cater to the specific operating conditions encountered, or an event-based procedure is unavailable.**

Placing an Automated Control System on Manual Control

Automated control systems have the following key features:

a) They feed back a result to effect a change in an input.

b) They are able to respond quickly to transients.

c) They have built-in safety limits to trigger a safety response.

NOTES AND REFERENCES

If manual control is initiated (with appropriate approvals), **then the same constraints as designed into the automated system must be satisfied**, or compensation must be made for their absence. For example, an operator may be dedicated to controlling the level in one liquid zone compartment above a specified minimum level, to simulate the 'undistracted' operation of the automatic controller.

⇔ *Obj. 3.6*

Experienced Workmanship

Work practices are established so that a person who has little experience with a task or job is supervised more closely than an experienced person. Thus, when quality of work is threatened by inexperience of the worker (*Defence in Depth* decreased), a compensating stratagem is employed--closer supervision (*Defence in Depth* increased to compensate).

Physical Barriers to Environmental Release of Fission Products

The following five barriers are built into the station design to prevent radioactivity escaping from the fuel to the public:

⇔ *Obj. 3.7*

1. **Ceramic Fuel** - The ceramic uranium dioxide fuel pellets entrap most of the fission products. These fission products would be released if the fuel were to melt. Fortunately, the fuel has a high melting point, but continuous cooling is nevertheless required, whether the reactor is at power or not, to prevent fuel failures. Another safety feature of the ceramic fuel is that it is relatively chemically inert with the heavy water coolant. Therefore, dispersion of fission products via corrosion and erosion when a sheath defect permits contact between the fuel pellets and the coolant is a relatively slow process.

2. **Fuel Sheath** - The fuel pellets are enclosed in a high integrity, welded zircaloy sheath. This sheath contains the gaseous and volatile fission products which escape from the pellets. It also prevents corrosion and erosion of the pellets by the coolant, and hence dispersion of fission products from the pellets which would result from these processes. The sheath is designed to withstand the stresses resulting from pellet thermal expansion, gaseous fission product build-up, external hydraulic pressure, and forces imposed by fuel handling.

3. **Heat Transport System Boundary** - The high integrity pressure tubes, piping, and vessels contain most fission products escaping via sheath defects until they are removed via the coolant purification system.

NOTES AND REFERENCES

4. **Containment Boundary** - This is designed to withstand the pressure surge of a worst case LOCA, with a small 'puff release' during the overpressure transient. Post LOCA containment venting via a filtered, monitored pathway minimizes the environmental radioactive release.

5. **Exclusion Zone** - No permanent residence is allowed within a 1 km radius from any reactor. This ensures significant dilution of an airborne radioactive release before it reaches any public habitation, thus reducing the resulting public dose.

Obj. 3.8 ⇔

Impact of large-scale fuel failures on Physical Barriers

Inadequate fuel cooling results in fuel overheating, and potentially in large scale fuel failures. In the event of large scale fuel failures, **at least two of the five physical barriers would be breached**--the fuel and the fuel sheath. In the case of a LOCA, the third barrier, the heat transport boundary, is also breached, leaving only the containment and exclusion zone barriers. In the case of a LOCA coincident with containment failure (dual failure), only the exclusion zone would remain as a physical barrier. Thus **the Containment boundary is a very strategic *Defence in Depth* barrier to fission product release**.

NOTES AND REFERENCES

Categories of Safety Related Systems

In assessing failures which could lead to the escape of radioactivity, station systems providing a safety function are classified as safety related systems. This classification is shown in Figure 3.2. The dotted tie between Safety Support Systems and Special Safety Systems refers to the active system support provided by the Safety Support Systems for the operation of the Special Safety Systems.

⇔ *Obj. 3.9*

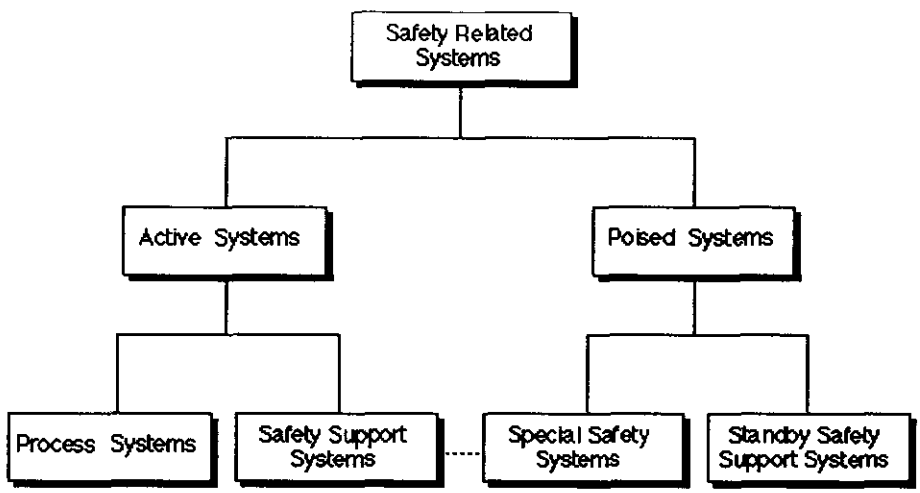

Figure 3.2: Safety related systems classification

NOTES AND REFERENCES

Obj. 3.10 ⇔

Examples of various safety related systems are given in Table 3.1. The active (normally operating) systems are found in either the Process System or Safety Support System category. The normally poised systems are found in the Special Safety System category or the Standby Safety Support System category. In some cases, safety related systems may fulfill requirements of more than one category. For example, the moderator system is a process system moderating the neutrons and removing heat resulting from gamma absorption. The moderator is also a Safety Support System since it may act as a heat sink in a loss of coolant accident with a coincident loss of emergency coolant injection. The primary heat transport system is a process system transferring heat from the fuel to the boilers. The primary heat transport system is also a Safety Support System since it is used to inject emergency coolant into the core.

The broad classification of backup heat sinks and secondary control areas are also found in two categories. In the case of backup heat sinks, some are active in normal operation while others are in the poised state. Similarly, some panels in the secondary control area are actively functioning while others are poised for operation.

Considering active safety related systems as the first line of defence, Standby Safety Support Systems, Special Safety Systems, and Emergency water and power systems constitute successive Defence in Depth barriers against large environmental releases. For example, class IV boiler feed water is backed up by class III Auxiliary Boiler Feed water and Steam Generator (Boiler) Emergency Cooling water (Standby Safety Support Systems). These are backed up by Emergency water to the boilers, with Emergency power supplying the Emergency water pumps.

Active Systems		Poised Systems	
Process System	Safety Support System	Special Safety System	Standby Safety Support System
• PHT • Mod. Aux.	• Electrical power • Process water • Instrument air • Backup heat sinks • Secondary control area • Annulus gas • PHT • Moderator	• SDS1 • SDS2 • ECI • Containment	• Steam Gen./Boiler Emergency Cooling • Standby generators • Containment venting • Setback and stepback • Emergency water • Emergency power • Secondary control areas • Backup heat sinks

Table 3.1: Examples of active and passive safety related systems

Margins and Trip Coverage

⇔ *Obj. 3.11*

Safety systems are designed to control, cool, and contain over a wide range of analyzed transients. The safety systems and equipment are operated in a conservative manner and are not continuously on the verge of tripping or breaking down. The difference between the operating level of a parameter and the value where something unsafe occurs, such as exceeding a design limit, is called the margin of safety for that parameter. For example, assume the reactor operates at 100% full power. If fuel element center-line melting will not occur below 130% full power, then the margin of safety against center-line melting is 30%.

Margin to trip also becomes a factor in operational safety. To illustrate, assume the reactor operates at 100% full power. If the shutdown system trip set point is at 110% full power, the margin to trip is 10%. Margin to trip is a measure of how much a parameter must vary before a protective trip is actuated, or simply the difference between the operating point and trip set point of a given parameter. Both concepts of margin of safety and margin to trip are illustrated in Figure 3.3.

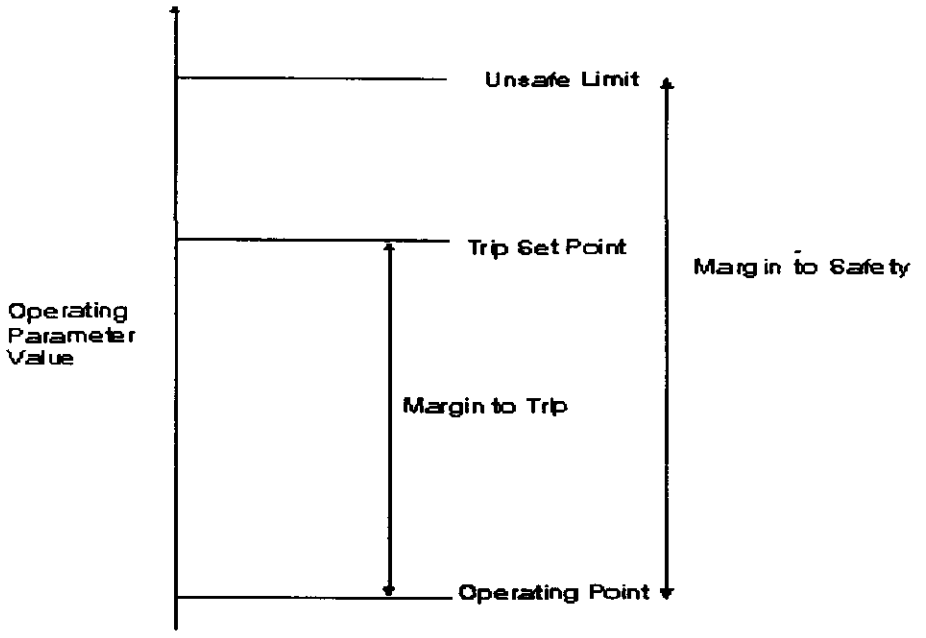

Figure 3.3: Margin To Trip and Margin of Safety

In choosing the safety system trip set points for margin to trip, an analytical approach is used to determine the most limiting set of circumstances in the design basis set. Error allowances are assigned to the trip set points to allow for operational uncertainties. Allowances may include such things as simulation and instrumentation errors, precision of calibration, and uncertainty in the parameter measurement.

The smaller the margin to trip is, the more likely spurious trips will occur. A protective system that unnecessarily trips the reactor is undesirable. In practice, the reactor may be derated to provide an adequate margin to trip if this margin is too small. For adequate trip coverage to provide safe operation, the margin to trip must always be less than the margin of safety, so that the protective trip occurs before the unsafe condition.

In summary, operational safety via the safety systems is provided in several ways:

a) An adequate margin of safety is designed into the system,

b) Sufficient margin to trip provides an operating buffer to prevent unnecessary trips,

c) Trip set points are chosen to provide adequate coverage taking into account allowances for error,

d) Margin to trip is kept less than margin of safety.

In the case of reactor trips, Defence in Depth is provided in that primary and back-up trips exist within each shutdown system (SDS) for most analyzed, higher frequency process failures.

SUMMARY OF THE KEY CONCEPTS

- The *Defence in Depth* operating philosophy is that multiple methods of high quality assurance are required of NPP design, construction, operation and maintenance.
- Assumptions underlying *Defence in Depth* philosophy:
  a) NPP operating personnel will occasionally make mistakes
  b) NPP equipment will occasionally fail;
  c) NPP design will have occasional imperfections.
- A *Defence in Depth* model was presented, featuring 12 barriers to protect workers, public and environment from large releases of fission products.
- Three aspects of the *Defence in Depth* approach to managing reactor accidents are:
  a) accident prevention
  b) accident mitigation
  c) accident accommodation/management
- When operation or maintenance activities impair one or more layers of defence, compensating actions are taken to decrease risk.

NOTES AND REFERENCES

- Use of approved procedures ensures adequate review for legal, technical and operating constraints, for system interactions and for deterioration of physical barriers to the release of radioactivity.

- Review and approval of *abnormal incidents* procedures ensures that the upset unit is placed in a safe state.

- A *Defence in Depth* approach to event diagnosis is provided by the SS independently verifying the CRO diagnosis, and by the CSP monitoring and restoration procedure, which should return the unit to a safe state even if the diagnosis was wrong, or the event-based procedure fails to cater to the specific operating conditions encountered.

- When an automated system is placed on manual control, the same constraints designed into the automated system apply. An operator may be dedicated to controlling a parameter, to simulate the undistracted operation of the automatic controller.

- Training and qualification equip personnel to recognize situations where levels of defence may be jeopardized or impaired.

- The five physical barriers between fission products and the public are:

  a) Ceramic fuel,

  b) Fuel Sheath

  c) Heat Transport System

  d) Containment Boundary

  e) Exclusion Zone

- When large scale fuel failures occur, at least two of the five physical barriers are breached--the Ceramic fuel, and the fuel sheath. In the case of a LOCA, the third barrier, the primary heat transport system boundary is also breached. In the unlikely event of a LOCA with coincident loss of containment (dual failure), the only barrier remaining is the exclusion area.

- *Defence in Depth* is provided for the control/cool/contain functions of safety related process systems via the following back-ups: standby safety support systems, special safety systems, and Emergency water and power systems.

NOTES AND REFERENCES

- The primary stratagem for preventing operating parameters from reaching unsafe values, is to choose an operating point which provides a conservative margin of safety. *Defence in Depth* is provided by an automatic protective trip. The trip set point is chosen such that the trip margin is less than the safety margin, so that the trip occurs before the unsafe condition is reached, allowances for uncertainties in measured and calculated values having been taken into account.

- *Defence in Depth* is enhanced for reactor trips in that primary and back-up trips exist within each SDS for most analyzed system failures.

NOTES AND REFERENCES

ASSIGNMENT

1. Carefully prepare detailed answers for the Module 3 learning objectives.

2. List 6 standby safety support systems and describe the purpose of each system with respect to nuclear safety.

3. As directed by your Instructor, review the following reactor incidents:

   a) Pickering Unit 2 flux tilt incident of 1990

   b) TMI accident of 1979

   c) Chernobyl Accident of 1986

   d) Salem marsh grass incident of 1994

   For each incident,

   a) Identify the initiating event,

   b) Identify which of the 12 layers of the *Defence in Depth* model were violated.

   c) State which, in your opinion, was the greater problem--equipment failures or inappropriate human activity. Give your rationale.