UNITED STATES
ATOMIC ENERGY COMMISSION
WASHINGTON, D.C. 20545

June 11, 1969

R. S. Boyd, AD/RP, DRL
D. J. Skovholt, AD/RO, DRL
L. D. Low, Director, CO
E. G. Case, Director, DRS
J. A. McBride, Director, DML
THRU: P. A. Morris, Director
Division of Reactor Licensing

REACTOR TECHNOLOGY MEMORANDUM NO. 6 -- CONTROL ROOM DESIGN CONSIDERATIONS

The enclosed RTM sets forth proposed guidelines with respect to minimum requirements for control room design considerations.

This information is intended to be used in safety evaluations of power reactor facilities and such other facilities as may be appropriate. Comments on this RTM are requested on or before July 11, 1969, in order that necessary revisions can be made prior to further distribution. A copy of any correspondence pertaining to this RTM should be sent to C. W. Moon, Safety Systems Technology Branch, Division of Reactor Licensing.

Saul Levine, Assistant Director
for Reactor Technology
Division of Reactor Licensing

RT-391A
DRL:I&PTB:ODP

Enclosure:
RTM-6

cc w/encl:
C. K. Beck, DR
M. M. Mann, DR
C. L. Henderson, DR
R. L. Doan, DR
Branch Chiefs, DRL
B. Grimes, DRL
Assistant Directors, CO
Branch Chiefs, CO
J. McEwen, DRS
Branch Chiefs, DRS
Branch Chiefs, DML

Issued: June 11, 1969

REACTOR TECHNOLOGY [illegible] NO. 6

CONTROL ROOM DESIGN CONSIDERATIONS

I. INTRODUCTION

The purpose of this RTM is to provide minimum requirements which should be taken into account in the evaluation of the control room design for a nuclear facility against Criterion 11, Part 50, General Design Criterion for Nuclear Power Plant Construction Permits. The requirements were developed using the basic approach that:

1. The control room should be designed to allow occupancy during all accidents which have been analyzed for the facility up to and including the design basis accident.

2. If access to the control room is lost, it shall be possible to shut the reactor down and maintain it in a safe condition from a location(s) outside the control room.

II. MINIMUM REQUIREMENTS

1. Radiation Protection

The control room shall be so designed as to provide adequate radiation protection for personnel within the limits defined by 10 CFR Part 20. As established by 10 CFR 20, the present exposure limit is 3 rem whole body dose in any calendar quarter for individual in a restricted area. This protection shall be designed so as to permit access, even under accident conditions, to equipment in the control room or other areas as necessary to shut down and maintain safe control of the facility. The exposure limit for the operating personnel during a nuclear incident should not exceed 5 rem whole body dose in any calendar year.

2. Fire Protection

The control room design shall be such as to minimize the possibility of fire. Continuing occupancy where possible should be provided for in the case of control room fire or smoke. The control room building components, finish materials and furnishings shall be noncombustible. Combustible supplies

such as logs, records, procedures and manuals should be limited to the amounts required for plant operation. Fire fighting equipment including fire extinguishers and breathing apparatus should be available to the control room.

3. Evacuation of Control Room

In the event that it becomes necessary to evacuate the control room, it shall be possible to shut the reactor down and maintain it in a safe condition from a location(s) outside the control room.

(a) It should be assumed that, during normal plant operation with all plant equipment operable, access to the control room is lost for a relatively long time.

(b) The facility should be examined to assure that hot shutdown from full power can be accomplished from outside the control room in a relatively short time of the order of an hour or so. The applicant should provide a general plan and show that adequate instrumentation and control are available to allow the plant to be safely placed in hot shutdown from outside the control room.

(c) The facility should be further examined to assure that without necessarily adding any equipment, existing equipment, instrumentation, panels, etc., can be manipulated (including opening panels, jumpering wires, etc.) in order to achieve cold shutdown in a period of time not to exceed several days. The applicant should provide a general plan and show that it is feasible to safely bring the plant to cold shutdown from outside the control room.

(d) The facility should be examined to establish the length of time that it can be easily maintained in a hot standby condition from outside the control room. This period of time should exceed that in (c) above.

III. ITEMS TO BE FURNISHED AT A LATER DATE

The following will be provided at a later date:

(1) Control room ventilation system radiation protection requirement.

(2) Control room lighting.

(3) Control room communications.

(4) Technical bases for the RTM.

NRC's present philosophy and criteria for control room design data display equipment and instrumentation appear in the following documents:

General Design Criteria and Control 13 - Instrumentation

Criterion 13—Instrumentation and control. Instrumentation shall be provided to monitor variables and systems over their anticipated ranges for normal operation, for anticipated operational occurrences, and for accident conditions as appropriate to assure adequate safety, including those variables and systems that can affect the fission process, the integrity of the reactor core, the reactor coolant pressure boundary, and the containment and its associated systems. Appropriate controls shall be provided to maintain these variables and systems within prescribed operating ranges.

General Design Criterion 19 - Control Room

Criterion 19—Control room. A control room shall be provided from which actions can be taken to operate the nuclear power unit safely under normal conditions and to maintain it in a safe condition under accident conditions, including loss-of-coolant accidents. Adequate radiation protection shall be provided to permit access and occupancy of the control room under accident conditions without personnel receiving radiation exposures in excess of 5 rem whole body, or its equivalent to any part of the body, for the duration of the accident.

Equipment at appropriate locations outside the control room shall be provided (1) with a design capability for prompt hot shutdown of the reactor, including necessary instrumentation and controls to maintain the unit in a safe condition during hot shutdown, and (2) with a potential capability for subsequent cold shutdown of the reactor through the use of suitable procedures.

General Design Criterion 21 - Protection System Reliability and Testability

Criterion 21—Protection system reliability and testability. The protection system shall be designed for high functional reliability and inservice testability commensurate with the safety functions to be performed. Redundancy and independence designed into the protection system shall be sufficient to assure that (1) no single failure results in loss of the protection function and (2) removal from service of any component or channel does not result in loss of the required minimum redundancy unless the acceptable reliability of operation of the protection system can be otherwise demonstrated. The protection system shall be designed to permit periodic testing of its functioning when the reactor is in operation, including a capability to test channels independently to determine failures and losses of redundancy that may have occurred.

General Design Criterion 22 - Protection system independence

Criterion 22—Protection system independence. The protection system shall be designed to assure that the effects of natural phenomena, and of normal operating, maintenance, testing, and postulated accident conditions on redundant channels do not result in loss of the protection function, or shall be demonstrated to be acceptable on some other defined basis. Design techniques, such as functional diversity or diversity in component design and principles of operation, shall be used to the extent practical to prevent loss of the protection function.

General Design Criterion 24 - Separation of protection and control systems

Criterion 24—Separation of protection and control systems. The protection system shall be separated from control systems to the extent that failure of any single control system component or channel, or failure or removal from service of any single protection system component or channel which is common to the control and protection systems leaves intact a system satisfying all reliability, redundancy, and independence requirements of the protection system. Interconnection of the protection and control systems shall be limited so as to assure that safety is not significantly impaired.

General Design Criterion 63 - Monitoring fuel and waste storage

Criterion 63—Monitoring fuel and waste storage. Appropriate systems shall be provided in fuel storage and radioactive waste systems and associated handling areas (1) to detect conditions that may result in loss of residual heat removal capability and excessive radiation levels and (2) to initiate appropriate safety actions.

General Design Criterion 64 - Monitoring radioactivity releases

Criterion 64—Monitoring radioactivity releases. Means shall be provided for monitoring the reactor containment atmosphere, spaces containing components for recirculation of loss-of-coolant accident fluids, effluent discharge paths, and the plant environs for radioactivity that may be released from normal operations, including anticipated operational occurrences, and from postulated accidents.

NRC's present-day review of control rooms and instrumentation is covered under the aegis of Standard Review Plans:

7.1 "Instrumentation and Controls"

7.2 "Reactor Trip System"

7.3 "Engineered Safety Features Systems"

7.4 "Systems Required For Safe Shutdown"

7.5 "Safety-Related Display Instrumentation"

7.6 "All Other Instrumentation Required For Safety"

7.7 "Control Systems Not Required For Safety"

7-A (Appendix) - ICSB Branch Technical position 21
"Guidance for Application of Regulatory Guide 1.47"
ICSB Branch Technical Position 23
"Qualification of Safety-Related Display Instrumentation
For Post-Accident Condition Monitoring and Safe Shutdown"

In addition to meeting the general design criteria, present-day control rooms and instrumentation are required to meet the following NRC requirements copies of which are attached to this enclosure:

Regulatory Guide 1.47 - "Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety Systems" (May 1973)

Regulatory Guide 1.78 - "Assumptions for Evaluating the Habitability of a Nuclear Power Plant Control Room during a Postulated Hazardous Chemical Release" (June 1974)

Regulatory Guide 1.95 - "Protection of Nuclear Power Plant Control Room Operation Against an Accidental Chlorine Release" (Rev. 1, January 1977)

Regulatory Guide 1.97 - "Instrumentation for Light-Water-Cooled Nuclear Power Plants to Assess Plant Conditions During and Following An Accident" (Rev. 1, August 1977)

5 - Control Room Design /Approval/Acceptance: as presently understood control room designs are developed by the utility in conjunction with the architect-engineer - under the broad NRC guidelines described in Item 4 above. The utility apparently has the overall veto power - as they are the customer.

The NRC looks at specific equipment in accordance with the aforementioned GDC's, RG's, SRP's, and does not look at overall control room design or "human factors engineering." The bulk of these detailed reviews are done by NRR's Instrumentation and Control Systems Branch of DSS with secondary review responsibilities held by the Auxiliary Systems Branch, Containment Systems Branch, Reactor Systems Branch, Power Systems Branch, Quality Assurance Branch, Mechanical Engineering Branch, and the Core Performance Branch.

The reviews are done from the early CP application stage through the final granting of the operating license.

6. What were and are NRC requirements (or limitations on) use of computers for alarms, display, etc.

The NRC has not permitted the use of computers to alarm or display the status of system variables for the purpose of diagnosing departure from safety limits that would require manual operator action to mitigate the consequences of an event. Computer use for such diagnostics has generally been discouraged because of the stringent qualifications and independence requirements imposed upon systems required for safety. Seismic qualification, quality control, and redundancy requirements make the use of computers impractical from an economic standpoint.

Diagnostics (alarms, display) for manual operator actions to mitigate the consequences of an event must be hard wired and meet all the qualification requirements imposed on systems important to safety.

The use of computers has been permitted for monitoring safety systems variables, through qualified isolation devices, for normal plant control within the hard-wired safety limits. This use of computers has not been within the NRC staff's scope of review because normal plant control systems are not assumed to interact adversely with systems important to safety negating their proper response. Therefore, diagnostics (alarms, displays, etc.) for operator actions has been limited to the needs of the individual licensee and his plant operational philosophy.

Regarding NRC's requirements on alarms, and display instrumentation the licensee is guided by General Design Criterion (GDC) 13 "Instrumentation and Control," Regulatory Guide (G.G.) 1.47 "Bypassed and and Inoperable Status Indication for Nuclear Power Plant Safety System," and R.G. 197 "Instrumentation for Light Water Cooled Nuclear Power Plants to Assess Plant Conditions During and Following an Accident."

7. Prepare lists of:

Times When Instruments were Disbelieved by Operators

1. One pressurizer code safety valve tail pipe high temperature alarm with RCDT pressure at 12 psig and increasing should have alerted operator to continuous flow of primary coolant to RCDT.

2. The pressurizer level was generally increasing during the 1-4 minute time frame and this is the indication that controlled operator response. The decreasing primary system pressure was not believed as an indicator of water inventory.

3. Same as 1 above.

4. RCS hot leg temperature reached saturation with pressure. Should have indicated to operators that voids existed in system.

5. Reactor building level alarm (10 min. 48 sec.) should have told operator a leak existed in system.

6. Increase in RB pressure of about one psi at 14 minutes should have indicated leak.

7. Loop flow indication -- slow reduction in flow from about 2 min. to 15 min. should have indicated presence of voids.

8. Intermediate cooling water radiation monitor alarms were believed to be due to high background radiation levels-61 minutes.

9. Operators were unable to account for increased reactor building temperature, should have indicated leak.

10. When loop B RCPs were turned off at 74 minutes, OTSG pressure dropped from 960 psig to 140 psig in 18 minutes. This should have indicated presence of voids in loop and lack of backflow.

11. At 81 minutes, operator requests computer printout of pressurizer relief and safety valve outlet temperatures. Takes no action based on high temperature readings.

12. RCS sample shows a factor of 10 increase in activity at 90 minutes. Apparently not attributed to fuel failure even through a crud burst or iodine spike in a "new" plant is very unlikely.

13. All radiation monitors exhibiting substantial ramp increase at 100 minutes should have indicated fuel damage.

14. RCS hot and cold leg temperatures diverged widely with the hot leg reaching superheated conditions. Should have indicated core uncovery to operators (~103 minutes).

15. Station manager did not believe direct readings of incore thermocouples which were reading as high as 2620°F (4-5 hrs.).

16. RB experienced pressure spike of about 28 psig initiating RB spray. Indication believed to be "noise" or electrical problem and not indicative of real pressure. Recognition of H_2 burning did not occur.

b. Times when Instrumentation was Inadequate

1. Instruments in the condensate polisher resin transfer system may have been inadequate in that water was able to enter the compressed air system.

2. Alarm Printer output for makeup pump 1A, 1B, and 1C status (norm/trip) found to be reversed due to software error, potentially misleading operators who read printout.

3. No emergency feedwater flow indication, operators assumed flow because pumps were running. Relied upon water hammer noise for flow indication.

4. Accuracy of pressurizer level instrumentation

Because of the nature of the TMI-2 accident, the pressurizer level did not accurately represent the water levels in the RCS. The indications of high pressurzer level apparently misled the operators into believing that the RCS was full of water throughout the accident; thus, actions to refill and cool the core were not believed to have been needed.

5. Computer storage and printout capabilities

The alarm computer printout located in the control room began experiencing significant backups early in the accident, and was actually out of service for some time period. No permanent storage in the computer occurs, so that when the printer is out of service, information is lost completely. As a result of these problems, the computer apparently was of little value to the operators.

6. Operators misinterpreted SRM count rate increases (more than 2 decades) as a concern for criticality and borated system. Rate increase was apparently due to uncovering of core.

7. Instrumentation Ranges

   Various important instruments in the control room had ranges of indication which were quickly exceeded, so that inadequate or misleading information was presented to the operator. RCS hot leg temperature sensors, core exit thermocouples, and many radiation monitors experienced this problem.

8. Instrumentation environmental qualification

   Some instrumentation which was significant in controlling and understanding this accident experienced environmental conditions beyond their design basis. Pressurizer level sensors were sporadically failing throughout the accident; apparently some Reactor Building radiation monitors also failed.

9. PORV status instrumentation

   In the TMI-2 control room, the position of the PORV is indicated by a light. Since this light actually indicates that the electric power to the valve has been removed, it does not indicate the physical position of the valve. Thus the operators were led to believe by the PORV indicator that the valve had reclosed when in fact it remained open, causing the loss of RCS coolant.

10. No reactor vessel water level indication

In all PWRs, water level in the RCS is measured in the pressurizer. Thus in an accident such as that at TMI-2, when phenomena such as that discussed in 2.3.3 occur, an accurate measure of water level in the vessel and core is not available.

11. No remote visual observation equipment

No remote visual equipment such as television cameras are installed in the Reactor Building of any PWR; so no visual indication of the status of euipment, etc. was available to the operators in the TMI-2 control room.

8. Describe manuals and procedures operators at TMI-2 had available. Did they use any such procedures in this case?

The sets of procedures in the control room that relate to plant operation are broken into several categories: administrative procedures, normal operating procedures, instrumentation and control procedures, electrical systems, abnormal operations (which include turbine trip and reactor coolant pump emergencies), emergency operations (which include loss of coolant, excess radiation levels, loss of feedwater, reactor trip and pressurizer system failure).

Primarily, the operator would be expected to refer to the abnormal operation and emergency operation procedures for an accident.

The following specific procedures were applicable during the accident:

1. Emergency Procedure 2202-2.2, Rev. 3 10/13/78

   Immediate actions were apparently followed by operators following loss of main feedwater flow although some actions were delayed because of the rapid sequence of events.

2. Emergency Procedures 2203-2.2 Rev. 7 10/25/78 - turbine trip

   Immediate actions were apparently followed by operators following turbine trip. Operator checked status of emergency feedwater but did not notice block valves closed. This was a crucial point in the accident. Plant parameters would indicate that EFW flows were being throttled by operators even when OTSG level could not be maintained and was falling.

3. Emergency Procedure 2202-1.1 Rev. 6 10/25/78 - Reactor Trip

   Immediate actions were apparently followed by operators following reactor trip. Several of the procedure steps could not be accomplished because of plant conditions and a lack of understanding of what was happening by the operators; i.e., maintain pressurizer level at 100 inches.

4. Emergency Procedure 2202-1.3 Rev. 8, 5/12/78
   Loss of Reactor Coolant/Reactor Coolant System Pressure.

   With two major exceptions, the majority of the immediate and followup actions for the Loss of Reactor Coolant/Reactor Coolant System Pressure were followed. The operators throttled the HPI because they did not perceive a loss of coolant problem. Also, the reactor coolant pumps were not tripped when pressure dropped to 1200 psig.

5. Other procedures involved included:

   a. Abnormal Procedure 2203-1.1 - Loss of Boron Moderator Dilution
   b. 2102-3.3 - Decay Heat Removal VA OTSG
   c. 2103-1.4 - Reactor Coolant Pump Operator
   d. 2104-4.1 - Miscellaneous Liquid Rad Waste Disposal
   e. 2202-1.5 - Pressurizer System Failure

9. As of now, what do we know about ways in which the control room design, or layout itself, may have contributed to this accident? List or describe and discuss briefly each such way.

There are a number of ways in which the control room design and layout may have contributed to the accident. The significance of such contribution is not yet fully understood and is being addressed as part of this overall investigation. The following is a listing of those areas which currently are considered to be of potential significance.

(1) From the initiation of the accident, hundreds of alarms were received and annunciated in the control room. Because of the large number of alarms, the operators were not able to screen the alarms and to use them as a diagnostic tool in understanding what had happened and was in the process of happening. Their diagnosis, therefore, relied primarily upon indications on the instruments in the control room. This was essentially the same as there not being any alarms available to the operators, and, of course, the large number of alarm indications were a confusion factor which may have made it more difficult for the operators to arrive at reasoned decisions. The number of alarms in the control room the lack of prioritization of alarms, and the grouping of alarms, do not appear to have been optimized to aid the operators in understanding the more important aspects of any given event.

(2) There was no indication of auxiliary feedwater flow to the steam generators. Thus, the operator was forced to visit the feedwater panel three times before diagnosing a lack of feedwater flow. The first time, after a few seconds, he verified the pumps running. The second time, as level was

dropping through 30 inches, he verified the control valve opening. It was not until the third time, when generator levels had dropped to 10 inches that a lack of auxiliary feedwater flow was diagnosed.

(3) The demand light on the PORV, as opposed to a flow switch or absolute valve position indication, played a role in misleading the operator into thinking the PORV was closed. Alternate indications although ambiguous, were adequate in hindsight to indicate that the valve was open and, apparently, they were checked several times but not believed due to a combination of:

a. Confusion. Hundreds of alarms. Operators believed the tailpipe temperature was 235^{o} but the computer was telling them 285^{o}F. The valve would normally lift for this transient and heat the tailpipe somewhat. The valve had been previously leaking and the tailpipe was $\sim$ 190^{o}F prior to the transient.

b. Misinformation and lack of discipline to follow prescribed emergency procedures. Operators believed that if the valve were truly open temperatures would be much higher, on the order of 500^{o}F. In fact, about 285^{o}F is as hot as the tailpipe can get. Procedure indicates it should be isolated if over 130^{o}F normal reading and/or if over 200^{o}F.

c. General reluctance to isolate the valve because they did not want to rely on and cause the safety valves to actuate. The approach was followed despite indications of water in containment sump and ruptured drain tank. (It is not clear whether or not drain tank indications were actually checked).

(4) The reactor coolant draintank perimeters do not alarm on the alarm panels in the immediate view of the operators. To determine if there is an alarm on the reactor coolant draintank annunicator the operators must clear all audible alarms on the front panels. A knowledge of the alarm status of the PORV and more easily understood alarm indication may have helped the operators to diagnose this condition earlier in the accident.

(5) The fuel handling building exhaust radiation monitors showed ramp increases in iodine readings at about 18 minutes into the accident. The reactor building exhaust radiation monitor increased by a factor of about 10. These instruments are located on the lower part of the vertical back panel and operators standing at the front panels are not able to view these trends. If the operators could have been more fully aware of the magnitude of the increase in radiation readings as they were occuring, they may have better understood that fuel damage was actually occuring early in the accident.

(6) The operators relied upon the direct reading gauge for Th in the primary system. This gauge was not able to read the temperatures that were actually seen by the system and pegged out high early in the accident. There was, however, a strip chart recorder "primary system temperatures" #10 which is located on the back row of the vertical panels. This recorder clearly shows Th temperatures in the 700 to 800 degree F range. If the operators had been fully aware of this indication, it may have permitted them to appreciate early in the accident that there were superheated conditions in

the system.

(7) The control panels are not layed out in such a way that normal status is easily descernable. The valve position indication for example, indicates open-close and if it is required for normal or safe operation that certain valves be open and certain valves be closed then you will have some red and some green indications. Such a display is not conducive to recognizing misalignments. If the panels were arranged such that abnormal alignments were easily indicated, then it is unlikely that the feedwater block valves would have remained in the block conditions (assuming that they were inadvertantly left in that condition from some previous operation).

(8) The instruments in the control room are generally small and difficult to read from the position that an operator would normally stand to observe the process of an accident. In order to clearly see what an instrument is reading the operator must approach that instrument closely. In addition, many of these instruments record on a chart, however, the window which shows the recording is very small and recording speed is very slow such that the following of any trends is extremely difficult. A control room which had easily seen instrumentation which recorded trends in a clear fashion would likely have permitted a much clearer understanding of the events that had taken place and would perhaps have permitted the operators to appreciate the seriousness of the condition and to take the appropriate corrective action. There is a proliferation

of non-critical information displayed adjacent to those displays and controls which assume major importance during emergencies yet all presentations appear equally important as displayed.

(9) There was no indication of the level of the water in the RCS. Although other indications were available which indirectly provided course information on the water level, the operators were not able to properly interpret their indications. The presence of a reactor vessel water level gauge would likely have resulted in the operators taking actions which prevented significant core damage.

ATTACHMENT

To

ENCLOSURE 3

IEEE - 279, Regulatory Guides, TMI-2 PSAR

IEEE
No. 279
AUGUST 1968

Superseded by
IEEE 279-1971

Proposed IEEE Criteria for

NUCLEAR POWER PLANT PROTECTION SYSTEMS

(Effective August 30, 1968)

Send discard

PUBLISHED BY
THE INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS
345 EAST 47 STREET, NEW YORK, N.Y. 10017

1. SCOPE

These Criteria establish minimum requirements for the fety-related functional performance and reliability protection systems for stationary, land-based nuclear actors producing steam for electric power generation. lfillment of these requirements does not necessarily ly establish the adequacy of protective system funcnal performance and reliability. On the other hand, hission of any of these requirements will, in most inances, be an indication of system inadequacy. For purses of these Criteria, the nuclear power plant protection stem encompasses all electric and mechanical devices d circuitry (from sensors to actuation device input rminals) involved in generating those signals associated th the protective function. These signals include those at actuate reactor trip and that, in the event of a seus reactor accident, actuate engineered safeguards ch as containment isolation, core spray, safety injection, essure reduction, and air cleaning.

2. DEFINITIONS

The definitions in this Section establish the meanings words in the context of their use in these Criteria.

1 System. Where not otherwise qualified, the word ystem" refers to the nuclear power plant protection stem, as defined in the scope section of these Criteria.

2 Channel. An arrangement of components and odules as required to generate a single protective action gnal when required by a plant condition. A channel ses its identity where single action signals are combined.

3 Module. Any assembly of interconnected components hich constitutes an identifiable device, instrument or ece of equipment. A module can be disconnected, reoved as a unit, and replaced with a spare. It has dehable performance characteristics which permit it to e tested as a unit. A module could be a card or other ubassembly of a larger device, provided it meets the equirements of this definition.

4 Components. Items from which the system is asembled (e.g., resistors, capacitors, wires, connectors, ansistors, tubes, switches, springs, etc.).

5 Protective Action. An action initiated by the protecion system when a limit is exceeded. A protective action an be at channel or system level.

6 Protective Function. A system protective action hich results from the protective action of the channels onitoring a particular plant condition.

7 Type Tests. Tests made on one or more units to erify adequacy of design.

3. DESIGN BASIS

A specific protection system design basis shall be provided for each nuclear power plant. The information thus provided shall be available, as needed, for making judgments on system functional adequacy.

The design basis shall document as a minimum, the following:

(a) the plant conditions which require protective action;

(b) the plant variables (e.g., neutron flux, coolant flow, pressure, etc.) that are required to be monitored in order to provide protective actions;

(c) the minimum number and location of the sensors required to monitor adequately, for protective function purposes, those plant variables listed in 3(b) that have a spatial dependence;

(d) prudent operational limits for each variable listed in 3(b) in each applicable reactor operation mode;

(e) the margin, with appropriate interpretive information, between each operational limit and the level considered to mark the onset of unsafe conditions;

(f) the levels that, when reached, will require protective system action;

(g) the range of transient and steady-state conditions of both the energy supply and the environment (e.g., voltage, frequency, temperature, humidity, pressure, vibration, etc.) during normal, abnormal, and accident circumstances throughout which the system must perform;

(h) the malfunctions, accidents, or other unusual events (e.g., fire, explosion, missiles, lightning, flood, earthquake, wind, etc.) which could physically damage protection system components or could cause environmental changes leading to functional degradation of system performance, and for which provisions must be incorporated to retain necessary protection system action;

(i) minimum performance requirements including the following:

1) system response times;
2) system accuracies;
3) ranges (normal, abnormal and accident conditions) of the magnitudes and rates of change of sensed variables to be accommodated until proper conclusion of the protection system action is assured.

Note: The development of the specific information to be used in fulfillment of the above requirements is not within the scope of these Criteria. The development of standard criteria and requirements relating to the determination of such design basis information as unsafe conditions requiring protective functions, plant variables to be monitored, operational limits, margins, set points, etc., are under consideration in American Nuclear Society Standards Subcommittee 4.

4. REQUIREMENTS

4.1 General Functional Requirement. The nuclear power plant protection system shall, with precision and reliability, automatically initiate appropriate protective action whenever a plant condition monitored by the system reaches a preset level. This requirement applies for the full range of conditions and performance enumerated in 3(g), 3(h), and 3(i).

4.2 Single Failure Criterion. Any single failure within the protection system shall not prevent proper protection system action when required.

Note: "Single failure" includes such events as the shorting or open-circuiting of interconnecting signal or power cables. It also includes single credible malfunctions or events that cause a number of consequential component, module, or channel failures. For example, the overheating of an amplifier module is a "single failure" even though several transistor failures result. Mechanical damage to a mode switch would be a "single failure" although several channels might become involved.

4.3 Quality of Components and Modules. Components and modules shall be of a quality that is consistent with minimum maintenance requirements and low failure rates. Quality levels shall be achieved through the specification of requirements known to promote high quality, such as requirements for design, for the derating of components, for manufacturing, quality control, inspection, calibration, and test.

4.4 Equipment Qualification. Type test data or reasonable engineering extrapolation based on test data shall be available to verify that equipment that must operate to provide protection system action will meet, on a continuing basis, the performance requirements determined to be necessary for achieving the system requirements.

Note: Attention is directed particularly to the requirements of 3(g) and 3(i).

4.5 Channel Integrity. All protection system channels shall be designed to maintain necessary functional capability under extremes of conditions (as applicable) relating to environment, energy supply, malfunctions, and accidents.

Note: See especially the requirements documented in response to 3(f), 3(g), 3(h), and (i).

4.6 Channel Independence. Channels that provide signals for the same plant protective function shall be independent and physically separated to accomplish decoupling of the effects of unsafe environmental factors, electric transients, and physical accident consequences documented in the design basis, and to reduce the likelihood of interactions between channels during maintenance operations or in the event of channel malfunction.

4.7 Control and Protection System Interaction. Where a plant condition that requires protective action can be brought on by a failure or malfunction of the control system, and the same failure or malfunction prevents proper action of a protection system channel or channels designed to protect against the resultant unsafe condition, the remaining portions of the protection system shall independently meet the requirements of paragraphs 4.1 and 4.2.

4.8 Derivation of System Inputs. To the extent feasible and practical, protection system inputs shall be derived from signals which are direct measures of the desired variables.

4.9 Capability for Sensor Checks. Means shall be provided for checking, with a high degree of confidence, the operational availability of each system input sensor during reactor operation.

This may be accomplished in various ways, for example:

(a) by perturbing the monitored variable; or
(b) within the constraints of paragraph 4.11, by introducing and varying, as appropriate, a substitute input to the sensor of the same nature as the measured variable; or
(c) by cross checking between channels that bear a known relationship to each other and that have read-outs available.

4.10 Capability for Test and Calibration. Capability shall be provided for testing and calibrating channels and the devices used to derive the final system output signal from the various channel signals. For those parts of the system where the required interval between testing will be less than the normal time interval between plant shutdowns, there shall be capability for testing during power operation.

4.11 Channel Bypass or Removal from Operation. The system shall be designed to permit any one channel to be maintained, and when required, tested or calibrated during power operation without initiating a protective function. During such operation the active parts of the system shall of themselves continue to meet the single failure criterion.

Exception: "One-out-of-two" systems are permitted to violate the single failure criterion during channel bypass provided that acceptable reliability of operation can be otherwise demonstrated. For example, the bypass time interval required for a test, calibration, or maintenance operation could be shown to be so short that the probability of failure of the active channel would be commensurate with the probability of failure of the "one-out-of-two" system during its normal interval between tests.

4.12 Operating Bypasses. Where operating requirements necessitate automatic or manual bypass of a protective function, the design shall be such that the bypass will be removed automatically whenever permissive conditions are not met. Devices used to achieve automatic removal of the bypass of a protective function are part of the protection system and must be designed in accordance with these Criteria.

...ne part of the system has been bypassed or deliberately ...dered inoperative for any purpose, this fact shall be ...ntinuously indicated in the control room.

...4 Access to Means for Bypassing. The design shall ...rmit the administrative control of the means for man...lly bypassing channels or protective functions.

...5 Multiple Set Points. Where it is necessary to change ... a more restrictive protective action set point to pro...de adequate protection for a particular mode of oper...ion or set of operating conditions, the design shall pro...de positive means of assuring that the more restrictive ... point is used. The devices used to prevent improper use ...less restrictive set points shall be considered a part of the ...otection system and shall be designed in accordance ...th the other provisions of these Criteria regarding per...rmance and reliability.

...6 Completion of Protective Action Once It Is Initiated. ...e protection system shall be so designed that, once ...tiated, a protection system action shall go to com...tion. Return to operation shall require subsequent ...liberate operator action.

4.17 Manual Actuation. Means shall be provided for manual initiation of protection system action. Failure in an automatic protection circuit shall not prevent the manual actuation of protective functions. Manual actuation shall require the operation of a minimum of equipment.

4.18 Access to Set Point Adjustments, Calibration, and Test Points. The design shall permit the administrative control of access to all protective action set point adjustments, module calibration adjustments, and test points.

4.19 Identification of Protective Actions. Protective actions shall be indicated and identified down to the channel level.

4.20 Information Read-Out. The protection system shall be designed to provide the operator with accurate, complete, and timely information pertinent to its own status and to plant safety. The design shall minimize the development of conditions which would cause meters, annunciators, recorders, alarms, etc.. to give anomalous indications confusing to the operator.

4.21 System Repair. The system shall be designed to facilitate the recognition, location, replacement, repair, or adjustment of malfunctioning components or modules.

TMI 2 PSAR

7.4 OPERATING CONTROL STATIONS

Following proven power station design philosophy, all control stations, switches, controllers, indicators, and other information display necessary to start up, operate, and shut down Unit 2 will be located in one control room. Control functions necessary to maintain nuclear unit safe conditions after a loss-of-coolant accident will be initiated from the centrally located control room. Controls and instruments for certain auxiliary systems may be located at remote control stations when the system controlled does not involve power generation control or emergency functions.

7.4.1 GENERAL LAYOUT

The control room, as shown in Figure 7-14, will be designed so that one man can supervise operation of Unit 2 during normal steady-state conditions. During other than normal steady-state operating conditions, other operators will be available to assist the control operator. The control room will be arranged so that emergency and frequently used instruments and controls are located on an operating console which is clearly visible and close to the operator. Less frequently used control and informational displays will be located more remotely on vertical panel boards. The console will be formed by short, straight sections of bench boards arranged to form an approximately semicircular operating console that allows the operator easy access to each section.

7.4.2 INFORMATION DISPLAY AND CONTROL FUNCTION

The necessary information for routine monitoring of the nuclear steam supply system and the balance of the plant will be displayed on the operator's console and the various vertical boards located within the control room. Information display and control equipment frequently employed on a routine basis, or protective equipment quickly needed in case of an emergency, will be mounted on the desk-type console sections. Recorders and radiation monitoring equipment will be mounted on the separate vertical panel sections located behind the consoles. Infrequently used equipment, such as indicators and controllers used primarily during startup and shutdown, will be mounted on vertical panels which may not be within the operator's direct field of viewing.

A plant data logger/computer will be available in the control room for alarm monitoring, performance monitoring, and data logging. On-demand printout is available to the operator at his discretion in addition to the computer periodic logging of plant variables.

7.4.3 SUMMARY OF ALARMS

Visible and audible alarm units will be incorporated into the control room to warn the operator if unsafe conditions are approached by any system. Audible reactor building evacuation alarms are to be initiated from the radiation monitoring system, or manually by the operator. Audible alarms will be sounded in appropriate areas throughout the plant if high radiation conditions are present.

7.4.4 COMMUNICATION

Plant telephone and paging systems will be provided with redundant power supplies to provide the control room operator with constant communication with all

areas of the plant. Acoustical phones will be supplied in areas where the background noise level is high. Battery-powered portable radio equipment will be available in the plant for normal and emergency use. Communication outside the plant will be through the full period leased lines of the telephone company and Met. Ed. Mobile Radio System.

7.4.5 OCCUPANCY

The control room will be designed so that safe occupancy of the control room during abnormal conditions will be assured. Adequate shielding will be used to maintain tolerable radiation levels in the control room for maximum hypothetical accident conditions. The integrated direct dose from all sources of radiation to control room personnel working on 8-hour shifts during a 90-day period following a maximum hypothetical accident will not exceed 3 rem (including ingress and egress), which is approximately the yearly quarter-dose permitted in 10 CFR 20. Gas masks and other protective equipment will be provided for personnel entering or leaving the control room through areas which potentially may have higher radiation levels than the control room. The control room ventilation system will be provided with radiation detectors and appropriate alarms. Provisions will be made for the control room air to be recirculated through absolute and charcoal filters. Emergency lighting will be provided.

The potential magnitude of a fire in the control room will be limited by the following factors:

a. The control room construction will be of noncombustible materials.

b. Control cables and switchboard wiring will be constructed of materials that have passed the flame test as described in Insulated Power Cable Engineers Association Publication S-61-402 and National Electrical Manufacturers Association Publication WC 5-1961.

c. Furniture used in the control room will be of metal construction.

d. Combustible supplies such as logs, records, procedures, manuals, etc., will be limited to the amounts required for plant operations.

e. All areas of the control room will be readily accessible for fire extinguishing.

f. Adequate fire extinguishers will be provided.

g. The control room will be occupied at all times by a qualified person who has been trained in fire extinguishing techniques.

h. Gas masks and protective clothing will be provided.

The only flammable materials inside the control room will be:

a. Paper in the form of logs, records, procedures, manuals, diagrams, etc.

b. The coaxial cables required for nuclear instrumentation.

c. Small amounts of combustible materials used in the manufacture of various electronic equipment.

The flammable materials will be distributed so that a fire would be unlikely to spread. Therefore, a fire, if started, would be of such small magnitude that it could be extinguished by the operator using a hand fire extinguisher. The resulting smoke and vapors would be removed by the ventilation system.

The ventilation system and other connections between the control room and areas of potential fire will be designed to preclude fire or smoke from rendering the control room uninhabitable.

In the unlikely event that abandonment of the control room becomes necessary, the operator will immediately take the following actions after making the decision to evacuate the control room:

a. Before leaving the control room the operator will actuate the reactor scram button and quickly scan the rod group position lights and power range neutron flux level indicators to ascertain that the control rods have been inserted and the neutron flux level has decreased. The turbine-generator will be tripped automatically as a result of this action, and the plant electrical load will be transferred automatically from the unit auxiliary transformer to the startup transformer.

6| b. The operator will perform the following procedures prior to leaving the control room:

(1) Start emergency feedwater pumps.

(2) Trip main feedwater pumps.

(3) Trip reactor coolant pumps.

(4) Trip makeup pumps.

(5) Close the letdown valve.

(6) Close the reactor coolant pump seal return valve.

(7) Close the reactor coolant pump seal injection water valves.

(8) Maintain the pressurizer water level as required by starting the makeup pumps and manually operating the makeup valves and the borated storage tank supply valves.

(9) Steam will be removed from the steam generators by the automatic action of the turbine bypass to the main condenser, and, if heat input to the steam system is sufficiently high after reactor shutdown, by automatic opening of the steam safety valves. In addition to this, steam may be removed to the atmosphere by manual operation of the emergency turbine bypass valves.

Local controls at the motor control centers or switchgear locations will be used to start and trip pumps described in the procedures above.

These controls will be designed to minimize the possibility of unauthorized actuation during normal plant operation, but for reasonable access during emergency conditions. Where possible, the unauthorized operation of these controls will be indicated in the control room.

All valves, described in the procedures above, which will be operated manually, will be equipped with hand operators which override the normal remote controls. The control valves which bypass steam to the main condenser will not be equipped with hand operators because opening of these valves without a proper vacuum in the condenser could cause a rupture of the low-pressure turbine diaphragms.

The following items, which are normally monitored within the control room, will be provided also at locations outside of the control room and in accordance with the locations at which the emergency procedures are to be performed:

a. Pressurizer water level.

b. Reactor coolant outlet temperature.

c. Feedwater pressure.

d. Steam pressure.

e. Steam generator water level.

f. Plant paging system.

It is expected that the required operations in the control room can be executed within one or two minutes and those outside of the control room within ten minutes. If the emergency conditions that cause evacuation of the control room are of a less serious nature, permitting a longer time between the decision to leave and the actual departure, then Steps 1 through 7 as described above may be performed more conveniently within the control room prior to departure. There will be several hours available to place the makeup system in operation.

Although cooldown is not considered necessary to maintain a safe shutdown condition in the event the control room has to be evacuated, the type and extent of instrumentation and control that will be installed outside of the control room will provide this capability, subject to the following conditions and assumptions:

a. No second control room or the equivalent in the form of centralized instrumentation and control equipment will be provided.

b. It is assumed that there is no damage to the instrumentation and control equipment in the vacated control room.

c. No time limit is to be set on the actions taken during the cooldown.

d. Offsite power is available.

7.4.6 AUXILIARY CONTROL STATIONS

Auxiliary control stations will be provided where their use simplifies control of auxiliary systems equipment such as waste evaporator, sample valve selectors, chemical addition, etc. The control functions initiated from local control stations will not directly involve either engineered safety features or reactor

control. Sufficient indicators and alarms will be provided so that the central control room operator is made aware of abnormal conditions involving remote control stations.

7.4.7 SAFETY FEATURES

The primary objectives in the control room layout are to provide the necessary controls to start, operate, and shut down the nuclear unit with sufficient information display and alarm monitoring to insure safe and reliable operation under normal and accident conditions. Special emphasis will be given to maintaining control integrity during accident conditions. The layout of the engineered safety features section of the control board will be designed to minimize the time required for the operator to evaluate the system performance under accident conditions. Any deviations from predetermined conditions will be alarmed so that the operator may take corrective action using the controls provided on the control panel.