U.S. Department of Energy
Washington, D.C.

ORDER

DOE 5480.30

1-19-93
Chg. 1: 3-14-01
Certified: 11-18-10

SUBJECT: NUCLEAR REACTOR SAFETY DESIGN CRITERIA

1. PURPOSE. To establish nuclear safety design criteria applicable to the design, fabrication, construction, testing, and performance requirements of nuclear reactor facilities and safety class structures, systems, and components (SSCs) within these facilities. This Order applies to both new and existing reactor facilities.

2. CANCELLATIONS. Paragraphs 8a and 8b of DOE 5480.6, SAFETY OF DEPARTMENT OF ENERGY-OWNED REACTORS, of 9-23-86.

3. SCOPE. Except for the exclusions in paragraph 3b, the provisions of this Order apply to all Departmental Elements, including the National Nuclear Security Administration (NNSA).

   a. Application to Contracts. Except for the exclusions in 3b, the provisions of this Order are to be applied to covered contractors and the provisions will apply to the extent implemented under a contract or other agreement. A covered contractor is a seller of supplies or services designing, constructing, operating, or decommissioning, a DOE-owned or -leased nuclear facility, exempt from Nuclear Regulatory Commission (NRC) licensing, and awarded a procurement contract, or a subcontract, containing one of four contract clauses as follows: (1) Safety and Health (Government-owned or -leased) facility [DEAR 970.5204-2], (2) Nuclear Facility Safety [DEAR 970.5204-26], (3) Radiation Protection and Nuclear Criticality [DEAR 952.223-72], or (4) another clause whereby DOE elects to require compliance with DOE nuclear safety requirements. All paragraphs of this Order are to be applied to covered contractors except paragraph 7, RESPONSIBILITIES AND AUTHORITIES.

   b. Exclusions. To avoid duplicative or conflicting requirements, DOE facilities, projects and programs that are licensed or subject to regulation by the NRC or an NRC Agreement State shall use the rules, standards and criteria specified by the NRC or NRC Agreement State in lieu of this Order. Also excluded from the provisions of this Order are naval reactor facilities and activities covered under Executive Order 12344.

4. REFERENCES. See Attachment 1. The latest edition of required references shall be used, subject to backfit considerations.

5. DEFINITIONS. See Attachment 2.

Vertical line denotes change.

6. POLICY. It is the policy of the Department of Energy (DOE) that the general public be protected such that no individual bears significant additional risk to health and safety from the operation of a DOE nuclear facility above the risks to which members of the general population are normally exposed. DOE facility workers are to be protected such that the risks to which they are exposed as a result of operating the facility are to be maintained ALARA. Accordingly, DOE nuclear reactor facilities and activities shall be designed, constructed, operated, and decommissioned to assure the protection of the public, workers, and the environment.

7. RESPONSIBILITIES AND AUTHORITIES.

a. The Secretary of Energy (S-1). Many provisions in this Order permit and/or necessitate the exercise of discretion and/or judgement in carrying out the requirements of the Order. In those instances, the determination of whether, in the exercise of such discretion and/or judgement, the requirements of this Order were complied with rests initially with the relevant Department authority and, ultimately, with the Secretary. The Secretary retains the sole and final authority to determine what acts are necessary to comply with this Order. Further, the Secretary retains the authority to suspend any and all requirements under this Order whenever the Secretary deems it necessary. This authority may be delegated by the Secretary as appropriate.

b. Program Secretarial Officers (PSOs) or their designee in the line organization shall:

(1) Require that contractors/operators design and construct nuclear reactor facilities in accordance with the provisions of this Order.

(2) Verify that the safety analysis establishes an adequate safety design basis and evaluates the adequacy of the safety design features of the facility in accordance with the provisions of this Order.

(3) Assure that all commitments made to design features are satisfactorily implemented by the contractors/operators for each nuclear reactor facility.

(4) (a) Approve deviations and temporary (up to one year) exemptions from the requirements of this Order to contractors/operators. Notify appropriate Headquarters-level offices of all temporary exemptions granted.

Vertical line denotes change.

(b) When appropriate recommend that the Secretary grant a permanent exemption from requirements of this Order. A copy of the recommendation should be forwarded to the Assistant Secretary Environment, Safety, and Health, so that the Assistant Secretary may provide advice to the Secretary on the recommendation.

(c) Issue the permanent exemptions approved by the Secretary.

(5) Provide guidance and assistance to field organizations in the performance of reviews, appraisals, etc., to assure contractor compliance with the provisions of this Order.

(6) Conduct appraisals to assure contractor compliance with this Order.

(7) Transmit the results of the actions taken above to the responsible program managers and field organizations with any necessary or appropriate instructions as to subsequent action to be taken, with copies to the Assistant Secretary for Environment, Safety and Health.

c. DOE Field Office Managers or Field Program Managers shall:

(1) Review, and make recommendations to the PSO relative to the approval of, all safety analyses and evaluations of the design basis.

(2) Oversee contractor/operator preparation and review of safety analyses and evaluations of design features including establishing pertinent design criteria as directed by the PSO.

(3) Conduct appraisals to assure contractor compliance with this Order.

(4) Keep appropriate Headquarters program organizations, the Assistant Secretary for Environment, Safety and Health (EH-1), and the field and area offices advised of safety issues, deficiencies, needs and actions taken under this Order.

(5) Heads of Headquarters Elements and heads of field organizations (the senior ranking DOE official at a DOE office location) shall include in a procurement request

Vertical line denotes change.

package, for each procurement requiring the application of this Directive, the following:

(a) Identification of the Directive.

(b) Identification of the specific requirements with which a contractor or other awardee is to comply, or, if this is not practicable, identification of the specific paragraphs or other portions of this Directive with which a contractor or other awardee is to comply.

(c) Requirements for the flowdown of provisions of this Directive to any subcontract or subaward.

For application to awarded management and operating contracts, Heads of Headquarters Elements and heads of field organizations may set forth this information in a written communication to the contracting officer rather than in a procurement request package.

d. Assistant Secretary for Environment, Safety and Health (EH-1), acting as the independent element responsible for safety aspects relative to public and worker health and safety, environmental protection, and independent oversight of line management for the Department, shall:

(1) Develop and maintain the policy, requirements, guidance, and, technical standards, and provide advice and assistance, as requested, concerning implementation of nuclear safety policy as it relates to the application of this Order to the design of nuclear reactor facilities;

(2) Monitor and review the implementation of all aspects of this Order, including field organization and contractor performance;

(3) Review or designate responsibility for the review of documentation such as Technical Safety Appraisals, Safety Analyses, Hazard Evaluations, implementation schedules, headquarters/field office reports, and observe on-site activities;

Vertical line denotes change.

(4) Identify circumstances that are indicative of deteriorating or poor performance that may warrant further action;

(5) Provide recommendations on requests for permanent exemptions from the requirements of this Order, as requested by the PSO or directed by the Secretary; and

(6) Provide enforcement policy and programs associated with the civil and criminal authority of the Price-Anderson Amendments Act.

Vertical line denotes change.

8. REQUIREMENTS.

a. These Nuclear Safety Design Criteria (NSDC) establish requirements for the design of all safety class structures, systems and components of DOE nuclear reactor facilities. Each covered DOE contractor shall use these criteria in the review and development of existing and proposed directives, plans, or procedures relating to the design of new and existing DOE nuclear reactor facilities. Attachment 3 provides guidance to help implement the nuclear safety design criteria of this order.

b. The criteria provided here are not necessarily complete. There may be some facilities for which additional nuclear safety design criteria must be satisfied in the interest of worker and public safety. There are some criteria that do not relate to the design of the reactor but are, nonetheless important to the safety of the facility. Such criteria would include: emergency planning for the facility, the development of symptom based emergency procedures, the analysis and evaluation of emergency core cooling systems, and reactor vessel material surveillance. These items are required to be included in the Safety Analysis Reports by DOE 5480.23 and will be the subject of future DOE documentation. Furthermore, there are some reactor concepts (such as liquid metal reactors and modular high temperature gas reactors) that require unique design criteria. Some implementation guidance for specific design criteria for such facilities are discussed in Attachment 3, paragragh 3, “Implementation Guidance.” However, not all of the design criteria may be necessary or appropriate for a specific facility. For example, some test and research reactors may not require the same degree of containment as are required by the NRC for commercial power reactors. A DOE contractor responsible for such reactors must identify the unique criteria or deviations and include them in the design and operation of such a facility after obtaining DOE approval.

This order applies to all varieties of reactors including, but not limited to: light water moderated reactors, heavy water moderated reactors, liquid metal cooled reactors, gas cooled reactors and short-pulse transient reactors. Space reactor power and propulsion systems and critical facilities require special design criteria. Attachment 4 is reserved for Nuclear Safety Design for critical facilities and space reactors.

A graded approach shall be uses in the application of these nuclear safety design criteria to ensure that the depth of detail required and the magnitude of resources expended for the design are commensurate with each facility’s programmatic importance and the potential environmental, safety, and/or health impact of normal operations,

anticipated operational events (AOEs), and design basis accidents (DBAs) .

c. General Design Requirements.

The overall design philosophy to achieve the highest level of reactor safety is to provide "defense-in depth." The principle of defense-in-depth includes: the use of conservative design margins and quality assurance; the use of successive physical barriers for protection against the release of radioactivity; the provision of multiple means to ensure the primary safety functions (reactor shutdown, heat removal, and fission product confinement); the use of equipment and administrative controls which restrict deviations from normal operation and provide for recovery from anticipated events or accidents; and the provision of emergency plans for minimizing the effects of a reactor accident. In addition to defense in depth, the design shall meet OSHA safety and health requirements.

The design of safety class structures, systems and components (SSCs) shall provide defense-in-depth features against the uncontrolled release of radioactive materials to the environment under normal conditions, AOEs, and DBA conditions.

The design features of each DOE nuclear reactor facility shall meet the following requirements.

(1) Single Failure. Safety class SSCs shall be able to accommodate a single failure and still meet their intended safety function, as required, to ensure compliance with the facility acceptance criterion. A "single failure" means an occurrence which results in the loss of capability of a safety class structure, system or component to accomplish its required safety functions. Multiple failures resulting from a single occurrence are considered to be a single failure.

Fluid and electrical systems are considered to be designed against an assumed single failure if neither:

1) A single failure of any active component (assuming passive components function properly) nor

2) A single failure of a passive component (assuming active components function properly),

results in a loss of the capability of the system to perform its safety functions.

Single failures of passive components in electric systems should be assumed in designing against a single failure. A single failure of a passive component in other systems and structures should be considered as required.

(2) Quality Standards. Safety class structures, systems, and components shall be designed, fabricated, erected, and tested to quality standards commensurate with the importance of the safety functions to be performed.

Where generally recognized codes and standards are used, they shall be identified and evaluated to determine their applicability, adequacy, and sufficiency and shall be supplemented or modified as necessary to ensure a quality product in keeping with the required safety function.

A quality assurance program, consistent with DOE standards, including DOE 5700.6C shall be implemented.

(3) Design Basis for Protection Against Natural Phenomena. The natural phenomena hazard design basis for safety class SSCs shall reflect the importance of the safety functions to be performed and the requirements set forth in DOE 5480.28.

(4) Fire Protection. The probability and effect of fires, explosions, and related perils at DOE facilities shall be minimized. Safety class structures, systems, and components shall be designed and located to minimize, consistent with other safety requirements, the probability and effect of fires and explosions. Noncombustible and heat resistant materials shall be used whenever practical throughout the unit, particularly in areas vital to the control of hazardous materials and maintenance of safety functions. Fire detection and fighting systems shall be designed and provided with sufficient capacity and capability to minimize the adverse effects of fires and explosion on safety class structures, systems, and components.

Firefighting systems shall be designed to ensure that their rupture or operation does not significantly impair the safety capability of these structures, systems, and components.

Current requirements for fire protection programs are provided in DOE 5480.7.

(5) Environmental Effects Design Bases. The facility shall meet the requirements set forth in DOE 5480.27.

(6) Sharing of Structures, Systems, and Components. Safety class structures, systems, and components shall not be shared among nuclear facilities unless it can be shown that such sharing will not impair their ability to perform their safety functions, including, in the event of an accident in one nuclear facility, an orderly shutdown and cooldown of the remaining nuclear reactor facilities.

(7) Siting. Nuclear reactors are to be sited in a manner that gives adequate protection for health and safety of the public and on-site workers and co-located workers at adjacent facilities in accordance with uniform standards, guides, and codes which are consistent with those applied to comparable licensed nuclear facilities and the non-nuclear industry. A DOE facility located near other facilities shall be designed to ensure that the cumulative effects of their combined operations will not constitute an unacceptable risk to health and safety of workers and the public. Specific site evaluation criteria are provided in DOE N 5480.6 (Article 128), DOE 5400.5, DOE 5480.6, and DOE 5480.28.

(8) Containment and Confinement Barriers. For large Category A reactors (see Attachment 3), a reactor containment and associated systems shall be provided to establish a barrier against uncontrolled release of radioactive materials to the environment and ensure that the containment design conditions do not exceed design limits for as long as postulated accident conditions require.

For those DOE reactors that require a containment, the containment design shall meet the requirements of 10 CFR Part 50, Appendix A, criteria 50 through 57 along with the containment heat removal and atmospheric cleanup criteria (38 through 43).

For reactor facilities which do not require a containment, confinement barriers and associated systems shall provide defense against the uncontrolled release of radioactive materials to the environment under normal conditions, AOEs, and DBAs.

(9) Human Factors Engineering (HIE). HFE shall be considered per DOE 5480.23 in the design of nuclear reactors or nuclear reactor systems that have a human interface for operating or maintenance. The formality and the extent of the HFE program shall be graded on the basis of the extent of the human interaction, the overall design effort, and the risk associated with human performance failures.

(10) Dynamics Effects Design Bases. Safety class structures, systems, and components shall be designed such that they are protected against dynamic effects, including the effects of postulated pipe ruptures, missiles, pipe whipping (applicable for high energy pipe systems), and discharging fluids, that may result from equipment failures and from events and conditions outside the nuclear reactor facility.

Pipe Whip and Discharge of Fluid associated with postulated pipe ruptures may be excluded from the design basis when it can be demonstrated that:

(a) The probability of fluid system pipe rupture is extremely low, or

(b) The fluid system energy is sufficiently low to preclude pipe whip and high pressure jets, under conditions consistent with the design basis for the piping.

(11) Safeguards and Security. The design basis of the facility shall reflect the basic requirements of DOE 5632 series, DOE 5633 series, and DOE 5630.11.

To the extent practical, safety class SSCs shall be designed to impede radiological material sabotage, indicate timely indication of such attempted sabotage and facilitate damage control and consequence mitigation. The facility design shall include features to protect the health and safety of workers and the public while minimizing the impact on safeguards and security.

(12) Effluent and Emission Control

(a) Control of Releases of Hazardous Materials to the Environment. The nuclear reactor design shall include means to control the release of radioactive materials in gaseous and liquid effluent and to handle radioactive solid wastes produced during normal reactor operation, including AOEs.

Sufficient holdup capacity shall be provided for retention of gaseous and liquid effluent containing radioactive materials, particularly where unfavorable site environmental conditions can be expected to impose unusual operational limitations upon the release of such effluent to the environment. In addition, radioactive effluents shall meet the provisions of the National Environmental Policy Act as required in DOE 5400.1.

The design shall limit the release of radioactive materials in effluents and emissions to ALARA levels during normal operation; and control the release of radioactive materials under accident conditions so that Rad Con Manual limits are not exceeded.

Means for measuring the amount of radionuclides in effluents and emissions during normal operation and accident conditions shall be provided. Systems designed to monitor the release of radioactive materials shall have means for calibration and testing their operability.

There shall be no interconnections between liquid effluent streams such as streams containing radioactive and/or hazardous waste, potable water streams, other incoming non-potable streams, and other outgoing streams.

(b) Monitoring Hazardous Materials. Means shall be provided for monitoring the reactor compartment, reactor building, and plant environs for radioactivity that may be released from normal operations, including AOEs, and from postulated accidents.

Alarms shall be provided that will annunciate in the event that radioactivity levels above specified limits are detected in the exhaust stream. Appropriate manual or automatic protective features that prevent the uncontrolled release of radioactive material to the environment or workplace shall be provided.

(13) Reactor Decontamination and Decommissioning. Design of the areas to which access is required in the reactor facility that may become contaminated with radioactive materials under normal or abnormal operating conditions shall incorporate measures to simplify decontamination and to facilitate decontamination for future decommissioning.

(14) Waste Management. The facility's radioactive waste management systems shall include equipment necessary to collect, store, sample, and treat gaseous, liquid, or solid radioactive material and prepare them for reuse or disposal.

Radioactive waste systems shall include monitoring and control equipment necessary to ensure that radioactive exposures resulting from normal system operation and releases from the system are maintained ALARA in accordance with DOE 5480.11.

Volume reduction equipment for both liquid and solid wastes shall be required where feasible and shall be designed for process capability and capacity commensurate with the types and quantities of wastes expected.

(15) Support Systems. Support systems (e.g., electrical power, cooling) required to ensure that safety class structures, systems and components can provide their required safety function shall also be considered safety class systems.

(16) Non-Safety Class Structures, Systems, and Components. Safety class structures, systems, or components shall not be prevented from performing their required safety functions by the failure of non-safety class structures, systems and components.

d. Specific Design Requirements

(1) Reactor Coolant Boundary.

(a) Reactor Coolant Boundary Integrity. The reactor coolant boundary shall be designed, fabricated, erected, and tested so as to have an extremely low probability of abnormal leakage, rapidly propagating failure, and gross rupture.

(b) Quality of Reactor Coolant Boundary. Components that are part of the reactor coolant boundary shall be designed, fabricated, erected, and tested to the highest quality standards practical. Means shall be provided for detecting and, to the extent practical, identifying the location of the source of reactor coolant leakage.

(c) Fracture Prevention. The reactor coolant boundary shall be designed with sufficient margin to ensure than when stressed under operating, maintenance, testing, and postulated accident conditions, the boundary behaves in a nonbrittle manner, and the probability of rapidly propagating fracture is minimized.

The design process shall consider service temperatures, unacceptable thermal stress due to rapid thermal cycles, and other conditions of the boundary material under normal operation, maintenance, testing, and postulated accident conditions and uncertainties in determining:

1 Material properties;

2 The effects of irradiation on material properties;

3 Residual, steady state, and transient stress; and

4 Flaw size, including orientation, number, location, and grouping pattern.

Where applicable, adequate fluid chemistry control must be established to ensure against erosion, corrosion, inter-granular stress corrosion cracking, (IGSCC), trans-granular stress corrosion cracking (TGSCC) in sensitized metals, fuel cladding failures, contamination and potential degradation of reactor core internals.

(d) Inspection. Components which are part of the reactor coolant boundary shall be designed to permit:

1 Periodic inspection and testing of important areas and features to assess their structural and leaktight integrity, and

2 An appropriate material surveillance program for the reactor vessel.

(2) Electric Power Systems.

(a) Electric Power Systems Design. An on-site electric power system and an off-site electric power system shall be provided to permit functioning of safety class structures, systems, and components. The safety function for each system (assuming the other system is not functioning) shall be to provide sufficient capacity and capability to ensure that (1) specified acceptable design limits and design conditions of the reactor coolant pressure boundary are not exceeded as a result of AOEs and (2) the core is cooled and containment integrity and other vital functions are maintained in the event of postulated accidents.

The on-site electric power supplies, including the batteries, and the on-site electric distribution system, shall have sufficient independence, redundancy, and testability to perform their safety functions assuming a single failure.

Provisions shall be included to minimize the probability of losing electric power from any of the remaining supplies as a result of or coincident with the loss of power from the transmission network, or the loss of power from the on-site electric power supplies. The potential for loss of all

sources of AC power due to the effects of natural phenomenon shall be analyzed in accordance with DOE 5480.28.

(b) Inspection and Testing. Safety class electric power systems shall be designed to permit appropriate periodic inspection and testing of important areas and features such as wiring, insulation connections, and switchboards to assess the continuity of the systems and the condition of their components. The systems shall be designed with a capability to test periodically:

1 The operability and functional performance of the components of the systems, such as on-site power sources, relays, switches, and buses; and

2 The operability of the systems as a whole and, under conditions as close to design as practical, the full operation sequence that brings the systems into operation, including operation of applicable portions of the protection system and the transfer of power between the offsite power system and the on-site power system.

(3) Reactor Core.

(a) Reactor Core Design. The reactor core and associated coolant, control, and protection systems shall be designed with appropriate margin to ensure that acceptable design limits are not exceeded during any condition of normal operation, including the effects of AOEs.

(b) Reactor Inherent Protection. The reactor core and associated coolant system shall be designed so that in the anticipated power operating range the net effect of the prompt inherent nuclear feedback characteristics provides an acceptable level of compensation for a rapid increase in reactivity.

(c) Suppression of Reactor Power Oscillations. The reactor core and associated coolant, control, and protection systems shall be designed to ensure that power oscillations and power distributions which can result in conditions exceeding specified acceptable design limits are not possible or can be reliably and readily detected and suppressed.

(4) Protection Systems.

(a) Protection System Functions. The protection system shall be designed for high functional reliability with the capability to:

1 Initiate automatically the operation of appropriate systems including the reactivity control systems, to ensure that specified acceptable design limits are not exceeded as a result of AOEs; and

2 Sense accident conditions and to initiate the operation of protection systems.

The system shall be designed to permit periodic appropriate inspection and testing.

(b) Protection System Independence. The protection system shall be designed to ensure that the effects of normal operations, AOEs, maintenance, testing, and DBAs on redundant channels do not result in loss of the protection function. Design techniques, such as redundancy, physical separation, functional diversity, or diversity in component design and principles of operation, shall be used to prevent loss of the protection function. The protection shall be sufficient to ensure no single failure results in loss of protection and capability exists to test channels independently to determine failures and loss of redundancy.

(c) Protection System Failure Modes. The protection system shall be designed to fail into a safe state or into a state demonstrated to be acceptable on some other defined basis if conditions such as faults, disconnection of the system, loss of energy, or postulated adverse environments are experienced.

(d) 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 system 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 ensure that safety is not significantly impaired.

(e) Protection System Requirements for Reactivity Control Malfunctions. The protection system shall be designed to ensure that specified acceptable design limits are not exceeded for any single malfunction of the reactivity control systems.

(f) Protection Against Anticipated Operational Occurrences. The protection and reactivity control systems shall be designed to ensure an extremely high probability of accomplishing their safety functions in the event of AOEs.

(5) Instrumentation and Control Systems.

(a) Instrumentation and Control. Instrumentation shall be provided to monitor variables and system performance over their anticipated ranges for normal operation, AOEs, and DBAs as appropriate to ensure adequate safety, including those variables and systems that can affect the fission process, the integrity of the reactor core, and the reactor coolant boundary and if applicable, the containment and its associated systems

Appropriate controls shall be provided to maintain these variables and the performance of these systems within prescribed operating ranges.

(b) Reactivity Control System Redundancy and Capability. Two independent reactivity control systems of different design shall be provided. One of the systems shall be capable of reliably controlling reactivity changes to ensure that under conditions of normal operation, including AOEs, and with appropriate margin for malfunctions such as stuck rods, specified acceptable design limits are not exceeded.

The second reactivity control system shall be capable of reliably controlling the rate of reactivity changes resulting from planned, normal power changes (including xenon burnout) to ensure acceptable design limits are not exceeded. One of the systems shall be capable of holding the reactor core subcritical under cold conditions.

(c) Combined Reactivity Control Systems Capability. The reactivity control systems shall be designed to have a combined capability to ensure that under DBA conditions excess reactivity noes not cause acceptable design limits to be exceeded and that the reactor core is subcritical with appropriate margin.

(d) Reactivity Limits. The reactivity control systems shall be designed with appropriate limits on the potential amount and rate of reactivity increase to ensure that the effects of postulated reactivity accidents can neither (1) result in damage to the reactor coolant pressure boundary greater than limited local yielding nor (2) sufficiently disturb the core, its support structure or other reactor pressure vessel internals to impair significantly the capability to cool the core.

(e) Control Room. A control room or control area shall be provided from which actions can be taken to operate the nuclear reactor safely under normal conditions and to maintain it in a safe condition during AOEs and DBAs including ensuring protection against toxic gases. Adequate radiation protection shall be provided to ensure access and occupancy of the control room or control area under accident conditions without personnel receiving radiation exposures in excess of the Rad Con Manual limits.

(f) Remote Shutdown. Based on the nuclear reactor safety analysis, the design shall provide equipment at appropriate locations outside the control room that is capable of promptly shutting down the reactor, including necessary instrumentation and controls to maintain the unit in a safe condition during shutdown.

(6) Heat Removal Systems and Ultimate Heat Sink.

(a) Heat Removal Systems. The reactor heat removal system and associated auxiliary, control, and protection systems shall be designed with sufficient margin to ensure that the design conditions of the reactor coolant pressure boundary are not exceeded during any condition of normal operation, nor any AOEs.

(b) Residual Heat Removal. A system to remove residual heat shall be provided. The system safety function shall be to transfer fission product decay heat and other residual heat from the reactor core at a rate such that specified acceptable design limits and the design conditions of the reactor coolant pressure boundary are not exceeded.

Suitable redundancy in components and features, and suitable interconnections, leak detection, and isolation capabilities shall be provided to ensure that for on-site electric power system operation (assuming offsite power is not available) and for offsite electric power system operation (assuming

onsite power is not available) the system safety function can be accomplished, assuming a single failure.

(c) Reactor Coolant Makeup. A system to supply reactor coolant makeup for protection against small breaks in the reactor coolant boundary shall be provided. The system safety functions shall ensure that specified acceptable design limits are not exceeded as a result of reactor coolant loss due to leakage from the reactor coolant pressure boundary and rupture of small piping or other small components which are part of the boundary. The system shall be designed to ensure that for on-site electric power system operation (assuming off-site power is not available) and for off-site electric power system operation (assuming on-site power is not available) the system safety function can be accomplished using the piping, pumps, and valves used to maintain coolant inventory during normal reactor operation.

(d) Emergency Core Cooling. If required, a system to provide emergency core cooling shall be provided such that the decay heat removal capability is not compromised. The system safety function shall be to transfer heat from the reactor core following any loss of reactor coolant such that specified acceptable design limits are not exceeded including clad-metal-coolant reactions.

The system shall be designed to permit appropriate periodic inspection and testing to ensure the structural integrity of its components and the capability and performance of the active components of the system and the operability of the system as a whole.

Suitable redundancy in components and features, and suitable interconnections, leak detection, isolation, and containment capabilities shall be provided to ensure that for on-site electric power system operation (assuming off-site power is not available) and for off-site electric power system operation (assuming on-site power is not available) the system safety function can be accomplished, assuming a single failure.

(e) Cooling System. If required to maintain its safety function, a system to transfer heat from safety class structures, systems, and components to an ultimate heat sink shall be provided. The system safety function shall be to transfer the combined heat load of these structures, systems, and components under normal operation, AOEs and DBAs.

The system shall be designed to permit appropriate periodic inspection and testing to ensure the structural integrity of its components and the capability and performance of the active components of the system and the operability of the system as a whole.

Suitable redundancy in components and features, and suitable interconnections, leak detection, and isolation capabilities shall be provided to ensure that for on-site electric power system operation (assuming off-site power is not available) and for off-site electric power system operation (assuming on-site power is not available) the system safety function can be accomplished, assuming a single failure.

(7) Heating, Ventilation, and Air Conditioning (HVAC) Systems.

(a) Airflow. In order to minimize the spread of contamination to the environment, ventilation systems shall be designed to provide a continuous airflow pattern from the environment into the building and then from noncontaminated areas to potentially contaminated areas and then to normally contaminated areas.

(b) Equipment Reliability. Equipment in ventilation and off-gas systems shall be appropriately qualified to ensure reliable operation during normal operating conditions, AOEs, and DBAs.

(c) Air Cleanup Systems. Safety class air cleanup systems shall be designed to withstand a single failure without loss of systems functions and to remain functional throughout DBAs and to retain collected hazardous material after the accident. The design should accommodate safe removal of any collected hazardous waste.

(8) Fuel Handling and Storage and Radioactive Waste Storage.

(a) Fuel and Radioactive Waste Storage. The fuel storage and handling and radioactive waste system shall be designed to ensure adequate safety under normal operations, AOEs and DBAs. These systems shall be designed:

1 With a capability to permit appropriate periodic inspection and testing of components;

2 With suitable shielding for radiation protection; and

3 With appropriate containment, confinement, and filtering systems.

(b) Prevention of Criticality in Fuel Storage and Handling. Criticality in the fuel storage and handling system shall be prevented by physical systems or processes to maintain adequate subcriticality at all times. The preferred order to maintain subcriticality is favorable geometry, other passive engineered safety features then active engineered safety features.

The facility design basis shall reflect the requirements of DOE 5480.24.

(c) Monitoring of Fuel and Radioactive Waste Storage. Appropriate systems shall be provided in fuel storage areas, 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.

(d) Fuel Storage and Handling Systems Heat Removal Capability. The fuel storage and radioactive waste storage systems shall be provided with systems to protect coolant inventory and remove residual heat under normal operation, AOEs and DBAs with a high degree of reliability.

9. IMPLEMENTATION.

a. New DOE Nuclear Reactor Facilities. For new nuclear reactor facilities, all safety class structures, systems, and components (SSCs) shall be designed, fabricated, erected, and tested in accordance with the provisions of this Order.

b. Existing DOE Nuclear Reactor Facilities. For DOE nuclear reactor facilities, the Upgraded Safety Analysis Report (SAR) prepared per DOE 5480.23 shall serve to establish and evaluate the adequacy of the safety bases for existing facilities. Attachment 1, paragraph 4f(9) of DOE 5480.23 provides guidance on the development of safety bases for existing nuclear facilities. Approval of the upgraded SARs by the Program Secretarial Officer (PSO) shall be based on Safety Evaluation Reports (SERs) that document the safety bases. The safety bases in the upgraded SAR shall demonstrate that the appropriate provisions of this order are compared and evaluated against the original/current safety design bases. The need for any modifications to the facility

design, or operations, resulting from the comparison and evaluation shall be subject to paragraph 9c.

c. Modifications. Modifications to Safety class systems, structures, and components in existing facilities, or changes to the operations, to comply with the requirements of this Order shall be considered in accordance with Attachment 1, paragraph 4f(9) of DOE 5480.23. This provision in DOE 5480.23 will be supplemented by using the procedures provided in DOE N 5480.5, IMPOSITION OF PROPOSED NUCLEAR SAFETY REQUIREMENTS, This process should ensure cost effective modifications that maximize the safety benefit while avoiding unnecessary or unproductive expense in retrofitting existing facilities.

d. Unreviewed Safety Questions. For "Unreviewed Safety Questions" pursuant to DOE 5480.21; paragraph 9c of DOE 5480.23 and paragraph 4f(11) of the Attachment to DOE 5480.23 address the updating of SARs that are necessary to keep the SAR current. As discussed above, SAR updates are distinct from SAR upgrades that refer to changes that must be made in SARs to bring them into compliance with this Order.

e. Schedule. This order becomes effective immediately; however, the implementation of the requirements of this order will be coordinated with the next scheduled update of the facility SAR per the requirements of DOE 5480.23 (paragraph 9c).

10. CRITERIA EXEMPTIONS/DEVIATIONS. Nothing in these criteria shall preempt the specific requirements contained in other DOE directives relative to their processes and procedures for requesting exemptions or deviations.

Exemptions and deviations must be issued in writing and must include an adequate basis justifying the action. Exemptions and deviations from these criteria shall be documented.

a. Exemptions. Review and concurrence by Headquarters-level offices as specified in paragraph 7 of this Order are required for permanent exemptions from the requirements of this Order. PSOs may grant temporary exemptions from this Order with notification of appropriate Headquarters-level offices. Temporary exemptions may be granted for durations up to one year, while permanent exemptions apply for the life of a facility. Exemptions are applicable when any of the following apply:

(1) Exceptions proposed for safety class structures, systems, and components, when such exception will or may constitute an adverse impact on environmental protection, safety or health or other DOE design policies or objectives.

(2) Exceptions from requirements in Federal laws or regulations or Executive Orders; such exceptions cannot be approved unless such laws, regulations, or Executive Orders provide for deviations or waivers.

b. Deviations. Deviations may be granted by the PSO responsible for facility projects or for the design of facilities when any of the following apply:

(1) It has been demonstrated that the exception is equivalent to, or more conservative than, the requirements such that the risk to the health and safety of the public and workers is not affected by the exception.

(2) A specific portion of the design criteria is determined to be inadequate or inappropriate for the facility under design.

(3) Minor exceptions are necessary or advantageous in the designer's professional judgment.

(4) A criterion does not reflect currently applicable codes, standards, regulations, or architectural or engineering principles and practices.

(5) A criterion affecting environmental protection or health and safety is less stringent than local or State codes or regulations

(6) Exceptions will not affect DOE design policy and objectives and are determined to be necessary in the acquisition of buildings by lease or purchase.

(7) Exceptions will not affect DOE design policy and objectives, are necessary, and are allowable under existing exemption provisions of another DOE directive.

LINDA G. STUNTZ
Acting Secretary of Energy

ATTACHMENT 1

REFERENCES

1. DOE SEN-35-91, Secretary of Energy Notice (SEN) titled "Nuclear Energy Policy."

2. DOE N 5480.5, IMPOSITION OF PROPOSED NUCLEAR SAFETY REQUIREMENTS, which establishes procedures for imposing proposed nuclear safety requirements.

3. DOE N 5480.6, RADIOLOGICAL CONTROL MANUAL

4. DOE 4300. 1B, REAL PROPERTY AND SITE DEVELOPMENT, which establishes DOE policies and procedures for the acquisitions, use, inventory, and disposal of real property.

5. DOE 5400.1, GENERAL ENVIRONMENTAL PROTECTION PROGRAM, which establishes environmental protection program requirements, authorities, and responsibilities for DOE operations.

6. DOE 5400.2A, ENVIRONMENTAL COMPLIANCE ISSUE COORDINATION, which sets forth policy, direction, and procedures for coordinating environmental issues that are of significance to DOE.

7. DOE 5400.5, RADIATION PROTECTION OF THE PUBLIC AND THE ENVIRONMENT, which establishes radiation protection standards and program requirements to protect the public and the environment from ionizing radiation.

8. DOE 5480.1B, ENVIRONMENT, SAFETY, AND HEALTH PROGRAM FOR DEPARTMENT OF ENERGY OPERATIONS, which sets forth the responsibilities and requirements for an ES&H program.

9. DOE 5480.4, ENVIRONMENTAL PROTECTION, SAFETY, AND HEALTH PROTECTION STANDARDS, which specifies the application of mandatory ES&H standards to DOE operations.

10. DOE 5480.6, SAFETY OF DOE-OWNED NUCLEAR REACTORS, which establishes reactor safety program requirements.

11. DOE 5480.7, FIRE PROTECTION, which establishes requirements for a comprehensive fire protection program sufficient to attain DOE objectives.

12. DOE 5480.10, CONTRACTOR INDUSTRIAL HYGIENE PROGRAM, which establishes the requirements and guidelines for DOE contractor's industrial hygiene programs.

13. DOE 5480.11, RADIATION PROTECTION FOR OCCUPATIONAL WORKERS, which establishes radiation protection standards and program requirements to protect workers from ionizing radiation.

14. DOE 5480.18A, ACCREDITATION OF PERFORMANCE BASED TRAINING FOR CATEGORY A REACTORS AND NUCLEAR FACILITIES.

15. DOE 5480.19, CONDUCT OF OPERATIONS REQUIREMENTS FOR DOE FACILITIES.

16. DOE 5480.20, PERSONNEL SELECTION, QUALIFICATION, TRAINING AND STAFFING REQUIREMENTS AT DOE REACTOR AND NONREACTOR NUCLEAR FACILITIES.

17. DOE 5480.21, UNREVIEWED SAFETY QUESTIONS, which gives the basis for determining the existence of an Unreviewed Safety Questions.

18. DOE 5480.22, TECHNICAL SAFETY REQUIREMENTS

19. DOE 5480.23, NUCLEAR SAFETY ANALYSIS REPORTS, which establishes the requirement for the safety analysis report for DOE-owned nuclear facilities.

20. DOE 5480.24, NUCLEAR CRITICALITY SAFETY, which establishes nuclear criticality safety program requirements for Department of Energy (DOE) nuclear facilities.

21. DOE 5480.27, EQUIPMENT QUALIFICATIONS (EQ) FOR NUCLEAR FACILITIES AND OPERATIONS 1-15-93, which establishes the environmental conditions under which equipment must perform their safety function during normal operations, anticipated operational occurrences, and DBAs they are required to operate during and after.

22. DOE 5480.28, NATURAL PHENOMENA HAZARDS MITIGATION, OF 1-15-93, which establishes natural phenomena design requirements for Department of Energy facilities.

23. DOE 5610.10, NUCLEAR EXPLOSIVE AND WEAPON SAFETY PROGRAM, establishes DOE policy, objectives, standards and criteria, authorities and responsibilities for its Nuclear Explosive and Weapon Safety Program.

24. DOE 5630.3, PROTECTION of DEPARTMENT FACILITIES AGAINST RADIOLOGICAL and TOXICOLOGICAL SABOTAGE, of 6-30-92, which establishes interim DOE policy and implementing instructions for performing graded assessments of radiological and toxicological sabotage vulnerability at DOE facilities. The two additional references will be included.

25. DOE 5630.11, SAFEGUARDS AND SECURITY PROGRAM, of 1-22-88 which established policy and procedures for the DOE Safeguards and Security Program.

26. DOE 5700.6C, QUALITY ASSURANCE, which establishes the Departmental Quality Assurance requirements.

27. DOE 6430.1A, GENERAL DESIGN CRITERIA, which provides useful practices and guidance for design of non-reactor facilities.

28. Code of Federal Regulations, Title 10, Part 50, Section 50.55a, “Codes and Standards” and Section 50.2.

29. Code of Federal Regulations, Title 10, Part 50, Section 50.60, “Acceptance Criteria for Fracture Prevention Measures for Normal Operation” and Section 50.61, “Fracture Toughness Requirements for Protection Against Pressurized Thermal Shock.”

30. Code of Federal Regulations, Title 10, Part 50, Appendix A, “General Design Criteria for Nuclear Power Plants, ” which establishes minimum general design criteria for NRC licensed light water nuclear power plants.

31. Code of Federal Regulations, Title 10, Part 50, Appendix G, “Fracture Toughness Requirements.”

32. Code of Federal Regulations, Title 10, Part 50, Appendix H, “Reactor Vessel Material Surveillance Program Requirements.”

33. Code of Federal Regulations, Title 10, Part 50, Appendix J, “Primary Reactor Containment Leakage Testing for Water-Cooled Power Reactors.”

34. Code of Federal Regulations, Title 10, Part 50, Appendix K, “ECCS Evaluation Models. ”

35. Code of Federal Regulations, Title 10, Part 100, “Reactor Site Criteria,”

36. Code of Federal Regulations,Title 10, Part 100, Appendix A, “Seismic and Geologic Siting Criteria for Nuclear Power Plants.”

37. Code of Federal Regulations,Title 29, Part 1910, OCCUPATIONAL SAFETY AND HEALTH STANDARDS.

38. NUREG-0800, "Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants, June 1987.

39. NUREG-0800, "Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants," Chapter 7.1, which, when combined with IEEE-603, establishes NRC requirements for instrumentation and control systems important to safety.

40. NUREG/CR-3587, "Identification and Evaluation of Facilitation Techniques for Decommissioning Light Water Power Reactors."

41. NUREG/CR-4618, "Evaluation of Reliability Technology Applicable to LWR, Operational Safety," August 1988, M.A. Azarm and E.V. Wilgren, BNL.

42. NRC Regulatory Guide 1.26, "Quality Group Classifications and Standards for Water-, Steam-, and Radioactive Waste-Containing Components of Nuclear Power Plants."

43. NRC Regulatory Guide 1.47, "Inservice Inspection Code Case Acceptability ASME Section XI Division 1."

44. NRC Regulatory Guide 1.52, "Design Testing and Maintenance Criteria for Post Accident Engineered-Safety-Feature Atmosphere Cleanup System Air Filtration and Adsorption Units of Light-Water-Cooled Nuclear Power Plants."

45. NRC Regulatory Guide 1.75, "Physical Independence of Electric Systems."

46. NRC Regulatory Guide 1.97, "Instrumentation for Light-Water-Cooled Nuclear Power Plants to Assess Plants and Environs Conditions During and Following an Accident."

47. USNRC Branch Technical Position ASB 9-2, "Residual Decay Energy for Light-Water Reactors for Long Term Cooling," USNRC 1981.

48. SECY-89-013, January 19, 1989, Design Requirements Related to the Evolutionary Advanced Light Water Reactors (ALWR).

49. ANSI/ANS-8.1-1983, "American National Criticality Safety in Operation with Fissionable Materials Outside Reactors."

50. ANSI/ANS-54.2-1985, "Design Bases for Facilities for LMFBR Spent Fuel Storage in Liquid Metal Outside the Primary Coolant Boundary."

51. ANSI/ANS-57.2-1983, “Design Requirements for Light Water Reactor Spent Fuel Storage Facilities at Nuclear Power Plants.”

52. ANSI/ANS-57.3-1983,"Design Requirements for New Fuel Storage Facilities at Light Water Reactor Plants.”

53. ASME Boiler and Pressure Vessel Code, Section XI.

54. IEC 964 Standard, “Design for Control Rooms of Nuclear Power Plants.”

55. IEEE 308, “Standard Criteria for Class 1E Power System for Nuclear Power Generating Stations.”

56. IEEE 323, “Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations.”

57. IEEE 353-1975, “Guide for General Principle of Reliability Analysis of Nuclear Power Generating Station Protection Systems.”

58. IEEE 379, “Standard Application of the Single Failure Criterion to Nuclear Power Generating Station Class 1E Systems.”

59. IEEE 384, “Standard Criteria for Independence of Class 1E Equipment and Circuits."

60. IEEE 603, “Standard Criteria for Safety Systems for Nuclear Power Generating Stations.”

61. IEEE 1023, “Guide for the Application of Human Factors Engineering to Systems, Equipment, and Facilities of Nuclear Power Generating Stations.”

62. IEEE 730-1984, “IEEE Standard for Software Quality Assurance Plans.”

63. EPRI-NP-6433, “Source Book for Chemical Decontamination of Nuclear Power Plants,” August 1989.

64. EPRI-NP-2777, “Comparison of Decontamination Techniques for Reactor Coolant System Applications. ”

65. UCRL 15673, Human Factors Design Guidelines for Maintainability of DOE Nuclear Facilities.

66. UCRL 53526, Rev. 1, Natural Phenomena Hazards Modeling Project: Extreme Wind/Tornado Hazard Models for Department of Energy Sites, by D.W. Coats and R.C. Murray.

67. UCRL 53582, Rev. 1, Natural Phenomena Hazards Modeling Project: Seismic Hazard Models for Department of Energy Sites, by D.W. Coats and R.C. Murray.

68, D. Meister, Behavioral Analysis and Measurement Methods, John Wiley & Sons, New York, 1985.

69. NFPA 70, National Electric Code (NEC).

70. NFPA 101, Life Safety Code.

71. NFPA 496, Purged and Pressurized Enclosures for Electrical Equipment.

72. TM 5-1300, Structures to Resist the Effects of Accidental Explosions.

73. DOD-HDBK-761A Human Engineering Guidelines for Management Information Systems.

74. DOD-HDBK-763 Human Engineering Procedures Guide.

75. MIL-STD-1472D, Human Engineering Design Criteria for Military Systems, Equipment, and Facilities.

76. DOE/EH-0173T, Environmental Regulatory Guide for Radiological Effluent Monitoring and Environmental Surveillance.

ATTACHMENT 2

DEFINITIONS

Administrative Controls mean those provisions relating to organization and management, procedures, record keeping, assessment, and reporting necessary to ensure safe operation of a facility.

Administrative Limits means those procedural limits, self-imposed by the contractor, relating to nuclear safety. These limits are generally more restrictive and specific than externally imposed limits by Federal, State, or other entities.

ALARA As low as reasonably achievable

Anticipated Operational Event (AOE) means an abnormal event that is expected to occur during the lifetime of the facility (e.g., small radioactive materials spills, small fires).

Category A Reactor Facilities means those production, test, and research reactors designated by DOE based on power level (e.g., design thermal power rating of 20 megawatts steady state and higher), potential fission product inventory, and experimental capability,

Category B Reactor Facilities means those test and research reactors designated by DOE based on power level (e.g., design thermal power rating of less than 20 megawatts steady state), potential fission product inventory, and experimental capability.

Certification means that process by which contractor facility management provides written endorsement of the satisfactory achievement of qualification of a person for a position.

Confinement System means the barrier and its associated systems (including ventilation) between areas containing hazardous materials and the environment or other areas in the nuclear facility that are normally expected to have levels of hazardous materials lower than allowable concentration limits.

Containment System means a structurally closed barrier and its associated systems (including ventilation) between areas containing hazardous materials and the environment or other areas in the nuclear facility that are normally expected to have levels of hazardous materials lower than allowable concentration limits. A containment barrier is designed to remain closed and intact during all design basis accidents.

Contractor means any person under contract with the Department of Energy with responsibility to perform activities in connection with any facility.

Controlled Document means a document whose content is maintained uniform among the copies by an administrative control system.

Controls means, when used with respect to nuclear reactors, apparatus and mechanisms that, when manipulated, directly affect the reactivity or power level of a reactor or the status of an engineered safety feature. When used with respect to any other nuclear facility, "controls" means apparatus and mechanisms that, when manipulated could affect the chemical, physical, metallurgical, or nuclear process of the nuclear facility in such a manner as to affect the protection of health and safety.

Criticality Incident means an accidental, self-sustained nuclear chain reaction.

Decommissioning means the process of closing and securing a nuclear facility, or nuclear materials storage facility so as to provide adequate protection from radiation exposure and to isolate radioactive contamination from the human environment.

Decontamination means the act of removing a chemical, biological, or radiologic contaminant from, or neutralizing its potential effect on, a person, object or environment by washing, chemical action, mechanical cleaning, or other techniques.

Department or DOE means the Department of Energy.

Design Basis is the design inputs, the design constraints, and the design analysis and calculations. It includes topical areas such as seismic qualification, fire protections, and safe shutdown. It encompasses consideration of such factors as plant availability, plant efficiency, costs, and maintainability, and that subset that relates to safety and the authorization basis.

Design Basis Accidents (DBAs) Those postulated accidents that establish design and performance requirements for systems, structures, and components important to safety.

Emergency Power means a DBA-qualified and seismic Category-I-qualified, fully redundant power generation, switching, and distribution system that meets the IEEE 379 and IEEE 384 criteria. It is designated to activate on loss of the normal power supply (or in the cause of UPS systems, be online) and is used to supply components, and/or systems with power to allow them to maintain their safety functions.

Engineered Safety Features means systems, components, or structures that prevent and/or mitigate the consequences of potential accidents described in the FSAR including the bounding design basis accidents.

Existing Facility means a DOE nuclear facility that has received authorization to operate on or before the effective date of the requirement, or if authorization is not required, a DOE nuclear facility that has begun normal operation on or before the effective date of the requirement.

Facility Boundary means the fence or other barrier that surrounds and prevents uncontrolled access to the nuclear facility or facilities.

Fail-Safe means a design characteristic by which a unit or system will become safe and remain safe if a system or component fails or loses its activation energy.

Fire Hazards Analysis means an assessment of the risks from fire within an individual fire area in a DOE nuclear facility analyzing the relationship to existing or proposed fire protection. This shall include an assessment of the

consequences of fire on safety systems and the capability to safely operate a facility during and after a fire.

Graded Approach means a process by which the level of analysis, documentation, and actions necessary to comply with a requirement in this Part are commensurate with: (1) the relative importance to safety, safeguards, and security; (2) the magnitude of any hazard involved; (3) the life cycle stage of a facility; (4) the programmatic mission of a facility; (5) the particular characteristics of a facility; and (6) any other relevant factor.

Hazard means a source of danger (i.e., material, energy source, or operation) with the potential to cause illness, injury, or death to personnel, or damage to a facility or to the environment (without regard for the likelihood or credibility of accident scenarios or consequence mitigation).

Hazardous Materials are those materials that are toxic, explosive, flammable, corrosive, or otherwise physically or biologically health threatening.

Human Factors means those biomedical, psychosocial, work place environment, and engineering considerations pertaining to people in a human-machine system. Some of these considerations are allocation of functions, task analysis, human reliability, training requirements, job performance aiding, personnel qualification and selection, staffing requirements, procedures, organizational effectiveness, and workplace environmental conditions.

Human Factors Engineering means the application of knowledge about human performance capabilities and behavioral principles to the design, operation, and maintenance of human-machine systems so that personnel can function at their optimum level of performance.

Labeled means that equipment or materials to which has been attached a label, symbol, or other identifying mark of an organization acceptable to the cognizant DOE authority for fire protection concerned with product evaluation, that maintains periodic inspection of production of labeled equipment or materials and whose labeling the manufacturer indicates compliance with appropriate standards or performance in a specified manner.

Modification means any change made to structures, systems, components or procedures during any phase of the life of the nuclear facility.

Natural Phenomena Hazard means an act of nature (for example; an earthquake, wind, hurricane, tornado, flood, volcanic eruption, lightning strike, or extreme cold) which poses a threat or danger to people, structures, systems, and components.

New Facility means a DOE nuclear facility that does not qualify as an existing facility.

Nuclear Facility means reactor and nonreactor nuclear facilities.

Nuclear Safety means those aspects of safety that encompass activities and systems that present the potential for uncontrolled releases of fission products or other radioactive materials to the environment or for inadvertent criticality.

Overpressure means the maximal effective pressure is the highest of:

(1) The peak incident pressure;

(2) The incident plus dynamic pressure; or
(3) The reflected pressure (ref. TM 5-1300).

Program Secretarial Officers (PSOs) means an Assistant Secretary, Office Director, or NNSA Deputy Administrator. In the context of field operations, a PSO funds work at a particular site, facility or laboratory and is a "customer" of the field office."

Quality means the condition achieved when an item, service, or process meets, or exceeds the user's requirements and expectations.

Quality Assurance means all those actions that provide confidence that quality is achieved.

Quality Assurance Program or QAP The overall program established by an organization to implement the requirements of this Order. The Program assigns responsibilities and authorities, defines policies and requirements, and provides for the performance and assessment of work.

Reactor means, unless it is modified by words such as containment, vessel, or core, the entire nuclear reactor facility, including the housing, equipment, and associated areas devoted to the operation and maintenance of one or more reactor cores. Any apparatus that is designed or used to sustain nuclear chain reactions in a controlled manner, including critical and pulsed assemblies and research, test, and power reactors, is defined as a reactor. All assemblies designed to perform subcritical experiments that could potentially reach criticality are also to be considered reactors. Critical assemblies are special nuclear devices designed and used to sustain nuclear reactions. Critical assemblies may be subject to frequent core and lattice configuration change and may be used frequently as mockups of reactor configurations.

Risk means the quantitative or qualitative expression of possible loss that considers both the probability that a hazard will cause harm and the consequences of that event.

Safety Analysis means a documented process:

(1) To provide systematic identification of hazards within a given DOE operation;

(2) To describe and analyze the adequacy of the measures taken to eliminate, control, or mitigate identified hazards; and

(3) To analyze and evaluate potential accidents and their associated risks.

Safety Analysis Report or SAR means that report which documents the adequacy of safety analysis for a nuclear facility to ensure that the facility can be constructed, operated, maintained, shut down, and decommissioned safely and in compliance with applicable laws and regulations.

Safety Basis means the combination of information relating to the control of hazards at a nuclear facility (including design, engineering analyses, and administrative controls) upon which DOE depends for its conclusion that activities at the facility can be conducted safely.

Vertical line denotes change.

Safety Analysis Report or SAR means that report which documents the adequacy of safety analysis for a nuclear facility to ensure that the facility can be constructed, operated, maintained, shut down, and decommissioned safely and in compliance with applicable laws and regulations.

Safety Basis means the combination of information relating to the control of hazards at a nuclear facility (including design, engineering analyses, and administrative controls) upon which DOE depends for its conclusion that activities at the facility can be conducted safely.

Safety Class SSCs - Systems, Structures or Components including primary environmental monitors and portions of process systems, whose failure could adversely affect the environment, or safety and health of the public as identified by safety analysis.

Site Boundary means a well-marked boundary of the property over which the owner or operator can exercise strict control without the aid of outside authorities.

Structural Collapse means the failure of a structural component as a direct result of loss of structural integrity of the nuclear facility being subjected to various loadings.

Uninterruptible Power Supply (UPS) means a power supply that provides automatic, instantaneous power, without delay or transients, on failure of normal power. It can consist of batteries or full-time operating generators. It can be designated as standby or emergency power depending on the application. Emergency installations must meet the requirements specified for emergency power.

ATTACHMENT 3

PRELIMINARY GUIDANCE

FOR

NUCLEAR REACTOR NUCLEAR SAFETY DESIGN CRITERIA

TABLE OF CONTENTS

TABLE OF CONTENTS (Continued)

PRELIMINARY GUIDANCE FOR NUCLEAR REACTOR
NUCLEAR SAFETY DESIGN CRITERIA (NSDC)

1. INTRODUCTION. The nuclear safety design criteria (NSDC) described in this Order establish requirements for the design of all safety class structures, systems and components (SSCs) at DOE reactor facilities not subject to NRC review. Each DOE contractor should use these criteria and the guidance provided in this attachment in the review and development of existing and proposed directives, plans or procedures relating to the design of new DOE reactor facilities and the modification and evaluation of existing DOE reactor facilities.

   A graded approach should be used in the application of the guidelines provided in this attachment to ensure that the depth of detail required and the magnitude of resources expended for the design are commensurate with each facility's programmatic importance and the potential environmental, safety, and/or health impact of normal operations, Anticipated Operational Events (AOEs) and Design Basis Accidents (DBAs).

   Some preliminary guidance on the use of the graded approach is available in a DOE draft Standard on Hazard Categorization. Further guidance on the graded approach with regard to classifying safety class SSCs is under development.

2. DISCUSSION. The reactor design should be fundamentally safe to ensure that the reactor is capable of being shutdown safely and adequately cooled following postulated accidents. In addition, the reactor facility should be designed to provide defense-in-depth needed to prevent or mitigate the consequences of accidents that could result in uncontrolled release of radioactive materials to the environment. The nuclear safety design criteria ensure that the reactor and the associated safety class SSCs perform their intended safety functions.

   The scope of this order applies to the NSDC for all reactor types including, but not limited to: critical facilities, light water moderated reactors, heavy water moderated reactors, pool type reactor, liquid metal cooled reactors, gas cooled reactors, and short-pulse transient reactors. The complete set of design criteria for a reactor facility should also address requirements for facility siting, general component design, natural phenomena, conduct of operations, initial testing programs, accident analyses, technical safety requirements, and quality assurance.

   Portions of this Order recommend industry codes and ANSI standards and the applicable portions of 10 CFR Part 50 including the General Design Criteria in 10 CFR Part 50 Appendix A.

3. IMPLEMENTATION GUIDANCE. This document provides preliminary guidance on the applicability of each criterion to existing DOE reactors. For

this purpose, existing DOE reactors, were divided into five categories based on steady state power level:

1.	Large Category A reactors	Power (MWt) $\geq$ 200 MWt
2.	Small Category A reactors	20 MWt $\leq$ Power < 200 MWt
3.	Large Category B reactors	2 MWt $\leq$ Power < 20 MWt
4.	Small Category B reactors	Power < 2 MWt
5.	Critical assemblies	Power = 0 MWt

These five categories are provided as a rule of thumb for applying the NSDC. The operating characteristics of any specific reactor should be considered in determining the required level of protection.

Guidance for future DOE reactors is limited in certain areas because of the wide range of operating conditions that may occur. Where possible, applicable existing codes and standards are identified. Recommendations are made for standards to be used or the need for research to develop standards.

There are several sets of general design criteria available that may be applicable to various rector design concepts. For example, these include; the GDCs developed for the NPR-MHTGR, the NPR-HWR, the NPR-LWR, the commercial General Electric LMR design (PRISM), the commercial Rockwell International LMR design (SAFR), the commercial LMR design (CRBR). In addition, the ANS 54.1 committee has produced a set of GDCs for LMRs. These sources provide useful input for consideration in the development of criteria and standards for DOE reactor facilities. In addition there are several sets of international safety design criteria that are relevant to the considerations of this section, notably Safety Series 35.S1, "Code on the Safety of Nuclear Research Reactors: Design," November, 1991 which is under consideration by the NRC for guidance on reviews of research reactors. These codes and criteria have been developed through extensive participation by many experts in the nuclear community and should be consulted by DOE and DOE contractors in the development of criteria for applications involving plants similar in design to these concepts.

a. General Safety Design Criteria. The overall design philosophy to achieve the highest level of reactor safety is to provide defense in-depth. Defense-in-depth means that not only more than one system or component prevents uncontrolled releases, but that these multiple safety class SSCs individually can perform their safety function in the absence or malfunction of the others.

In order to meet this criterion, DOE nuclear reactor facilities should be designed, constructed, operated, and decommissioned with:

- Appropriate passive barriers, (i.e., fuel clad, coolant system boundaries, containment) to prevent or minimize potential radioactive releases;

- Engineered safety features to prevent accidents and to

mitigate the effects of DBAs; and procedural controls to mitigate the effects of potential releases.

(1) Single Failure. A "single failure" means an occurrence which results in the loss of capability of a component to perform its intended safety functions. Multiple failures resulting from a single occurrence are considered to be a single failure. Fluid and electrical systems are considered to be designed against an assumed single failure if neither:

- A single failure of any active component (assuming passive components function properly), nor
- A single failure of a passive component (assuming active components function properly), results in a loss of the capability of the system to perform its safety functions.

(2) Quality Standards. It is DOE policy to establish quality assurance requirements to ensure that risks and environmental impacts are minimized and that safety, reliability, and performance are maximized through the application of effective management systems commensurate with the risks posed by the reactor facility and its operation. DOE 5700.6C establishes the minimum requirements for and provides the guidance for developing and implementing quality assurance programs. Quality assurance programs may supplement these minimum requirements through the use of accepted industry standards such as those in ASME/NQA-1.

DOE 5700.6C establishes 10 minimum criteria in three areas for all quality assurance programs. These 10 criteria (and their main areas) are:

(a) Management.

1 Program-Organizations should develop, implement, and maintain a written Quality Assurance Program (QAP). The QAP should describe the organizational structure, functional responsibilities, levels of authority, and interfaces for those managing, performing, and assessing adequacy of work. The QAP should describe the management system, including planning, scheduling, and cost control considerations.

2 Personnel Training and Qualification-Personnel should be trained and qualified to ensure they are capable of performing their assigned work. Personnel should be provided continuing training to ensure that job proficiency is maintained.

3 Quality Improvement-The organization should establish and implement processes to detect and prevent quality

problems and to ensure quality improvement. Items and processes that do not meet established requirements should be identified, controlled, and corrected. Correction should include identifying the causes of problems and preventing recurrence. Item reliability, process implementation, and other quality-related information should be reviewed and the data analyzed to identify items and processes needing improvement.

4 Documents and Records-Documents should be prepared, reviewed, approved, issued, used, and revised to prescribe processes, specify requirements, or establish design. Records should be specified, prepared, reviewed, approved, and maintained.

(b) Performance.

1 Work Processes. Work should be performed to established technical standards and administrative controls. Work should be performed under controlled conditions using approved instructions, procedures, or other appropriate means. Items should be identified and controlled to ensure their proper use. Items should be maintained to prevent their damage, loss or deterioration. Equipment used for process monitoring or data collection should be calibrated and maintained.

2 Design. Items and processes should be designed using sound engineering/scientific principles and appropriate standards. Design work, including changes, should incorporate applicable requirements and design bases. Design interfaces should be identified and controlled. The adequacy of design products should be verified or validated by individuals or groups other than those who performed the work. Verification and validation work should be completed before approval and implementation of the design.

3 Procurement. The organization should ensure that procured items and services meet established requirements and perform as specified. Prospective suppliers should be evaluated and selected on the basis of specified criteria. The organization should verify that approved suppliers can continue to provide acceptable items and services.

4 Inspection and Acceptance Testing. Inspection and acceptance testing of specified items and processes should be conducted using established acceptance and performance criteria. Equipment used for inspections and tests should be calibrated and maintained.

(c) Assessment.

1 Management Assessment. Management at all levels should periodically assess the integrated quality ASSURANCE program and its performance. Problems that hinder the organization from achieving its objectives should be identified and corrected.

2 Independent Assessment. Planned and periodic independent assessments should be conducted to measure item quality and process effectiveness and to promote improvement. The organization performing independent assessments should have sufficient authority and freedom from the line organization to carry out its responsibilities. Persons conducting independent assessments should be technically qualified and knowledgeable in the areas assessed.

Specific guidance for each of these criteria is given in Attachment I of DOE 5700.6C, QUALITY ASSURANCE.

(3) Design Basis for Protection Against Natural Phenomena. The Nuclear safety design Criteria for DOE Reactors require that:

Safety class structures, systems, and components should be designed to withstand the effects of natural phenomena, without loss of capability to perform their safety functions.

In order to facilitate the implementation of this nuclear safety design criterion DOE 5480.28, NATURAL PHENOMENA HAZARDS MITIGATION, specifies the requirements for each new and existing DOE facility. The evaluation criteria for this DOE Order are built around a graded approach. DOE 5480.28 specifies that an NPH analysis will be performed for all new and existing DOE facilities. Specifically:

- The performance category should be determined for each structure, system or component.
- The site specific hazards should be determined and the resulting loads should be developed.
- The NPH evaluation should follow the procedures developed in DOE 5480.28 and the related DOE Standards.

(4) Fire Protection. Nuclear installations may contain varying quantities of solid, liquid, and gaseous radioactive materials which, if damaged by fire or explosion, may result in an unacceptable release of radioactive materials into the environment. The presence of these substances, combined with the possibility of the fire or explosion endangering

the safe operation of the facility, imposes unique requirements on a facility's fire protection program.

The Nuclear Safety Design Criteria for Fire Protection require the effective implementation of a fundamental fire protection philosophy known as "defense-in-depth". As applied to fire safety, this principle requires each facility to achieve an adequate balance of each of the following elements:

- Administrative controls necessary to assure the prevention of fires.
- Providing early detection and alarm capability and a means to rapidly suppress those fires that do occur.
- Designing plant safety systems so that redundant safety equipment is protected by automatic fire suppression systems and separated from each other and from other plant areas by fire barriers such that a fire would not endanger other safety related equipment required for safe shutdown. Alternate or dedicated shutdown capability should be provided where the protection of safety systems required for safe shutdown is not provided by established fire suppression methods.

Specific, detailed guidance for establishing and implementing a fire protection program necessary to assure this level of safety at DOE nuclear installations is provided in DOE 5480.7, FIRE PROTECTION, which has as its objectives:

- Minimizing the potential for the occurrence of a fire and related perils.
- Ensuring that the fire does not cause an unacceptable onsite or offsite release of hazardous material that could threaten the public health and safety of the environment.
- Establishing requirements that provide an acceptable degree of life safety to DOE and contractor personnel and to the public from fire in DOE facilities.
- Ensuring that vital DOE programs do not suffer unacceptable delays as a result of fire and related perils.
- Ensuring that property damage from fire and related perils are not greater than an acceptable level.

(5) Environmental Effects Design Bases. The general requirements for environmental design and qualification of

all safety class structures, systems, and components are embodied in DOE 5480.27.

(6) Sharing of Structures, Systems, and Components. To demonstrate that such sharing of safety class structures, systems, and components among reactor facilities does not significantly impair their ability to perform their safety functions, accident analyses should be performed and submitted for review. The accidents to be analyzed should reflect the full spectrum of events for the reactor type involved. There are no specific criteria that should be met by the analytical methods or data that are used. In general, the analytical methods and data base should be representative of the state of the art. The experiments used to validate the analytical methods used should be adequate and encompass a sufficient range.

(7) Siting. Insufficient experience has been accumulated to permit the writing of detailed acceptance criteria that would provide a quantitative correlation of all factors significant to the question of acceptability of reactor sites. The following criteria are intended as interim guidance to identify a number of factors to be considered in the evaluation of reactor sites.
The specific factors which should be in evaluating the suitability of a proposed reactor site include:

- The characteristics of the reactor design and proposed operation.
- The population density and use characteristics of the site and environs.
- The physical characteristics of the site, including geology, hydrology, and site specific natural phenomena.
- The ecology of the site and environment.
- Transportation and land use.

DOE 5480,28, NATURAL PHENOMENA HAZARDS MITIGATION, describes the basis for evaluating site specific natural phenomena hazards (NPH) such as, hurricanes, tornadoes, floods, volcanoes, lightning, snow, extreme cold and forest fires.

(8) Containment and Confinement Barriers. A containment is an essential design feature for providing defense in depth protection for health and safety of the public and on-site workers for large reactors. As such, the codes and standards of the nuclear industry should be applied in a

graded fashion for all large DOE Category A reactors, including the following criteria from 10 CFR Part 50 Appendix A:

Criterion 50 -	Containment design basis
Criterion 51 -	Fracture prevention of Containment pressure boundary
Criterion 52 -	Capability for containment leakage rate testing
Criterion 53 -	Provisions for containment testing and inspection
Criterion 54 -	Piping systems penetrating containment
Criterion 55 -	Reactor coolant pressure boundary penetrating containment
Criterion 56 -	Primary containment isolation
Criterion 57 -	Closed system isolation valves

In order to ensure functionality of the containment design during normal operations, AOEs and DBAs. 10 CFR 50, Appendix A, Criterion 38 - Containment Heat Removal, and Criteria 39 and 40 - Inspection and Testing of Containment Heat Removal Systems should be included as part of the graded approach assessment for the overall containment design.

Since there are important differences between commercial light water power reactors and DOE reactors, all of the containment nuclear safety design criteria should be applied in a graded approach making a full assessment of the potential hazard during operation (fission product inventory), the machanism for dispersal, and the duration of operation. Containment heat removal systems and containment testing and inspection procedures (10 CFR 50, Appendix J) should be considered for large Category A reactors but are probably not necessary for smaller facilities.

Containment enhancement provisions may also be part of a graded approach as augmentation or in lieu of 10 CFR 50 containment design criteria. For an example, a filtered vented containment or confinement system may provide adequate protection to the public and onsite workers so that a containment heat removal system may not be required to reduce ultimate risk to an acceptable level. Whatever containment design criteria are used, the ultimate goal of protecting the health and safety of the public and onsite workers should be assured.

For small Category A reactors, all Category B reactors, and critical facilities, implementation of the graded approach to hazard analysis should be used to evaluate the application of containment related design criteria.

A confinement system is required for any of the smaller

reactor facilities which do not justify a containment system.

(9) Human Factors Engineering (HFE). The standard, accepted practice within the disciplines of systems engineering and HFE is to apply HFE to the developing system as early in the design and development process as possible.

As with the other NSDC, the extent and formality of the HFE program should be graded in relation to the hazard category and the importance of HFE to safety.

The HFE program should include HFE planning, systems analysis, design and test, and evaluation to the level appropriate to the facility being designed. This program should meet the intent of IEEE-STD-1023. A formal HFE program is suggested for all safety systems. A formal HFE program should use qualified HFE personnel.

(a) Program Plan. A HFE program plan should be prepared during conceptual design of a system, the plan should address the approach to providing a human-oriented design of the facility. The plan should detail the types of HFE analyses, design efforts, evaluations, and schedule of the HFE effort to provide timely input to the overall design. The plan should reflect the integration of HFE with other design disciplines. The plan should provide a description of human performance objectives, applicable standards and specifications, and other project-specific information.

(b) Analysis of Requirements. HFE should be involved in function analysis where the various functions necessary to meet the facility mission objectives are determined. HFE should provide the analyses to properly allocate functions to man or machine (see Meister, 1985), identifying the role of the human in system/facility operation and maintenance. A Task Analysis should be performed, identifying and analyzing task for implications for design, human error, safety and other human performance issues. Human Factors Engineering design requirements related to human performance should be defined. These analyses should be reviewed during normal design reviews and evaluations. (DOD-HDBK-763, Meister, 1985)

(c) Design Process. The task analysis should be used in the design process to orient the design of the human-machine interface toward tasks to be performed by the operator(s) and maintainer(s). Specific design should be based upon appropriate HFE design criteria, such as DOE-STD-HFAC or MIL-STD-1472D, refined as needed for the evolving design. (DOD-HDBK-763, Meister, 1985)

(d) Test and Evaluation. The Human-Machine Interface should be validated using appropriate mockups, simulations, and prototypes during and following the design. The evaluations should begin early in the design process and continue throughout the design and should include a sample of all critical design scenarios.

(e) HFE Design Guidance. There are several sources of HFE design criteria from which a set of design criteria may be adopted. The areas covered by these criteria, when applicable, include the following:

- Controls: appropriate and usable;
- Displays: visible and readable;
- Control/Display Integration: appropriate controls and displays used and are compatible with one another, both in type and location;
- Labeling: clear and unambiguous;
- Workstation Design: allows operation and is adequate;
- Workspace Design: allows personnel movement and access to all necessary activities;
- Working Environment: safe, comfortable and compatible with human performance;
- Personnel Hazards and Safety: safe for personnel;
- Design for Maintainability: allows access to, space for maintenance and does not exceed human performance capabilities;
- Human-Computer Interface: user-friendly software interface;
- Design for Remote Operation: provides information and control for operation of remote equipment; and
- Physical Anthropometry: equipment is of the proper size to accommodate a reasonable range of operators.

(10) Dynamics Effects Design Bases. In general, these requirements of the Order apply to large Category A reactors which use a circulating fluid (light water, heavy water, helium, liquid metal, etc.) at high pressure to cool the reactor core.

For low pressure systems and smaller reactors, the dynamics effects requirements do not apply.

(11) Safeguards and Security. In general, the reactor design should make adequate provisions to prevent unauthorized entry to the site or buildings on the site in order to prevent theft or unauthorized removal of nuclear materials and sabotage to the reactor.

The major elements of a physical protection system include:

- Detection System: A System providing the capability to detect an adversary action or anomalous behavior.
- Assessment System: A system providing the capability to assess the nature of the adversary action.
- Communication System: A system providing the capability to communicate to response forces and other personnel.
- Barriers: A system of barriers or other impediments to delay, channel personnel, or deny access to Special Nuclear Material (SNM) or vital areas.
- Response: The capability of the security organization to neutralize the adversary.

To the extent possible the design should incorporate redundancy, physical separation, compartmentalization and access control for safety class SSCs in order to reduce the threat of insider sabotage.

(12) Effluent and Emission Control

(a) Control of Releases of Hazardous Materials to the Environment Hazardous effluents released to the environment (radioactive and nonradioactive) should not exceed the limits referenced in DOE 5400.1 and DOE 5400.5. Sampling and monitoring should ensure adequate and accurate measurements under normal operations, anticipated operational occurrences, and DBA conditions.

Releases of hazardous materials postulated to occur as a result of DBAs that would exceed DOE release guideline should be limited by designing facilities such that at least one confinement system remains fully functional following any credible DBA (i.e., unfiltered/unmitigated releases of hazardous levels of such materials should not be allowed following such accidents).

In addition, it is DOE's policy that exposure to radiation resulting from DOE operations be maintained As Low As Reasonably Achievable (ALARA). The application of ALARA to DOE nuclear reactors has two principle divisions: occupational exposure and public exposure.

1 Occupational Exposure. Specific evaluation criteria for radiation protection of the worker from ionizing radiation is provided by DOE

5480.11 and Chapter 2 of the Radiological Control Manual. The Radiological Control Manual also provides guidance on implementing ALARA with regard to occupational exposure to radiation.

2 Public Exposure. DOE 5400.5 provides specific guidelines for public exposure along with the overall goal of ALARA.

(b) Monitoring Hazardous Materials. All monitoring systems should be calibrated annually at a minimum with appropriate national standards to ensure validity of reported values.

All radiation monitoring, alarm, and warning systems that are required to function during a loss of normal power should be provided with an emergency uninterrupted power supply (UPS) unless it is demonstrated that they can tolerate a temporary loss of function without losing needed data and they are provided with standby or emergency (switched) power. Determination of the power supply type and quality should be based on the safety classification of the monitoring system or device. The sampling motivation (vacuum) should be installed to the same requirement.

In addition to a local station alarm, radiation monitoring systems should have central (i.e., control room or radiation monitoring office) readout and alarm panels that are accessible after a DBA to evaluate internal conditions.

(13) Reactor Decontamination and Decommissioning.

(a) Decontamination. In order to minimize occupational radiation exposure, the design of a nuclear reactor should include provisions for the reduction or removal of radioactive contaminants from plant components, plant equipment, protective clothing, and personnel. Two EPRI studies, NP-6433, "Source Book for Chemical Decontamination of Nuclear Power Plants," August, 1989 and NP-2777. "Comparison of Decontamination Techniques for Reactor Coolant System Applications," describe features necessary for effective "in-place" and "offsystem" decontamination operations. In-place decontamination is the decontamination of permanently installed equipment without removing it from the plant system. Off-system decontamination is decontamination of equipment which has been temporarily removed from its normally installed location specifically for decontamination purposes as well as the decontamination of small tools and instruments.

Since dedicated areas are needed to allow effective decontamination of equipment and personnel and to minimize the spread of contamination to adjacent areas during equipment handling operations, decontamination areas with sinks, workbench space, storage for hot tools and equipment, and decontamination supplies should be provided. Typical buildings to be furnished include primary containment, fuel handling and storage, health physics, contaminated shops, and plant radwaste facilities.

All permanently established decontamination areas should be provided with locally alarmed radiation monitors near potentially high radiation level collection devices such as tanks, filters, demineralizes, etc., in order to avoid unexpected exposure of personnel near the decontamination equipment. These areas should also be provided with exit radiation monitors to minimize the possibility of "hot particles" being picked up and transported by personnel out of the area. Special coatings should be applied to the floors and walls of areas containing radioactive fluids or other potential contaminants.

(b) Decommissioning. A nuclear facility should be retired from service and decommissioned at the end of its operating life. The decommissioning process, which consists of the dismantling of the facility and the subsequent isolation and/or removal of radioactive and hazardous materials, should be carried out in a manner which minimizes radioactive exposures to workers and to the environment and also minimizes the quantity of waste. The design and construction of a nuclear reactor should include features which facilitate these objectives. The following design principles are applicable.

- Use of modular separable confinements;
- Use of localized liquid transfer systems;
- Location of exhaust air cleanup components at or near individual enclosures;
- Equipment design that minimizes the accumulation of radioactive or hazardous materials;
- Designs that ease cut-up, dismantlement, removal, and packaging of contaminated equipment;
- Fully drainable piping systems, including tanks; and

- Choice of materials and design that minimize the activation of components and structures.

As part of the NRC's evaluation of its decommissioning policy and its modification of regulations pertaining to the decommissioning process, the NRC issued NUREG/CR-3587, "Identification and Evaluation of Facilitation Techniques for Decommissioning Light Water Power Reactors."

In accordance with the guidance presented in that document, provision for the following techniques should be considered in the design of a nuclear reactor, as applicable, in order to facilitate decommissioning at the end of the reactor's operating life. These techniques (grouped by primary objective) are the following:

1 Wastes Volume Reduction

a Sealed Nonporous Insulation - Use of such insulation materials prevents the absorption of contaminated liquids by the insulation.

b Enclosed Cable Trays - Totally enclosing the trays with solid sheet metal (to the extent that such enclosures do not interfere with plant maintainability) will prevent the contamination of large quantities of cabling.

c Minimize Cable Trays in Contaminated Areas - Locating the trays in clean areas to the extent possible minimizes contamination.

d Relocated Motor Control Centers - The amount of contaminated equipment will be reduced by locating motor control centers in areas that are not susceptible to contamination.

e Bolted Steel Construction - This construction technique reduces radioactive waste by using an easily decontaminated construction material. This technique will also reduce exposure by decreasing disassembly time.

f Smooth and Coat Concrete Surfaces - These are preventive and protective measures against the radioactive contamination of concrete surfaces and thus decrease the quantity of radwaste associated with the decontamination of such surfaces.

2 Exposure Reduction

a Scale Models - Exposure savings can be realized during and after the operational life of the facility by using models as planning aids.

b Remote Sampling - This capability reduces exposure associated with environmental sampling activities by allowing the data to be collected remotely.

c Waste Storage Capacity - Provision should be made in the site layout for a waste storage facility (which may not be constructed until just prior to decommissioning if it is intended only for decommissioning wastes) to provide temporary storage space so that accumulated waste will neither slow down decommissioning nor be stored in areas which may pose exposure hazards.

d Flanged Construction - This construction technique (to the extent it does not compromise technical specifications on leakage) will reduce exposure by decreasing the time required to disconnect components and by reducing the use of dismantling methods which spread contamination (e. g., power hacksaws and circular cutters).

e Quick Disconnect Components - This construction technique (to the extent it does not compromise technical specifications on leakage) will reduce exposure by decreasing the time required to disconnect components.

f Non-Embedment of Pipes, Ducts and Equipment in Concrete - This design feature (to the extent it does not compromise release of fluids from the pipes) reduces the effort and exposure time required to remove items at the time of decommissioning.

g Removable Roof, Wall Panels and Plugs - This design feature provides improved access for removal of radioactive components and thus reduces exposure time

h Access to and into all Tanks - Such access will shorten setup time and thus reduce exposure.

i Plant Breathing Air Supply System - Breathing air supplies for decommissioning work should be incorporated in the plant design and installed at the time of construction to avoid the

problems with portable units at the time of decommissioning.

j Pre-Installed Manipulator Supports - This design feature is intended to reduce exposure during segmentation of the reactor vessel by performing the preliminary work in a low-radiation environment during construction rather than in a high-radiation environment after plant shut-down.

k Lifting Lugs on Large Components - Installation of the lifting lugs prior to plant startup rather than in a radioactive environment after plant shutdown will prevent significant radiation exposures.

l Anchor Points for Lifts - Incorporation of anchor devices for lifting large components prior to plant startup rather than in a radioactive environment after plant shutdown will prevent significant radiation exposures.

m Tracks for Remote Cutting Devices - Installation of guide tracks for segmentation cutting devices prior to plant startup rather than in a radioactive environment after plant shutdown will prevent significant radiation exposures.

n Preplaced Concrete Core Samples - In order to obtain activated concrete profiles for radiological characterization of the concrete, core samples are drilled or cast in place prior to plant startup rather than in a radioactive environment after plant shutdown. At that time, the cores are pulled out in minutes rather than hours, thus reducing exposure.

o Complete Drainage Capacity - Exposure due to pockets and traps containing contaminated liquids is minimized. Complete flushing and drying of the system is possible prior to dismantling.

p Canal Gate in Refueling Canal - The installation of a canal gate in the refueling canal would allow for parallel cutting of the reactor vessel and internals, resulting in a reduction in segmentation time and thus in exposure.

q Containment and Isolation of Liquid Spills - Containment features instituted during the design phase (e.g., curbing, dikes, reserve tankage, increased sump capacity) will reduce

contamination during the operational life of the plant and thus reduce the contaminated surface area to be removed during decommissioning.

r Preplaced Blast Holes - By incorporating blasting holes into monolithic concrete structures during the construction of the plant before they have become radioactive, the occupational exposure associated with their demolition is reduced.

s Substitution and Purification of Materials - Use of low-cobalt steels will result in lower Co-60 activation products and thus in lower occupational exposures during decommissioning.

t Material Selection - Apply design techniques and selection of materials to minimize activation or to assure that activated material can readily be removed and disposed.

(14) Waste Management

(a) The design maintenance and operation of DOE reactors should aim at minimizing the generation of radioactive wastes. Radioactive waste treatment systems should have adequate provisions for control and monitoring to keep releases below prescribed limits, provided in DOE 5480.1B, DOE 5400.1, and DOE 5400.5.

(b) The design should include appropriate means, such as shielding and filtering systems, to reduce the dose to personnel and releases to the environment to ALARA levels as prescribed in the Radiological Control Manual.

(c) The design should provide adequate means for control, sampling, and monitoring of discharges of radioactive effluent to the environment.

(d) The design should provide adequate facilities, as necessary, for handling, collecting, processing, storage, and disposal or removal from the site of radioactive wastes. In cases where liquid wastes are handled, such facilities shall have provisions for leakage detection and waste recovery, if appropriate.

b. Specific Design Requirements

(1) Reactor Coolant Boundary. The reactor coolant boundary means all those coolant-containing components of nuclear reactors, such as pressure vessels, piping, pumps, valves, and heat exchangers, which are part of the reactor coolant system, or connected to the reactor coolant system, up to

and including any and all of the following:

- The outermost containment isolation valve in system piping which penetrates primary reactor containment,

- The second of two valves normally closed during normal reactor operation in system piping which does not penetrate primary reactor containment,

- The reactor coolant system safety and relief valves.

In general, the requirements of this section apply to all large Category A reactors which use a circulating fluid (light water, heavy water, helium, liquid metal, etc.) to cool the reactor core.

(a) Reactor Coolant Boundary Integrity. The most detailed and widely accepted methodology to satisfy the nuclear safety design criteria for the reactor coolant boundary originates with the following sections of 10 CFR Part 50:

- 50.55a Codes and Standards
- 50.60 Acceptance Criteria for Fracture Prevention Measures for Normal Operation
- 50.61 Fracture Toughness Requirements for Protection Against Pressurized Thermal Shock
- 50, App G Fracture Toughness Requirements
- 50, App H Reactor Vessel Material Surveillance Program Requirements

While these sections specifically address water-cooled nuclear power reactors, the methodology is applicable to other nuclear reactors which have a primary coolant boundary.

From this basis, the more detailed design, analysis, and acceptance criteria are referenced. The primary references for the reactor coolant boundary are:

- ASME Boiler and Pressure Vessel Code, Section III
- Applicable ASME Section III Code Cases
- NRC Regulatory Guides
- NRC Standard Review Plan

In addition, DOE 5480.28 addresses natural phenomena hazards protection for DOE-owned facilities; it defines the design-basis external events for DOE-owned reactors.

1 ASME Section III Classification. Components which are part of the reactor coolant boundary should meet the requirements for Class 1

components in Section III of the ASME Boiler and Pressure Vessel Code.

Components which are connected to the reactor coolant system and are part of the reactor coolant boundary need not meet the requirements for Class 1 components, provided

a In the event of postulated failure of the component during normal reactor operation, the reactor can be shut down and cooled down in an orderly manner, with adequate makeup provided by the reactor coolant makeup system; or

b The component is or can be isolated from the reactor coolant system by two (2) valves in series (both closed, both open, or one closed and the other open). Each valve should be automatically actuated and, assuming the other valve is open, its closure time should be such that, in the event of postulated failure of the component during normal reactor operation, each valve remains operable, and the reactor can be shut down and cooled down in an orderly manner, with adequate makeup provided by the reactor coolant makeup system only.

The existence of an adequate reactor coolant makeup system is prerequisite to meeting either basis for exemption. Components which can be exempted from the Class 1 requirements, in accordance with the previous paragraph, should meet the requirements for Class 2 components in Section III of the ASME Boiler and Pressure Vessel Code.

Alternatives to the specified requirements may be permissible, if (1) the proposed alternative would provide an acceptable level of quality and safety, or (2) compliance with these requirements would result in hardship and unusual difficulties, without a compensating increase in the level of quality and safety.

2 ASME Code Section III Design Requirements. Class 1 Components should be designed and analyzed in accordance with Subsection NB. Class 2 Components should be designed and analyzed in accordance with Subsection NC.

In addition, NRC Regulatory Guide 1.84, “Design

and Fabrication Code Case Acceptability - ASME Section III Division 1" and NRC Regulatory Guide 1.85, "Materials Code Case Acceptability - ASME Section III Division 1" list the ASME code cases which have been approved for use by the NRC. These may be used, as applicable, to supplement Subsections NB and NC.

3 Elevated-Temperature Design. NRC Regulatory Guide 1.87, "Guidance for Construction of Class 1 Components in Elevated-Temperature Reactors (Supplement to ASME Section III Code Cases 1592, 1593, 1594, 1595, and 1596)" was issued in June 1975 to address "requirements with respect to ASME Class 1 components operating at elevated temperatures. This guide applies to high-temperature gas-cooled reactors (HTGRs), liquid metal fast-breeder reactors (LMFBRs) and gas-cooled fast-breeder reactors (GCFBRs)."

The following current ASME Code Cases supplement ASME Section III for elevated-temperature applications:

Code Case No.	Subject
N-47 (1592)	Class 1 Components in Elevated Temperature Service
N-48 (1598)	Fabrication and Installation of Elevated Temperature Components
N-49 (1594)	Examination of Elevated Temperature Nuclear Components
N-50; N-467 (1596)	Testing of Elevated Temperature Components
N-51; N-257 (1596)	Protection Against Overpressure of elevated Temperature Components
N-201	Class CS Components in Elevated Temperature Service
N-253	Construction of Class 2 or Class 3 Components for elevated Temperature Service
N-254	Fabrication and Installation of Elevated Temperature Components, Class 2 and 3

These Code Cases should be used, as applicable, to supplement Subsection: NB and NC for elevated-temperature design.

(b) Alternate Integrity Criteria. The design of a reactor coolant boundary which is outside the scope of ASME Code Section III and associated code cases, due to design temperature, materials selection and/or any other design feature, should meet the nuclear safety design criteria of this section and should employ a design and analysis methodology which is consistent with the requirements of ASME Code Section III.

(c) Fracture Prevention. Non-ductile failure of the reactor coolant boundary is an unacceptable condition. Specific requirements have been defined in 10 CFR Part 50 for water-cooled nuclear power reactors. The methodology, and the specified margins of safety should be applied to the primary coolant boundary for large Category A DOE reactors, to the extent practical. The intent is to assure a comparable level of safety for DOE reactors.

For normal operation, the fracture prevention criteria are defined in 10 CFR Part 50.60 and the referenced Part 50 Appendices G and H.

Fracture toughness requirements for protection against pressurized thermal shock are defined in 10 CFR Part 50.61. These requirements should be reviewed for applicability; if applicable, they provide the basis for ensuring the integrity of the reactor vessel for pressurized thermal shock conditions.

(d) Primary Containment Penetrations. Each line that is part of the reactor coolant pressure boundary and that penetrates primary reactor containment should be provided with containment isolation valves, unless it can be demonstrated that the containment isolation provisions for a specific class of lines, such as instrument lines, are acceptable on some other defined basis.

The following four configurations of isolation valves provide adequate isolation capability during reactor operations:

	(1)	(2)	(3)	(4)
Inside Containment	Locked Closed	Automatic	Locked Closed	Automatic
Outside Containment	Locked Closed	Locked Closed	Automatic*	Automatic*

* A simple check valve should not be used as the automatic isolation valve outside containment.

Isolation valves outside containment should be located as close to containment as practical and upon loss of actuating power, automatic isolation valves should be designed to take the position that provides greater safety.

(2) Electric Power Systems. Guidance related to the implementation of the NSDC for Electrical Systems at DOE nuclear facilities is currently contained in a variety of sources including existing DOE Orders, industry standards, and guidance documents prepared by the NRC (see Reference section of this Order), It should be recognized, however, that the applicability of certain specific criteria may vary in accordance with the type of facility and the nature of the activities or processes performed.

General guidance related to the overall design, operation, and maintenance requirements of electrical distribution systems at DOE facilities is provided in Division 16 of DOE 6430.1A. The criteria contained in this section of the Order are based on accepted industry standards for electrical system design and operation, such as NFPA 70, National Electrical Code (NEC) and those promulgated by NRC, IEEE, ANSI, NEMA, and UL. Additionally, all systems should comply with the NEC and ANSI C2, "National Electrical Safety Code."

(3) Reactor Core Design. The many types of DOE reactor designs and the wide range of their missions precludes offering specific guidance. The intent of the guidance in this section is to ensure that the fuel remains within specific limits so that the fission products remain within the fuel, thus providing the first fission product barrier in a defense-in-depth strategy. The following general guidance is adapted from NUREG-0800, "Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants," Section 4.3, "Nuclear Design." This guidance was originally developed for commercial, light water power reactors, but may by useful for other types of reactors.

(a) Reactor Design. This criterion requires that acceptable design limits be specified that are not to be exceeded during normal operation, including the effects of AOEs. The selection of acceptable design limits should demonstrate that the a high percentage of fission products would be retained in the fuel to a specified confidence level. These limits should be justified by the use of analytical techniques and experimental data. There are no specific criteria that should be met by the analytical methods or data that are used. In general, the analytical methods and data base should be representative of the state of the art. For large category A reactors, experiments should be used to validate the design limits and the analytical methods.

(b) Reactor Inherent Protection. This criterion can be satisfied by the existence of a negative doppler coefficient and negative power coefficients. Other criteria may be acceptable for special types of reactor designs.

(c) Suppression of Reactor Power Oscillations. The intent of this criterion, is to ensure that no transient power conditions occur that would cause the reactor design limits to be exceeded. The criterion can be met either by showing that no such power oscillation exists or if it does, it can be easily detected and remedied. There are no direct or explicit criteria for the power densities and power distributions allowed during (and at the limits of) normal operations, either steady-state or transient.

Criteria for acceptable values and uses of uncertainties in operation, instrumentation numerical requirements, limit settings for alarms or scram, frequency and extent of power distribution measurements, and use of excore and incore instruments and related correlations and limits for offsets and tilts, all vary with reactor type. Guidance will need to be developed for each specific reactor type.

(4) Protection Systems. The criteria in this section ensure that mechanisms are in place to terminate the nuclear chain reaction under all normal operating conditions, AOEs, and DBAs.

General guidance for meeting the criteria in this section has been, adapted from NUREG-0800, “Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants,” Section 4.3, “Nuclear Core Design,” with respect to specified acceptable reactor design limits. The analyses should demonstrate:

- That normal operation, including the effects of AOEs, have met reactor design criteria;

- That the automatic initiation of the protection system assures that reactor design criteria are not exceeded as a result of AOEs and ensures the automatic operation of safety class SSCs under DBAs; and

- That no single malfunction of the protection system causes violation of the reactor design limits.

Additional guidance for this area can be obtained from, IEEE-603, "Standard Criteria for Safety Systems for Nuclear Power Generating Stations."

(5) Instrumentation and Control Systems.

(a) Instrumentation and Control. Instrumentation and control should be provided to monitor variables and systems over their anticipated ranges for normal operation, for AOEs, and DBAs as appropriate to assure adequate safety, including those variables and systems whose operating continuity is vital for the control of hazardous materials and protection of health, life, and property. Appropriate controls should be provided to maintain those variables and systems within prescribed operating ranges. The design should incorporate sufficient redundancy and/or diversity to ensure that a single failure will not result in a loss of monitoring capability for safety class systems, and should ensure that sufficient monitoring capability remains available in the event of natural phenomena events, AOEs, or (DBAs).

The criteria applicable to Instrument and Control (I&C) systems establish minimum requirements necessary to ensure that adequate monitoring and control capability is provided for safety class SSCs. The different designs and operating characteristics of DOE nuclear facilities limit the amount of specific guidance that can be provided. However, helpful general guidance for implementing these criteria at a particular DOE facility may be obtained by reviewing the existing DOE and NRC design requirements and guidance documents; including:

- IEEE-603, "Criteria for Safety Systems for Nuclear Power Generating Stations".

- Division 13 of DOE Order 6430.1A, "General Design Criteria".

- Chapter 7.1 of NUREG-0800, "Standard Review Plan for the Review of Safety Analysis Reports for

Nuclear Power Plants."

- Title 10 to the Code of Federal Regulations, Part 50, (10 CFR 50), Appendix A, "General Design Criteria for Nuclear Power Plants," specifically: GDC 1, 13, 15, 19, 20, 22, 23, 24, and 64.

- USNRC Regulatory Guides (Reg. Guides): 1.47, 1.75, and 1.97.

(b) Reactivity Control System Redundancy and Capability. The intent of these two criteria (paragraph 8d(5)(b) and (5)(c) of this Order) is to ensure that there are at least two separate mechanisms for controlling the nuclear chain reaction and holding the reactor subcritical. The number of different DOE reactor designs and the wide range of their missions means that the acceptance limits for these criteria can not be specific and that a large number of different and novel approaches may be used to meet these criteria. Additionally, small Category B reactors and critical assemblies with large negative feedback coefficients may be exempted from one or both of these design criteria.

(c) Reactivity Limits. The criterion in this section ensures that no reactivity accident will damage the reactor coolant boundary or impair the coolability of the reactor core. General guidance for meeting this criterion has been adapted from NUREG-0800, "Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants," different Section 4.6, "Functional Design of Control Rod System,". The different designs of the reactivity control systems and design features for DOE reactors means that specific lists of transients will need to be developed for each reactor type. The list accident to be analyzed should include all events which add positive reactivity to the system. These events would generally include:

- coolant temperature changes,

- control rod ejections (if possible), and

- system pressure changes.

(d) Control Room. A control room should be provided for all large category A nuclear reactor facilities. The control room environment will be protected to ensure that the reactor operators do not exceed the guidelines for occupational exposure given by DOE 5480.11, the Radiological Control Manual, and NRC

Regulatory Guide 8.8.

In addition, the control room should remain habitable during all AOEs and DBAs for the duration of the events. Thus, the control room, lighting and ventilation system should have backup emergency power to ensure habitability for the duration of postulated accidents. The control rooms should also have adequate shielding to ensure that no operator is exposed to more than the Radiological Control Manual limits for the duration of the accident.

(e) Remote Shutdown. All large Category A DOE reactors should have sufficient equipment and instrumentation outside the control room to bring the reactor to a safe, stable condition remotely. This redundant shutdown capability should be sufficiently remote from the reactor to ensure accessibility and operability during all AOEs and DBAs.

(6) Heat Removal Systems and Ultimate Heat Sink.

(a) Heat Removal Systems. Heat removal systems should be included in the reactor design to provide for sufficient heat dissipation such that core fuel temperature and reactor coolant system (RCS) pressure are maintained within acceptable limits during normal operating conditions and AOEs. The sources of heat that should be removed include decay heat, heat stored in the fuel and other structures, and heat generated by operating safety class SSCs. A number of different systems may be required to adequately dissipate the required heat loads. Typically, a reactor design will include the following systems for heat removal:

1 A system to provide RCS cooldown, following any reactor shutdown from normal operating conditions. This system should also include a means for long term decay heat removal to maintain the RCS in a cold shutdown condition.

2 A system to provide heat removal capability for all safety class structures, systems, and components. This system should have the capability to remove the total heat-load during all normal conditions and AOEs and transfer this heat to the ultimate heat sink (described below).

3 A system to provide makeup inventory to the RCS following small break loss of coolant accidents (LOCAs) and maintain adequate core cooling such that reactor conditions do not exceed acceptable safety limits (outlined below).

The makeup capability of this system should be sufficient to provide adequate cooling during events involving RCS inventory loss from pressure boundary leakages up to and including small pipe ruptures.

4 A system to provide RCS and core cooling following any loss of coolant event up to and including the rupture of the largest diameter piping system. This system should provide adequate coolant inventory to the RCS such that the following conditions are met:

- Acceptable reactor design limit are maintained
- The core geometry remains coolable for long term cooling
- Fuel-clad oxidation is not above prescribed limits (if applicable)
- Maximum amount of hydrogen generated is below acceptable limits (if applicable)

Although these cooling systems have different design conditions required by the wide range of operating conditions under which they should provide RCS cooling, certain functional characteristics are common to the designs. These character sties include:

a Suitable redundancy should be provided in the design such that system operation can be accomplished assuming any single failure. Analysis of system performance should be completed assuming that the most critical single failure has occurred.

b The components of each cooling system that are required for meeting the minimum system operating performance requirements should be designed and qualified as safety class equipment.

c System operation should be accomplished from the control room or control area with only limited operator actions required at remote locations.

d The functions of the cooling systems should not be shared with other facilities unless it can be shown that the design requirements for providing adequate cooling are not compromised by the interaction with other facilities.

e Components and sub-systems included in the

cooling system design may have design pressures lower than the design pressure of the RCS. Isolation capability should be provided to ensure that these sub-systems and components are protected from possible overpressurization through communication with the RCS at a higher pressure. Adequate isolation can be demonstrated through the use of one or more check valves in series with a motor-operated valve, two testable check valves in series, or three check valves in series.

f Pressure relief capability should be provided to protect the cooling systems from all credible overpressurization events. The relief capability should be determined in accordance with the ASME Boiler and Pressure Vessel code.

g The design and operation of all cooling system pumps should provide pump protection from overheating, cavitation, and loss of net. positive suction head.

h Computer codes used for design analysis and the analysis of cooling system performance during AOEs should have validation and verification described in IEEE Std 730-1984, "IEEE Standard for Software Quality Assurance Plans." This validation and verification should support the use of the code in each intended application. Specific recommendations on appropriate computer codes cannot be given due to the wide spectrum of reactor designs and applications affected by this Order. However, further guidance on the analysis of cooling system performance during loss of coolant accidents is provided in 10 CFR Part 50 Appendix K, "ECCS Evaluation Models" permitting the use of best estimate models.

i Adequate performance of the cooling systems should be determined by the fuel design limits.

j The analysis that supports the design of the various cooling systems should demonstrate that the limiting event has been identified and that a variety of single failures have been identified. In particular, for LOCA analysis, a variety of potential break locations should be evaluated.

NUREG-800, "USNRC Standard Review Plan," provides additional guidance on the evaluation of heat removal systems. The following sections

are particularly useful:

5.4.7 Residual Heat Removal (RHR) System
5.6 Emergency Cooling System
9.2.1 Station Service Water System
9.2.2 Reactor Auxiliary Cooling Water Systems

(b) Ultimate Heat Sink. The ultimate heat sink (UHS) provides a source of cooling for the dissipation of reactor decay heat and other essential plant heat loads following a normal reactor shutdown or a shutdown following an accident. These heat loads are transferred to the UHS by the plant cooling systems discussed previously in paragraph 3b(6) of this attachment. Of particular importance in the design of the UHS are the type of cooling water supply (i.e., passive natural or man made water body or cooling tower), the determination of the essential heat loads, and the environmental qualification of the critical system components required for effective heat load dissipation. Specific functional characteristics that should be considered in the design of the UHS systems are described in the following paragraphs. Guidance for the evaluation of UHS systems is provided in NUREG-800, "USNRC Standard Review Plan," Section 9.2.5, "Ultimate Heat Sink".

1 The total heat dissipation capability of the UHS should include conservative estimates of reactor decay heat, heat stored in reactor coolant system components and structures, and other heat sources removed by the cooling systems. This heat removal capability should be available during normal operation and following AOEs.

2 The UHS should have the capability to dissipate the maximum heat load described above for a period of time which ensures an adequate margin of safety. This capability should be analytically demonstrated to be available assuming the worst case environmental conditions including freezing. In addition, makeup to the water supply inventory should be accounted for only if it can be demonstrated that sufficient time and water inventory will be available before the UHS loses its cooling capability.

3 The UHS should be designed with sufficient component redundancy such that the heat removal safety function can be accomplished assuming a single active component failure coincident with the loss of offsite electrical power. Analysis should be available to demonstrate this single failure capability.

4 The function of the UHS can be shared with another facility if analysis indicates that this sharing does not compromise safe shutdown assuming a single failure.

5 The cooling function of this UHS system can be provided by cooling towers or the natural or man-made passive water sources (e.g., reservoirs, rivers or lakes). For the case of cooling towers, the structure should be designed to withstand the effects of natural phenomena including tornadoes, tornado missiles, hurricane winds, floods, and the design basis earthquake. In addition, it should be demonstrated analytically that the mechanical systems can withstand a single active failure including failure of any auxiliary electric power source and not prevent delivery of sufficient cooling water to maintain the plant in a safe shutdown condition. A technique suitable for this analysis is a Failure, Modes, and Effects Analysis (FMEA). IEEE Std. 353-1975, "Guide for General Principles of Reliability Analysis of Nuclear Power Generating Station Protection Systems," provides additional guidance on the preparation of FMEAs.

For the case of large natural or man-made water sources, analyses should demonstrate the adequacy of the water source assuming the effects of design basis natural phenomena. Assurance should be provided that a 30 day water supply is provided and can be maintained during these events.

(c) Inservice Inspection and Testing. In nuclear reactors, safety class SSCs are required to be designed, fabricated, erected, constructed, tested and inspected to quality standards commensurate with their importance to safety. ASME Section XI preservice and inservice inspection, testing, and repair and replacement provides requirements that form an acceptable basis for satisfying the inspection and testing requirements of this Order.

NSDC require in part that the subject systems be designed to permit appropriate periodic inspection and testing to ensure the structural integrity of its components and the operability and performance of the active components of the system. ASME section XI should be implemented to the extent practical within the limitations of existing design, geometry, and materials of construction of the components. New Category A reactor facilities should be designed and

constructed to enable the performance of testing and inspections in accordance with Section XI.

As used in this implementation guidance, reference to Section XI of the ASME Boiler and Pressure Vessel Code refers to Section XI, Divisions 1-Rules for Inspection and Testing of Components of Light-Water Cooled Plants, 2-Rules for Inspection and Testing of Components of Gas Cooled Plants and 3-Rules for Inspection and Testing of Components of Liquid-Metal Cooled Plants, the 1989 Edition with addenda through 1991. Code Cases contained in Regulatory Guide 1.147 may also be useful.

Section XI provides requirements for the preservice and periodic inservice inspections; pump, valve and snubber tests; pressure tests; and for the repair and replacement of pressure retaining components, including their integral attachments and component supports, classified as ASME Class 1, 2, and 3. 10 CFR Part 50.2, 10 CFR Part 50.55a(c), NRC Regulatory Guide 1.26 and Standard Review Plan Section 3.2.2 provide guidance for quality group classifications that may also be useful for DOE reactors. Additionally, risk-based classifications of components and systems may be utilized to ensure that components are inspected and tested commensurate with their importance to safety.

Inservice inspections, tests, and repairs and replacements conducted during the ten year inspection intervals should comply with the latest edition and addenda of the Code referenced in this implementation guidance 12 months prior to the start of the next inspection interval. Later editions and addenda of the Code that are incorporated by reference into this paragraph may be used subject to any limitations and modifications noted in this implementation guidance.

Proposed alternatives to Section XI may be utilized when authorized by the PSOs, when the Section XI Code requirements are impractical or would result in a hardship or unusual difficulty without a compensating increase in the level of quality and safety, or when the proposed alternatives provide an acceptable level of quality and safety.

Section XI contains the duties and qualification requirements for an Inspector (IWA-2100). The duties required to be performed by the Authorized Nuclear Inservice Inspector (ANII) may be performed by a group independent to those performing or overseeing the work, in lieu of an ANII, when allowed by the enforcement authority having jurisdiction at the plant

site. Additionally, Code Summary Reports should be prepared at the completion of a refueling outage, or annually for those facilities that do not have long outages corresponding to refueling outages and submitted to Program Secretarial Officers (PSOs). Other reporting requirements may be instituted at the direction of the PSOs.

PSOs, at their discretion, may apply this guidance where appropriate, to Category B reactors.

(7) Heating, Ventilation, and Air Conditioning (HVAC) Systems. The design professional should evaluate building HVAC systems and sub-systems and select major HVAC equipment components based on a consideration of health and safety requirements, initial costs, operating costs, and maintenance costs.

HVAC equipment should be sized to satisfy the building, heating and cooling load requirements and to meet all general equipment design and selection criteria contained in the ASHRAE Fundamentals handbook, ASHRAE Equipment handbook, ASHRAE Systems handbook, ASHRAE Applications handbook, and ASHRAE Refrigeration handbook. Calculations and equipment selection should be made according to the procedures given in ASHRAE GRP 158 and appropriate chapters of the ASHRAE Fundamentals handbook.

(a) Confinement Systems. The design of a confinement ventilation system should ensure the ability to maintain desired airflow characteristics when personnel access doors or hatches are open. When necessary, air locks or enclosed vestibules should be used to minimize the impact of this on the ventilation system and to prevent the spread of airborne contamination within the facility. The ventilation system design should provide the required confinement capability under all AOEs and DBAs with the addition of a single failure in the system.

If the maintenance of a controlled continuous confinement airflow is required, electrical equipment and components required to provide this airflow should be supplied with safety class electrical power and provided with an emergency power source.

Air cleanup systems should be provided in confinement ventilation exhaust systems to limit the release of radioactive or other hazardous material to the environment and to minimize the spread of contamination within the facility as determined by the safety analysis.

Guidance for confinement systems is included in DOE

6430.1A, section 1550.99

(b) Containment Systems. For reactors with a containment system, Regulatory Guide 1.140 presents guidance for design testing and maintenance for exhaust systems air filtration that is acceptable to the DOE. As with the confinement systems the basic criteria are based on the As Low As Reasonably Achievable (ALARA) concept given the present state of technology. 10 CFR Part 50, Appendix I presents specific methods and evaluation criteria that are acceptable to DOE in implementing ALARA with respect to exhaust systems from a containment system.

(c) Control Room. Key components of the HVAC systems for the control room and remote shutdown area should have sufficient emergency power to ensure that the control room remains habitable during design basis events. The NRC Regulatory Guide 1.52 provides design testing and maintenance criteria for adsorption and filtration equipment which are designed to operate during and after an accident.

(8) Fuel Handling and Storage and Radioactive Waste Storage.

(a) Fuel and Radioactive Waste Storage. Storage and handling of nuclear fuel requires that consideration be given to prevention of theft, criticality, protection from sabotage or physical damage, and receipt inspection. Wastes should be characterized by activity, half life, and chemical toxicity. The guidance contained in the American Nuclear Society standard, "Design Requirements for Light Water Reactor Spent Fuel Storage Facilities at Nuclear Power Plants," ANSI/ANS-57.2-1983 and the American Nuclear Society standard, "Design Requirements for New Fuel Storage Facilities at Light Water Reactor Plants," ANSI/ANS-57.3-1983 although written for light water reactor facilities is generally applicable to all water cooled DOE reactors, regardless of size. Additional guidance can also be obtained from NUREG-0800, Section 9.1.1, "New Fuel Storage," and Section 9.1.2, "Spent Fuel Storage. "

The American Nuclear Society standard, "Design Bases for Facilities for LMFBR Spent Fuel Storage in Liquid Metal Outside the Primary Coolant Boundary," ANSI/ANS-54.2-1985, provides guidance for the storage of fuel from sodium cooled reactors.

(b) Prevention of Criticality. A nuclear criticality safety analysis should be performed for each system that involves the handling, transfer or storage of fuel assemblies. The nuclear criticality safety

analysis should demonstrate that each system is subcritical under the design and operating limits specified for all plant conditions. The nuclear criticality safety analysis should include consideration AOEs, including:

1 Tipping or falling of a fuel assembly,

2 Tipping of a storage rack,

3 Misplacement of a fuel assembly,

4 Fuel drop accidents,

5 Stuck fuel assembly/crane uplifting forces,

6 Horizontal movement of fuel before complete removal from rack,

7 Placing a fuel assembly along the outside of the rack,

8 Object that may fall onto the stored assemblies, and

9 Missiles generated by failure of rotating machinery or generated by natural phenomena, as described in DOE Draft Order 5480.NPH, Natural Phenomena Hazards.

10 Control of heavy loads over the spent fuel pools.

The evaluated multiplication factor of fuel in storage racks under normal and AOEs should be equal to or less than an established maximum multiplication factor. Procedures for determining the limiting multiplication factor are given in detail in ANSI/ANS-8.1-1983, American National Criticality Safety in Operation with Fissionable Materials Outside Reactors.

(c) Monitoring of Fuel and Radioactive Waste Storage. Specific guidance is contained in the American Nuclear Society standard, "Design Requirements for Light Water Reactor Spent Fuel Storage Facilities at Nuclear Power Plants," ANSI/ANS-57.2-1983, Section 6.5. Although written for light water reactor facilities, this guidance is generally applicable to all water cooled DOE reactors, regardless of size.

The American Nuclear Society standard, "Design Bases for Facilities for LMFBR Spent Fuel Storage in Liquid Metal Outside the Primary Coolant Boundary," ANSI/ANS-54.2-1985, Section 4.4, provides guidance for

sodium cooled reactors.

(d) Residual Heat Removal Capability. The design of the residual heat removal system should be based on the maximum heat generation rate that would results from the maximum inventory of spent fuel assemblies, (including a full core discharge), and allowing for the burnup and post irradiation decay cooling time of fuel to be stored in the facility. Additionally, a redundant or backup system should be provided. Detailed specific guidance for water cooled reactors is given in the American Nuclear Society standard, "Design Requirements for Light Water Reactor Spent Fuel Storage Facilities at Nuclear Power Plants," ANSI/ANS-57.2-1983, Section 6.3, Cleaning and Cleanup Systems and NUREG-0800, Section 9.1.3, "Spent Fuel Pool Cooling and Cleanup System."

ATTACHMENT 4

SPECIAL DESIGN CRITERIA

CRITICAL ASSEMBLIES

AND

SPACE REACTORS

(TO BE PROVIDED)

U.S. Department of Energy
Washington, D.C.

PAGE CHANGE

DOE 5480.30 Chg 1

3-14-00

SUBJECT: NUCLEAR REACTOR SAFETY CRITERIA

1. PURPOSE. To transmit revised pages to DOE 5480.30, NUCLEAR REACTOR SAFETY CRITERIA, dated 1-19-93.

2. EXPLANATION OF CHANGE. To change the requirement in DOE 5480.30, NUCLEAR REACTOR SAFETY DESIGN CRITERIA, for EH concurrence with requested exemptions from the Order and update other EH responsibilities. These changes facilitate the Department's organizational transition necessitated by establishment of the NNSA.

3. FILING INSTRUCTIONS.

Remove	Dated	Insert	Dated
Pages 1-5	1-19-93	Pages 1-5	3-14-01
Page 6	1-19-93	Page 6	1-19-93
Att. 2, Page 3	1-19-93	Att. 2, Page 3	1-19-93
Att. 2, Page 4	1-19-93	Att. 2, Page 4	3-14-01

After filing the attached pages, this transmittal may be discarded.

SPENCER ABRAHAM
Secretary of Energy

DISTRIBUTION:
All Departmental Elements

INITIATED BY:
Office of Environment, Safety and Health