MASTER

1000 MWe

L M F B R

Liquid Metal Fast Breeder Reactor

FOLLOW-ON STUDY

WESTINGHOUSE ELECTRIC
TASK V REPORT
Safety Studies

DISTRIBUTION OF THIS DOCUMENT IS UNLIMITED

Prepared for ARGONNE NATIONAL LABORATORY

DISCLAIMER

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency Thereof, nor any of their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.

DISCLAIMER

Portions of this document may be illegible in electronic image products. Images are produced from the best available original document.

1000-MWe LMFBR FOLLOW-ON STUDY
TASK V SAFETY STUDIES

LEGAL NOTICE

This report was prepared as an account of Government sponsored work. Neither the United States, nor the Commission, nor any person acting on behalf of the Commission:
A. Makes any warranty or representation, expressed or implied, with respect to the accuracy, completeness, or usefulness of the information contained in this report, or that the use of any information, apparatus, method, or process disclosed in this report may not infringe privately owned rights; or
B. Assumes any liabilities with respect to the use of, or for damages resulting from the use of any information, apparatus, method, or process disclosed in this report.
As used in the above, "person acting on behalf of the Commission" includes any employee or contractor of the Commission, or employee of such contractor, to the extent that such employee or contractor of the Commission, or employee of such contractor prepares, disseminates, or provides access to, any information pursuant to his employment or contract with the Commission, or his employment with such contractor.

December 1968

APPROVED

E. F. Beckett
Project Manager

R. G. Hobson, Manager
Plant Engineering

Prepared by the Advanced Reactors Division Staff
Compiled by
R. G. Cockrell, Manager
Safety Systems and Licensing

Prepared for Argonne National Laboratory
Under Contract No. 31-109-38-2000

WESTINGHOUSE ELECTRIC CORPORATION
Advanced Reactors Division
P.O. Box 158
Madison, Pennsylvania 15663

This document is
PUBLICLY RELEASABLE

B. Steel
Authorizing Official

Date: 5-4-67

DISTRIBUTION OF THIS DOCUMENT IS UNLIMITED

CONTRIBUTORS

WARD

C. A. Anderson, Jr.
A. A. Bishop
N. M. Bonhomme
R. D. Burch
R. G. Cockrell
N. G. Farquhar
P. F. Fox
J. A. George
J. Graham
R. G. Hobson

I. M. Keyfitz
G. Macrae
R. A. Markley
P. I. Persson
C. E. Phillips
J. D. Sutherland
R. W. Tilbrook
N. C. Wampole
J. Zoubek

WPWR

J. Moore
R. Wieseemann

CONTENTS

	Page
GENERAL INFORMATION.....	1
Part 1. PRELIMINARY DESIGN SAFETY REVIEW.....	2
Introduction.....	3
Overall Plant Requirements.....	6
General Criterion: 1 Quality Standards.....	6
2 Performance Standards.....	8
3 Fire Protection.....	10
4 Sharing of Systems.....	12
5 Records Requirements.....	13
Core Protection and Containment.....	14
General Criterion: 6 Reactor Core Design.....	14
7 Suppression of Power Oscillations.....	16
8 Overall Power Coefficient.....	17
9 Reactor Coolant Boundary.....	18
10 Reactor Containment.....	20
Nuclear and Radiation Controls.....	23
General Criterion: 11 Control Room.....	23
12 Instrumentation and Control	
Systems.....	25
13 Fission Process Monitors and Controls..	26
14 Core Protection Systems.....	28
15 Engineered Safety Features Protection	
Systems.....	29
16 Monitoring Reactor Coolant Boundary....	30
17 Monitoring Radioactivity Releases.....	31
18 Monitoring Fuel and Waste Storage.....	32
Reliability and Testability of Protection Systems.....	33
General Criterion: 19 Protection Systems Standards and	
Reliability.....	33
20 Protection Systems Redundancy and	
Independence.....	34
22 Separation of Protection and Control	
Instrumentation Systems.....	36

CONTENTS (Continued)

	Page
23 Protection Against Multiple Disability for Protection Systems.....	37
24 Emergency Power for Protection Systems.	38
25 Demonstration of Functional Operability of Protection Systems.....	40
26 Protection Systems Fail-Safe Design....	42
Reactivity Control.....	44
General Criterion: 27 Redundancy of Reactivity Control.....	44
28 Reactivity Hot Shutdown Capability.....	45
30 Reactivity Shutdown and Holddown Capability.....	47
31 Reactivity Control Systems Malfunction.	49
32 Maximum Reactivity Worth of Control Rods.....	50
Reactor Coolant Boundary.....	51
General Criterion: 33 Reactor Coolant Boundary Capability....	51
34 Reactor Coolant Boundary Rapid Propagation Failure Prevention.....	53
36 Reactor Coolant Boundary Surveillance..	55
Engineered Safety Features.....	57
A. General Requirements.....	57
General Criterion: 37 Engineered Safety Features Basis for Design.....	57
38 Reliability and Testability of Engineered Safety Features.....	60
39 Emergency Power for Engineered Safety Features.....	62
40 Missile Protection.....	64
41 Engineered Safety Features Performance Capability.....	65
42 Engineered Safety Features Components Capability.....	67
B. Emergency Core Cooling.....	69
General Criterion: 44 Emergency Core Cooling Capability.....	69

CONTENTS (Continued)

	Page
45 (46 to 48) Inspection and Testing of the System which Provides Emergency Core Cooling.....	71
C. Containment.....	73
General Criterion: 49 Reactor Containment Design Basis.....	73
50 NDT Requirement for Containment Material.....	75
51 Reactor Coolant Boundary Outside Containment.....	76
52 Containment Heat Removal Systems.....	77
53 Containment Isolation Valves.....	78
54 (55) Containment Leakage Rate Testing.....	80
56 Provisions for Testing of Penetra- tions.....	82
57 Provisions for Testing of Isolation Waves.....	83
D. Containment Pressure-Reducing Systems	
General Criterion: 58 Inspection of Containment Pressure- Reducing Systems.....	84
59 (60) Testing of Containment Pressure- Reducing Systems Components.....	85
61 Testing of Operational Sequence of Containment Pressure-Reducing Systems..	86
E. Air Cleanup Systems.....	87
General Criterion: 62 (63 to 65) Inspection and Testing of Air Cleanup Systems.....	87
Fuel and Waste Storage Systems.....	89
General Criterion: 66 Prevention of Fuel Storage Criticality.	90
67 Fuel and Waste Storage Decay Heat.....	91
68 Fuel and Waste Storage Radiation Shielding.....	93
69 Protection Against Radioactivity Release from Spent Fuel and Waste Storage.....	95

GENERAL INFORMATION

This report presents the results of a preliminary safety study of the Westinghouse reference 1000-MWe Liquid-Metal Fast Breeder Reactor (LMFBR) power plant. This study was carried out during the Preliminary Plant Safety Study included under Task V of the 1000-MWe LMFBR Follow-On Study.

The study was divided into two major subtasks. Under one subtask, existing AEC general safety/design criteria were reviewed, similar LMFBR safety/design criteria were prepared, and the Westinghouse 1000-MWe reference concept was examined in the light of the LMFBR criteria. The results of this work are reported in Part 1; Part 2 contains a discussion of the rationale supporting any differences between the LMFBR criteria and the AEC general criteria.

Under the second subtask, a survey of malfunctions that could occur during operation of the reference concept was conducted. The results of this study are presented in Part 3 in the form of a safeguards table that identifies potential initiating conditions for reactor accidents, the accidents that might result, the potential consequences thereof, and the safeguards to reduce or avoid the consequences. The safeguards table is keyed to a fault-tree display that shows causality, consequences, and interrelationships, in graphic form.

Part 1

PRELIMINARY DESIGN SAFETY REVIEW

INTRODUCTION

A set of general design criteria applicable to LMFBR Plants was prepared. The design criteria were based upon design experience gained on the 1000-MWe LMFBR Follow-On Study Program and other Westinghouse programs, and upon a review of the AEC's

"General Design Criteria for Nuclear Power Plant Construction Permits proposed as Appendix A of Part 50 of the AEC's regulations published in the Federal Register on July 11, 1967".

For each of the general LMFBR design criteria, there were prepared specific criteria with which the 1000-MWe reference concept design must comply in order to meet the general criteria*; the rationale supporting the selection of the specific criteria has been stated. Finally, there is a discussion for each criterion to show how the 1000-MWe reference concept meets, or can be designed to meet the criterion.

LMFBR GENERAL DESIGN CRITERIA

There are 70 AEC General Design Criteria, all of which predominantly reflect water-cooled thermal reactor experience. There is no reason why a set of criteria for liquid-metal-cooled fast reactors should have the same number. However, in order to make comparisons later (Part 2), the same titled subsections were retained, and an equivalent numbering system was used.

It is worth pointing out that any such set of general design criteria must contain indeterminate qualitative adjectives (e.g. "undue risk", "very low probability", "excessive radiation") that will later require exact definition in specific criteria for any particular system. At this later stage too, areas of uncertainty must be identified, and appropriate safety weightings made.

* This treatment of the general criteria and associated specific criteria follows the example set by Section II Principal Safety and Design Criteria of the Preliminary Safety Analysis Report for the Argonne Advanced Research Reactor (AARR), issued April 10, 1967. However, the specific AARR Criteria included in the document were prepared after completion of Title I design of AARR, and are therefore more detailed than the specific 1000-MWe Criteria which are based on the 1000-MWe conceptual design studies.

Each criterion has been categorized as Category A or Category B, following the precedent set by the AEC General Design Criteria. Experience has shown that more definitive information is needed at the construction permit stage for the items listed in Category A than for those listed in Category B.

Some of the LMFBR general criteria differ from the AEC general criteria only in detailed wording. Others are amalgams of previous criteria; this will be apparent from the numbering. However, some criteria differ substantially, and the rationale for these differences are given in Part 2.

1000-MWE SPECIFIC CRITERIA

The 1000-MWe plant is not yet at a development stage at which all design criteria can be stated explicitly. Until the project is further advanced, for example, hardware quality controls, while they will eventually be of high standard, are at present of academic interest. Also, there is reluctance at this stage of development to state quantitative limits in the criteria, since in most cases there is not sufficient analytical and/or experimental information to justify the setting of quantitative limits. For example, it is not possible at this time to be specific about fuel performance conditions consistent with public health and safety protection. In the conceptual design studies, the limits placed on certain core parameters (e.g. fuel cladding surface temperature) are within the range of values considered safe for operating the reactor under normal conditions. However, further work is required to determine the conditions under which fuel failure becomes highly probable, and thus to set the bounds of acceptable fuel performance conditions.

RATIONALE SUPPORTING SELECTION OF THE 1000-MWE CRITERIA

The specific criteria were required to at least cover the intent of the general criteria. In a few cases, it was necessary to repeat the general criteria, because at this stage of development, it was not possible to be more specific. In these few cases, the reason for repeating the general criteria was to be consistent and to indicate that the 1000-MWe plant will be designed to comply with the intent of the general criteria. In areas common to water reactors, the criteria are based upon current Westinghouse pressurized water reactor experience. Finally, where adequate conceptual design work has been done, the criteria were based on this experience.

COMPLIANCE WITH THE 1000-MWE CRITERIA

This section was prepared for each of the criterion to show how the 1000-MWe reference concept meets, or can be designed to meet, the criterion. In attempting to prepare compliance statements corresponding to the specific criteria, a dilemma arose because in many cases it was difficult to distinguish a statement of compliance from a criterion. For instance, consider the two extremes of the dilemma. One might prepare a comprehensive list of specific criteria; he then needs only to state that the design meets or will be designed to meet the criteria. In the other extreme, he

may state the general criteria and put all necessary details in the compliance section.

The first case is undesirable at this stage of development because there is not sufficient information upon which to base such detailed criteria. The other extreme is more desirable because it places the specifications in a position of informing rather than demanding. Furthermore, when a specification assumes the role of a criterion, it becomes less amenable to revision because, if a criterion is to be a standard, the design must be changed, as necessary, to conform to the criterion. Therefore, it is important that careful consideration be given to the selection of criteria if they are to satisfy some desired objective without placing unnecessary constraints on the design.

A compromise between the two extremes was sought when preparing the sections on 1000-MWe criteria and on compliance. If there was reason to believe that a specification would place unnecessary constraints on the design, or if there was insufficient information to give a satisfactory technical basis for a specific criterion, then the specific criterion was stated in more general terms or, in some cases, the general criterion, itself, was as specific as the current design status will permit. In all cases, the 1000-MWe reference LMFBR plant meets, or can be designed to meet the intent of the general design criteria.

OVERALL PLANT REQUIREMENTS

GENERAL CRITERION 1: QUALITY STANDARDS

Those systems and components of reactor facilities which are essential to the prevention, or the mitigation of consequences, of nuclear accidents which could cause undue risk to the health and safety of the public shall be identified and then designed, fabricated, and erected to quality standards that reflect the importance of the safety function to be performed. Where generally recognized codes and standards pertaining to design, materials, fabrication and inspection are used, they shall be identified. Where adherence to such codes or standards does not suffice to assure a quality product in keeping with the safety function, they shall be supplemented or modified as necessary. Quality assurance programs, test procedures, and inspection acceptance levels to be used shall be identified. A showing of applicability of codes, standards, quality assurance programs, test procedures, and inspection acceptance levels used is required. Where such items are not covered by applicable codes and standards, a showing of adequacy is required. (Category A)

1000-MWe Criteria

- 1.1 The requirements stated in General Criterion 1 will be met.
- 1.2 Where recognized codes or standards on design, materials, fabrication and inspection are used, they will be identified. The following specific codes, standards, and regulations shall apply where applicable:

United States Atomic Energy Commission - Code of Federal Regulations - Title 10

ASME Section I - Power Boilers
ASME Section II - Materials Specifications
ASME Section III - Nuclear Vessels
ASME Section VIII - Unfired Pressure Vessels
ASME Section IX - Welding Qualifications
ASTM American Society for Testing Materials
ASA American Standards Association
AISC American Institute of Steel
TEMA Tubular Exchanger Manufacturers Association
NEMA National Electrical Manufacturers Association
NFPA National Fire Protection Association Publication

ACI American Concrete Institute
AWS American Welding Society
ISA Instrument Society of America
AEC Cost Evaluation Handbook (for direct construction costs) where applicable

Rationale Supporting the Selection of the 1000-MWe Criteria

In Criterion 1.2, certain codes are listed because they are specifically designated in the contract.

Compliance with the 1000-MWe Criteria

All systems and components of the facility will be classified according to their importance. Those items vital to safe shut down and isolation of the reactor, or whose failure might cause or increase the severity of the core meltdown accident or the sodium fire accident or result in an uncontrolled release of excessive amounts of radioactivity, are designated Class I. Those items important to reactor operation, but not essential to safe shutdown and isolation of the reactor or control of the release of substantial amounts of radioactivity, will be designated Class II. Those items not related to reactor operation or safety will be designated Class III.

Class I systems and components are essential to the protection of the health and safety of the public. Consequently, they will be designed, fabricated, inspected, and erected, and the materials selected to the applicable provisions of recognized codes, good nuclear practice, and to quality standards that reflect their importance. Since the 1000-MWe LMFBR is still in the conceptual stage, the full extent of applicable codes and standards, quality assurance programs, test provisions, etc., have yet to be determined.

GENERAL CRITERION 2: PERFORMANCE STANDARDS

Those systems and components of reactor facilities which are essential to the prevention or to the mitigation of the consequences of accidents which could cause undue risk to the health and safety of the public shall be designed, fabricated, and erected to performance standards that will enable such systems and components to withstand, without undue risk to the health and safety of the public, the forces that might be imposed by natural phenomena such as earthquake, tornado, flooding condition, wind, or ice. The design basis so established shall reflect: (a) appropriate consideration of the most severe of these natural phenomena that have been recorded for the site and the surrounding area, and (b) appropriate margin for withstanding forces greater than those recorded to reflect uncertainties about the historical data and their suitability as a basis for design. (Category A)

1000-MWe Criterion

2.1 The requirements stated in General Criterion 2 will be met.

Rationale Supporting the Selection of the 1000-MWe Criterion

The general criterion is as specific as can be at this stage of the plant design and site selection.

Compliance with the 1000-MWe Criterion

All components and supporting structures of the reactor containment will be designed so that there is no loss of function of such equipment in the event of maximum potential ground acceleration acting simultaneously in the horizontal and vertical directions.

The reactor containment is defined as a Class I structure for purposes of seismic design. Its structural members will have sufficient capacity to accept, without exceeding specified stress limits, a combination of normal operating loads, functional loads due to a core meltdown and compaction accident, and the loading imposed by the maximum potential earthquake.

All electrical systems and components vital to plant safety, including the emergency diesel generators, will be designed as Class I and designed so that their integrity is not impaired by the maximum potential earthquake, wind storms, floods, or disturbances on the external electrical system.

Power, control and instrument cables, motors, and other electrical equipment required for operation of the engineered safety features will be suitably protected against the effects of either a nuclear system accident or of severe external environmental phenomena in order to assure a high degree of confidence in the operability of such components in the event that their use is required.

All piping, components, and supporting structures of the reactor coolant system are designed as Class I equipment, i.e. they are capable of withstanding:

- a. within code-allowable working stresses for the design seismic ground acceleration, and
- b. the maximum potential seismic ground acceleration acting simultaneously in the horizontal and vertical direction with no loss function.

GENERAL CRITERION 3: FIRE PROTECTION

A reactor facility shall be designed to minimize the probability of events such as fires and explosions and the potential consequences of such events and thus to ensure no undue risk to the health and safety of the public. Noncombustible and fire resistant materials shall be used wherever practical to preclude such risk throughout the facility, particularly in areas containing critical portions of the facility such as containment, control room, and components of engineered safety systems. (Category A)

1000-MWe Criteria

- 3.1 The reactor containment building, its contents, and all associated facilities will be constructed from noncombustible and fire resistant materials wherever practical, to minimize the risk of fire.
- 3.2 Fire detection systems acting upon the presence of heat and/or smoke will provide audible and visible warnings of the presence of fire.
- 3.3 No water, or other chemicals that react exothermically with sodium, will be used for fire protection inside the reactor containment building, where contact with sodium is even a remote possibility.
- 3.4 Inert gas will be used in the containment. (See Criterion 37.1)

Rationale Supporting the Selection of the 1000-MWe Criteria

The specific criteria are a restatement of the general criterion with particular emphasis on minimizing the probability or consequences of a sodium fire.

Compliance with the 1000-MWe Criteria

The reactor containment system will be designed to maintain its capability in case of fire, to safely shut down and isolate the reactor.

The containment and auxiliary building ventilation systems will be operable from the control room. Smoke or flame (ionization) detectors and control room alarms will be provided for each ventilation system.

Fire prevention in all areas of the nuclear-electric plant will be provided by structure and component design that optimizes the containment of combustible materials and maintains exposed combustible materials below their ignition temperature in the design atmosphere. Fire control requires the capability to isolate or remove fuel from an igniting source, or to reduce the combustibles' temperature below the ignition point, or to exclude the oxidant, and preferably, to provide a combination of the three basic control means. The latter two means are fulfilled by providing fixed or portable fire fighting equipment of capacities proportional to the energy that might credibly be released by fire. Also, during power and refuelling operations, the containment is inerted, thus eliminating the possibility of oxidation reaction. At any time when air is introduced into the containment, all possible sources of sodium will be secured.

The fire protection system will have the design capability to extinguish any probable combination of simultaneous non-sodium fires that might occur at the station without unnecessarily endangering operating personnel. The means will be available to extinguish any sodium fire that would endanger the public.

The system will be designed in accordance with the standards of the National Fire Protection Association, and is based generally on the recommendations of the Nuclear Energy Property Insurance Association (FIA).

GENERAL CRITERION 4: SHARING OF SYSTEMS

Reactor facilities may share systems or components if it is shown that such sharing will not result in undue risk to the health and safety of the public.
(Category A)

1000-MWe Criteria

- 4.1 Reactor facilities may share systems or components, such as instrumentation, control, safeguard and protective systems if it is shown that such sharing will not result in undue risk to the health and safety of the public.

Rationale Supporting the Selection of the 1000-MWe Criteria

The specific criteria merely restates General Design Criterion 4, but with examples given to be more specific and to add clarity and emphasis to the importance of the criterion.

Compliance with the 1000-MWe Criteria

Due to the preliminary state of the design, the full extent of the component sharing cannot be determined. When the design becomes more defined, analyses will be carried out to assure and confirm that the sharing of components among systems does not result in interference with the basic function and operability of the systems, and hence, result in undue risk to the health and safety of the public.

GENERAL CRITERION 5: RECORDS REQUIREMENTS

The reactor licensee shall be responsible for assuring the maintenance, throughout the life of the reactor, of records of the design, fabrication, and construction of major components of the plant essential to avoid undue risk to the health and safety of the public.
(Category A)

1000-MWe Criteria

5.1 The reactor licensee will be responsible for the following:

- a. the maintenance throughout the life of a complete set of as-built facility plant and system diagrams, including arrangement plans and structural plans;
- b. the maintenance of a set of completed test procedures for all plant testing; and
- c. seeing that a set of all the quality assurance data generated during fabrication and erection of the essential components of the plant are maintained.

Rationale Supporting the Selection of the 1000-MWe Criteria

The specific criteria are based on current practice with commercial nuclear power plants.

Compliance with the 1000-MWe Criteria

Development of a set of record requirements was beyond the scope of the 1000-MWe conceptual design studies. In general, equipment specifications will require record retention as required by applicable codes or Westinghouse. No unusual problems are anticipated in this area.

CORE PROTECTION AND CONTAINMENT

GENERAL CRITERION 6: REACTOR CORE DESIGN

The reactor core, with its related control and protection system, shall function throughout its design lifetime, without exceeding fuel performance conditions consistent with public health and safety protection. The core design, together with reliable process and decay heat removal systems, shall provide for this capability under all expected conditions of normal operation with appropriate margins for uncertainties and for transient situations which can be anticipated, including the effects of the loss of power to circulation pumps, tripping out of a turbine-generator set, isolation of the reactor from its primary heat sink, and loss of all off-site power.
(Category A)

1000-MWe Criteria

- 6.1 The core and blanket of the reactor, together with control rods and drives, shall operate throughout reactor life without damage to the fuel, bond, cladding, support structure, control rods, or flow paths that would endanger public health and safety. The design of the reactor, reactivity control system, and cooling system shall provide for such operation by use of appropriate nuclear and engineering hot-channel factors, a realistic over-power allowance, allowance for credible component malfunction or failure, allowance for loss of motive power to the primary or secondary coolant pumps, and allowance for all credible load changes.
- 6.2 The design of the reactor vessel internals, reactor vessel, and the containment around the reactor vessel will be such that a complete loss of sodium coolant flow through the core will not occur as a result of any credible accident, including a rupture in the primary coolant boundary; cooling, with adequate heat removal, will be maintained.

Rationale Supporting the Selection of the 1000-MWe Criteria

The ultimate objective cited is to not endanger public health and safety. This places limits on allowable damage to fuel, cladding, and internals. These limits correspond to specific numerical values of parameters, such as temperature, that are usually dependent on past history and on the

specific conditions (e.g. accidents) that could cause the limits to be exceeded. In order to analyze a sequence of events that could lead to an accident, conservative numerical values must be assigned to those parameters.

In order to ensure that the reactor design does not exceed the fuel performance conditions cited in General Criterion 6, the numerical values assigned to important parameters must be based on realistic analyses. Thus, design calculational errors and uncertainties must all be included in the hot channel factors. The design itself must enable the reactor to tolerate all credible malfunctions, failures, flow losses, and load changes, so as to be consistent with public health and safety criteria.

Compliance with the 1000-MWe Criteria

The four-module core and blanket arrangement was selected to reduce the reactivity increase upon voiding of a core and axial blanket to a value less than that which would result for a reactor design constrained only by thermal-hydraulic considerations. Instead of \$10.40 for such a reactor, the reactivity change for voiding of core and axial blanket of one module of the reference reactor is \$0.50. The reference reactor design could be further modified to provide a negative or zero reactivity change on voiding of core and axial blanket; but, considering the probable error of the present calculation, this has not been deemed worthwhile.

Many additional design features have great potential for satisfying Criterion 6. In some instances, compliance with Criterion 6 is obvious; however, in other instances, detailed analyses and experiments will be required to determine net trade-off in regard to Criterion 6. For example, no cans are used to enclose fuel assemblies. This design feature prevents flow blockage in an assembly from causing gross fuel assembly meltdown, because cross flow from adjacent fuel assemblies cools the blocked fuel assembly. It is impossible to state without detailed analyses and experiments whether uncanned fuel assemblies serve to inhibit rod bowing. The fuel rods are vented, reducing the probabilities of loss of sodium bond and gas blanketing of adjacent fuel rods if a fuel rod cladding failure occurs.

Two separate cooling loops provide reliable primary heat removal. Two separate reactivity control systems are employed. Containment around the reactor pressure vessel prevents complete loss of coolant if a leak or rupture occurs in the vessel. Operating experience with thermal reactors and comparison with industrial practice shows Westinghouse hot channel factors to be realistic. An overpower condition was considered in the design to determine peak fuel temperature.

As discussed above, there are some areas of the reactor core design that may or may not meet Criterion 6. Further information is needed to ensure that the criteria can be met, relating to fission product gas entrainment in the coolant, sodium bond behavior, and failure propagation between fuel rods. Additional information is also needed on coupled space - time reactor kinetics.

GENERAL CRITERION 7: SUPPRESSION OF POWER OSCILLATIONS

The design of the reactor core and related control and protection systems shall ensure that power oscillations which could cause fuel conditions in excess of limits consistent with public health and safety protection are not possible or can be readily suppressed. (Category B)

1000-MWe Criterion

- 7.1 The design of the core and blanket of the reactor, together with the primary coolant loops, vessel internal structures, and reactivity control systems, will be such as to prohibit power oscillations of sufficient magnitude to endanger public health and safety.

Rationale Supporting the Selection of the 1000-MWe Criterion

There is a clearer rationale for Criterion 7 for PWRs, where xenon-induced spatial instabilities are a common problem, than for LMFBRs. Because of our use of a modular core and because of the lack of suitable coupled space-time analytical techniques, this criterion has been written to ensure consideration of power oscillations if future study reveals that such oscillations are a problem.

Compliance with the 1000-MWe Criterion

Monitoring and control of local reactor regions, or modules, will help the operator observe and control power oscillations should they occur. Calculations performed to date indicate stability for reactors of this type, but more precise neutron kinetics calculations are needed to properly assess the possibility of power oscillations. Experiments will be needed to verify these calculations.

The mechanical design includes provisions to restrict bowing (temperature compensated strongbacks) and vibration (welded structures). This should prevent large positive structural contributions to the power coefficient. Until experimental verification of the design is made, however, the structural coefficient of reactivity cannot be accurately predicted.

GENERAL CRITERION 8: OVERALL POWER COEFFICIENT

The overall net reactivity change associated with a rapid increase in power in the power operating range shall not be positive. (Category B)

1000-MWe Criterion

- 8.1 In the power operating range, the reactivity change associated with a rapid increase in power shall not be positive. A "rapid" power increase is one that is more rapid than can be readily opposed by the action of one of the two reactivity control systems.

Rationale Supporting the Selection of the 1000-MWe Criterion

The specification "in the power operating range" is made because it is conceivable that a reactor could be safer if designed with a negative power coefficient in the operating range and a positive power coefficient elsewhere rather than designed with a smaller negative power coefficient at all power levels.

The definition of "rapid" is made to ensure that a delayed positive reactivity coefficient can be overcome by control rod action, and that situations too rapid for the control rods to control will be overcome by the inherent prompt negative power coefficient.

Compliance with the 1000-MWe Criterion

The power coefficient for the reference design reactor is negative from zero power to well in excess of full power for any rate of change of power.

The sodium expansion coefficient and Doppler coefficient combine to give a power coefficient of -0.07 c/MW .

GENERAL CRITERION 9: REACTOR COOLANT BOUNDARY

The reactor primary coolant boundary shall be designed and constructed so as to have a very low probability of gross rupture or abnormal leakage throughout its design lifetime. (Category A)

1000-MWe Criteria

- 9.1 The reactor vessel and all primary pipework will be designed to accept all operational loads and anticipated transient conditions imposed by the plant.
- 9.2 Thermal and neutron irradiation will be limited, by the design of suitable shielding, to values at which the vessel and pipework will be capable of fulfilling their functional requirements with a very low probability of leakage throughout their design lifetime.

Rationale Supporting the Selection of the 1000-MWe Criteria

Criterion 9 is concerned with the requirement that the coolant boundary be designed to withstand leakage or rupture anywhere. In the original (1967) AEC criteria, this criterion was concerned with the requirement that the vessel and primary pipe work should be designed to contain the pressure of the system (PWR); but, here we are merely concerned with the containment of coolant and, to a lesser extent, the containment of cover gas pressure. The specific criteria were written to ensure that design specifications should include limits on structural integrity, thermal and radiation conditions, together with an adequate inspection program. Quantitative definition of structural design limits, irradiation limits, and inspection extent and frequency will need to be specified in the Title I design.

Compliance with the 1000-MWe Criteria

Each component of the reactor coolant boundary, that is, reactor vessel, intermediate heat exchanger (IHx), primary coolant pumps and check valves shall be designed, constructed, and tested in accordance with the applicable specifications and recognized commercial practice. The major specifications are, Nuclear Pressure Vessels, Section III of the American Society of Mechanical Engineers Boiler and Pressure Vessel Code and the Nuclear Piping Code.

The complete reactor coolant system shall be designed in accordance with the above codes. Due consideration will be given to the applied loads from fluid pressure, dead weight, and thermal expansions. Material physical properties will be based on specific materials, design temperatures, number of stress reversals, integrated neutron flux, and environment.

Equipment will be adequately supported for the imposed loads to keep deflections within acceptable limits and prevent deleterious vibrations. However, the design will be such as not to impose excessive stresses from thermal expansions.

The equipment will be manufactured by experienced suppliers in accordance with the final drawings and specifications. Sufficient inspection and testing of the equipment shall be performed by competent inspectors and engineers to assure compliance within the design and specifications and suitability for its intended function.

All components of the primary coolant system boundary will be erected and installed by competent construction workers and millwrights. To the extent practical welding will be full penetration welds, and will be inspected in conformance with the applicable codes.

In view of the above careful design, inspection, and construction, the probability of gross rupture or leakage of the primary coolant boundary is extremely low.

GENERAL CRITERION 10: REACTOR CONTAINMENT

Reactor containment or equivalent protection shall be provided. The containment structure shall be designed (a) to sustain the effects of the worst credible core meltdown accident; and (b) to sustain the effects of the most severe credible radioactive sodium reaction and, together with other engineered safety features as long as the situation requires, the functional capability of the containment to the extent necessary to avoid undue risk to the health and safety of the public.

1000-MWe Criteria

- 10.1 The reactor and primary coolant system will be entirely enclosed within the reactor containment building.
- 10.2 The containment building will be designed to withstand the calculated peak pressure and temperature that could occur as a result of a sodium fire accident or a core meltdown accident which will be the Design Basis Accidents.
- 10.3 The design of any containment building penetration, air lock, pipework, etc., will conform to the applicable codes and standards to insure containment integrity under accident design temperature and pressure.
- 10.4 The design will accommodate earthquake loadings, high winds, and any environmental loadings that the site might make necessary, in addition to normal static loads.
- 10.5 A sodium-air reaction, i.e. sodium fire, associated with either the IHX vault or the upper containment structure, will be a Design Basis Accident for these areas. In the IHX vault, the fire surface will be assumed to cover the floor. The fire surface for the upper containment is assumed to be the same as the reactor and fuel storage area. Also, the most severe credible core meltdown accident leading to high reactivity insertion will be a Design Basis Accident for the containment.

Rationale Supporting the Selection of the 1000-MWe Criteria

The primary loop must be contained because the sodium in this loop is very radioactive and therefore, must not be allowed to escape following an accident. The secondary loop is permitted to penetrate the containment building only because sufficient shielding will be provided to keep the activity at a low level.

The containment must not only protect the public from internal accident effects, but must protect the reactor system from all external disturbances that could upset the normal operation of the system and cause an internal accident condition to arise, or aggravate an internal accident condition.

The Credible Design Basis Accident (CDBA) is an uncontrolled accident that is credible in the sense that a finite number of events -- including failure of the safety system -- all credible, could initiate it; but, which is nevertheless of low probability. Normally this class of accident might be expected to occur once in several reactor lifetimes. For example, during a reactor shutdown period, air may be introduced into the containment for extended maintenance.

It is conceivable that a coolant pipe could be broken or that, due to an operation error, the reactor plug or spent fuel cover could be removed. Both cases would lead to a sodium fire, a CDBA.

A partial core meltdown and compaction accident is also a Credible Design Basis Accident, and the worst credible case will be considered. The definition of the extent of the worst credible case requires further failure propagation analysis and experimentation.

Compliance with the 1000-MWe Criteria

The final design of the containment will be produced by the architect-engineer to comply with the 1000-MWe criteria when calculated peak pressures and temperatures have been finally specified. See Compliance to Criterion 49 for the design basis of the containment.

The Credible Design Basis Accidents, as defined, will be analyzed with a degree of pessimism consistent with the uncertainties involved. In the partial core meltdown accident, the largest possible reactivity insertions, as yet undefined, will be used together with a value of the Doppler coefficient taking calculational inaccuracies into account. The partition of the resulting energy will employ the reactor vessel as a first energy absorbing barrier.

A sodium fire using the worst spill configuration in the IHX vault and/or the upper containment volume will be used.

Present calculated peak pressures and temperature are 30 psig and 500°F; but, as the design proceeds, these figures may change, and the containment design requirements will be modified to accommodate the changes. The containment building will be designed to withstand the pressure and temper-

ature in accordance with applicable codes and standards (See Criterion 1.2) to ensure integrity.

A site has not been chosen, although a representative site (Middletown) is used in the design. Seismic data indicating horizontal and vertical accelerations as additional loadings will be used in the structural design of the containment building.

NUCLEAR AND RADIATION CONTROLS

GENERAL CRITERION 11: CONTROL ROOM

The facility shall be provided with a control room from which actions to maintain safe operational status of the plant can be controlled. Adequate radiation protection shall be provided to permit continuous occupancy of the control room under any credible post-accident condition or as an alternative, access to other areas of the facility as necessary to shut down and maintain safe control of the facility without excessive radiation exposures of personnel. (Category B)

1000-MWe Criteria

- 11.1 The requirements stated in General Criterion 11 will be met.
- 11.2 The control room will be designed to permit occupancy by the operators, without hazard or being subject to doses which in aggregate would exceed the suggested limits in 10 CFR 100, under postulated accident conditions, including the sodium fire accident and the core meltdown accident.

Rationale Supporting the Selection of the 1000-MWe Criteria

The specific criterion extends the range of accidents from which the control room operators must be protected to sodium fires and other Credible Design Basis Accidents. (See Criterion 49)

Compliance with the 1000-MWe Criteria

The plant will be equipped with a control room that will contain all controls and instrumentation necessary for operation of the reactor and turbine-generator under normal and accident conditions.

The control room will be capable of continuous occupancy by the operating personnel under all normal operating conditions within limits set by 10 CFR 20.

Sufficient shielding, distance, and containment integrity will be provided to assure that control room personnel shall not be subject to doses under postulated accident conditions during occupancy of the control room which, in the aggregate, will exceed 0.1 of the suggested limits of 10 CFR 100. The control room ventilation will consist of a system having a large percentage of recirculated air. The fresh air intake can be closed to control the intake of airborne activity if monitors indicate that such action is appropriate.

GENERAL CRITERION 12: INSTRUMENTATION AND CONTROL SYSTEMS

Instrumentation and controls shall be provided, as required, to monitor and maintain system variables within specified operational ranges to ensure no undue risk to the health and safety of the public at all times. (Category B)

1000-MWe Criterion

12.1 The requirements stated in General Criterion 12 will be met.

Rationale Supporting the Selection of the 1000-MWe criterion

The general criterion follows current Westinghouse commercial practice.

Compliance with the 1000-MWe Criterion

Instrumentation and controls will be provided to monitor and maintain neutron flux, primary coolant pressure, flow rate, temperature, and control rod positions within prescribed operating ranges.

The non-nuclear regulating process and containment instrumentation will measure temperatures, pressure, flow, and levels in the primary and secondary coolant systems, steam systems, containment and other auxiliary systems. Process variables required on a continuous basis for the startup, operation, and shutdown of the plant will be indicated and recorded; shutdown of the plant will be indicated, recorded, and controlled from the control room into which access is supervised. The quality and types of process instrumentation provided will ensure safe and orderly operation of all systems and processes over the full operating range of the plant.

GENERAL CRITERION 13: FISSION PROCESS MONITORS AND CONTROLS

Means shall be provided for monitoring and maintaining control, at a frequency consistent with anticipated rates of change, over the fission process throughout core life and for all conditions that can reasonably be anticipated to cause variations in reactivity, such as the indication of position of control rods. (Category B)

1000-MWe Criteria

- 13.1 The requirements stated in General Criterion 13 will be met.
- 13.2 The nuclear instrumentation system will be designed to monitor and control the reactor power, taking into account spatial variations due to the modular nature of the core.
- 13.3 The control of individual core modules will be to the same standards as would apply to a single-module core.

Rationale Supporting the Selection of the 1000-MWe Criteria

The specific criteria extend to each module of a multi-module core the same standards of monitoring and control as would apply to a single-module core.

Compliance with the 1000-MWe Criteria

The nuclear instrumentation system will be provided to monitor the reactor power from source range through the intermediate range and power range up to 120% of full power; the ranges will overlap by at least a decade. The system will provide indication, control, and alarm signals for reactor operation and protection.

The operational status of the reactor will be monitored from the control room. When the reactor is subcritical (i.e., during cold or hot shutdown, refueling and approach to criticality), the relative reactivity status (neutron source multiplication) will be continuously monitored and indicated by fission counters located in thimbles in the lower axial blanket. One source-detector channel per module will be provided for supplying information on multiplication while the reactor is subcritical. A reactor trip will be actuated from either channel if the neutron flux level should become

excessive. This system will be checked prior to operations in which criticality could be approached. This will be accomplished by the use of the spontaneous fission of Pu 240 in the fuel to provide a meaningful count rate even at the refueling shutdown condition. Any appreciable increase in the neutron source multiplication will be slow enough to give ample time to start corrective action to prevent the core from becoming critical.

When the reactor can be critical, means for showing the relative reactivity status of the reactor and modules will be provided by control bank positions displayed in the control room. The position of the control banks will be directly related to the reactivity status of the reactor when at power. Any unexpected change in the position of the control banks under automatic control or change in the coolant temperature under manual control will provide a direct and immediate indication of a change in the reactivity status of the reactor.

High nuclear flux protection will be provided both in the power and intermediate ranges by reactor trips actuated from either range if the neutron flux level should exceed trip set points. When the reactor can be critical, the best indications of the reactivity status in the core and modules (in relation to the power level and average coolant temperature) will be the control room display of the rod control group position.

GENERAL CRITERION 14: CORE PROTECTION SYSTEMS

Core protection systems, together with associated equipment, shall be designed to prevent or to suppress conditions that could result in exceeding acceptable fuel performance conditions. (Category B)

1000-MWe Criteria

- 14.1 The requirements stated in General Criterion 14 will be met.
- 14.2 The core protection systems will be designed to take account of the modular nature of the core and to consider spatial power variations when assessing an approach to unacceptable fuel conditions.

Rationale Supporting the Selection of the 1000-MWe Criteria

The specific criteria extend to each module of a multi-module core the same standard of protection as would apply to a single-module core.

Compliance with the 1000-MWe Criteria

Instrumentation and controls provided for the protective systems will be designed to trip the reactor when necessary to limit fission product release from the core to that normal for vented fuel; to limit energy release; to signal closure of containment isolation valves; and to control the operation of engineered safety features equipment.

During reactor operation in the startup and power modes, redundant safety limit signals will automatically actuate two reactor trip breakers that are in series with the rod drive mechanism coils. This action will interrupt power and initiate reactor trip. This criterion, as applied to the Reactor Protection System, is discussed more fully under the discussion of the criterion on Protection Systems Failure Analysis Design.

GENERAL CRITERION 15: ENGINEERED SAFETY FEATURE PROTECTION SYSTEMS

Protection systems shall be provided for sensing accident situations and initiating the operation of necessary engineered safety features. (Category B)

1000-MWe Criterion

15.1 The requirements stated in General Criterion 15 will be met.

Rationale Supporting the Selection of the 1000-MWe Criterion

The general criterion follows current Westinghouse commercial practice.

Compliance with the 1000-MWe Criterion

The reactor protection system will receive, from plant instrumentation, signals that will be indicative of an approach to an unsafe operating condition, actuate alarms, prevent control rod motion, initiate load cutback, and/or open the reactor trip breakers, depending on the severity of the condition.

The basic reactor tripping philosophy is to define a region of power and coolant temperature conditions allowed by the primary tripping functions, the overpower high ΔT trip, the over-temperature high ΔT trip, and the nuclear overpower trip. The allowable operating region within these trip settings is provided to prevent any combination of power, temperatures, and flow that would result in coolant boiling with all reactor coolant pumps in operation. Additional tripping functions such as reactor vessel low-low sodium level, loss of primary or secondary flow trips, steam and feedwater flow mismatch trip, high IHX primary to secondary ΔT trip, steam generator low-low level trip, turbine trip, source and intermediate range level trips, and manual trip are provided to back up the primary tripping functions for specific accident conditions and mechanical failures.

A rod stop and turbine cutback are initiated by a dropped-rod signal to provide additional core protection. The dropped rod is indicated from individual rod position indicators and by a rapid flux decrease on any of the power range nuclear channels.

Overpower and over-temperature rod stops are provided to prevent abnormal power conditions that could result from excessive control rod withdrawal initiated by a malfunction of the reactor control system or by operator violation of procedures.

GENERAL CRITERION 16: MONITORING REACTOR COOLANT BOUNDARY

Means shall be provided to detect leakage from the reactor coolant boundary. (Category B)

1000-MWe Criteria

16.1 The requirements stated in General Criterion 16 will be met.

16.2 Instrumentation will be provided to monitor the sodium inventory of the primary coolant system and to detect egress from that system.

Rationale Supporting the Selection of the 1000-MWe Criteria

These criteria are concerned with the effect of the loss of sodium from the primary circuit upon reactor performance and maintenance.

Compliance with the 1000-MWe Criteria

Positive indications in the control room of leakage of coolant from the reactor coolant system are provided by equipment that permits continuous monitoring. This will include level measurements in the reactor vessel and overflow tank, flame test and activity monitoring of the containment atmosphere, and leakage monitoring in selected regions of the primary circuit insulation.

GENERAL CRITERION 17: MONITORING RADIOACTIVITY RELEASES

Means shall be provided for monitoring the containment atmosphere and the facility effluent discharge paths for radioactivity released during normal operations, during anticipated transients, and during accident conditions. (Category B)

1000-MWe Criterion

17.1 The requirements stated in General Criterion 17 will be met.

Rationale Supporting the Selection of the 1000-MWe Criterion

The general criterion follows current Westinghouse commercial practice.

Compliance with the 1000-MWe Criterion

The containment atmosphere, the plant vent, and effluent disposal channels (exhaust stack gases, liquid channels within active waste treatment facilities, and solid waste disposal facilities) will be monitored for radioactivity concentration during all normal operations, during anticipated transients, and during accident conditions.

All gaseous effluent from possible sources of accidental releases of radioactivity external to the reactor containment (e.g., the spent fuel pit and waste handling equipment) will be exhausted from the plant vent that will be monitored. All accidental liquid spills will be maintained within the auxiliary building and collected in drain tanks.

For the case of leakage from the reactor containment under accident conditions, the plant area radiation monitoring system, supplemented by portable survey equipment to be kept in the control room, should provide adequate monitoring of accident releases. The details of the procedures and equipment for use in the event of an accident are specified in the plant emergency procedures to be developed prior to start up.

CRITERION 18: MONITORING FUEL AND WASTE STORAGE

Monitoring and alarm instrumentation shall be provided for fuel and waste storage and handling areas for conditions that might result in loss of decay heat removal capability and to detect excessive radiation levels. (Category B)

1000-MWe Criterion

18.1 The requirements stated in General Criterion 18 will be met.

Rationale Supporting the Selection of the 1000-MWe Criterion

This criterion is concerned with monitoring of radioactivity releases and waste storage cooling in order to detect and warn of conditions that might result in a radiation accident condition. This criterion differs from Criterion 17 in that Criterion 17 is more concerned with monitoring of the general atmosphere, whereas this criterion is specific to fuel and waste storage and handling areas. Here, one is concerned with the possibility of inadvertent criticality or gross damage to fuel resulting in excessively high levels of radiation.

Compliance with the 1000-MWe Criterion

Monitoring and alarm instrumentation will be provided for fuel and waste storage and handling areas to detect inadequate cooling and to detect excessive radiation levels. Radiation monitors will be provided to maintain surveillance over the release operation; but, the permanent record of activity releases will be provided by radiochemical analysis of known quantities of waste.

The spent fuel pit cooling loop will be flow monitored to assure proper operation.

A controlled ventilation system will remove gaseous radioactivity from the atmosphere and fuel storage and waste treating areas of the auxiliary building, and discharge it to the atmosphere via the plant vent. Radiation monitors will be in continuous service in these areas to actuate high-activity alarms on the control board annunciator.

GENERAL CRITERION 19: PROTECTION SYSTEMS STANDARDS AND RELIABILITY

Protection systems shall be designed to provide the high functional reliability and the in-service testing necessary to avoid undue risk to the health and safety of the public. (Category B)

1000-MWe Criteria

19.1 The requirements stated in General Criterion 19 will be met.

19.2 Protection systems will be designed in accordance with proposed IEEE standards for nuclear power plant protection systems.

Rationale Supporting the Selection of the 1000-MWe Criteria

The principles on which these criteria are based have been developed in the case of thermal reactor systems and are considered adequate and relevant to fast reactors.

Compliance with the 1000-MWe Criteria

The reactor uses a finer step-size version of the Westinghouse magnetic-type control rod drive mechanisms used in current PWR plants. Upon a loss of power to the coils, the control rod is released and falls by gravity into the core.

All reactor protection channels will be supplied with sufficient redundancy to provide the capability for channel calibration and test at power. Bypass removal of one trip circuit will be accomplished by placing that circuit in a half-tripped mode; i.e., a two-out-of-three circuit becomes a one-out-of-two circuit. Testing will not trip the system unless a trip condition exists in a concurrent channel.

Reliability and independence will be obtained by redundancy within each tripping function. In a two-out-of-three circuit, for example, the three channels will be equipped with separate primary sensors. Each channel will be continuously fed from its own independent electrical sources. Failure to de-energize a channel when required would be a mode of malfunction that would affect only that channel. The trip signal furnished by the two remaining channels would be unimpaired in this event.

GENERAL CRITERION 20: PROTECTION SYSTEMS REDUNDANCY AND INDEPENDENCE

Redundancy and independence designed into protection systems shall be sufficient to assure that no single failure or removal from service of any component or channel of such a system will result in loss of the protection function. The redundancy provided shall include, as a minimum, two channels of protection for each protection function to be served. (Category B)

1000-MWe Criteria

20.1 The requirements stated in General Criterion 20 will be met.

20.2 The design of the Reactor protection systems shall be based on the relevant IEEE criteria for standard nuclear power plant protection systems.

Rationale Supporting the Selection of the 1000-MWe Criteria

The principles on which these criteria are based have been developed in the case of thermal reactor systems and are considered adequate and relevant to fast reactors.

Compliance with the 1000-MWe Criteria

The design of the core protection system has not reached the stage where specific design can be discussed in detail. Compliance with the above criteria will, however, be achieved with current Westinghouse PWR protection systems that incorporate the following features:

Two reactor trip breakers are provided to interrupt power to the rod drive mechanisms. The breaker main contacts are connected in series with the power supply to the mechanism coils. Opening either breaker interrupts power to all mechanisms, causing them to release all rods to fall by gravity into the core. Each breaker is opened through an undervoltage trip coil. Each protection channel actuates two separate trip logic trains, one for each reactor trip breaker undervoltage trip coil. The protection system is thus inherently safe in the event of a loss of rod control power.

The coincident trip philosophy is carried out to provide a safe and reliable system since a single failure will not defeat the function of the channel and will also not cause a spurious plant trip. Channel independence is carried throughout the system extending from the sensor to the relay providing the logic. In most cases, the safety and control functions, when combined, are combined only at the sensor. Both functions are fully isolated in the remaining part of the channel; control is derived from the primary safety signal path through an isolation amplifier. As such, a failure in the control circuitry does not affect the safety channel.

GENERAL CRITERION 22:^{*} SEPARATION OF PROTECTION AND CONTROL INSTRUMENTATION SYSTEMS

Protection systems shall be separated from control instrumentation systems to the extent that failure or removal from service of any control instrumentation system component or channel, or of these common to control instrumentation and protection circuitry, leaves intact a system satisfying all requirements for the protection channels. (Category B)

1000-MWe Criteria

22.1 The requirements stated in General Criterion 22 will be met. As in the case of General Criterion 20, equipment design will satisfy the IEEE criteria wherever these are applicable.

Rationale Supporting the Selection of the 1000-MWe Criteria

The principles on which these criteria are based have been developed in the case of thermal reactor systems and are considered adequate and relevant to fast reactors.

Compliance with the 1000-MWe Criteria

The design of the core protection has not reached the stage when specific designs can be discussed in detail. Compliance with the above criteria will, however, be achieved with current Westinghouse PWR protection systems.

*Criterion 21 was deleted since it is more of a definition than a criterion, and since the implied requirement is adequately covered by Criterion 23.

GENERAL CRITERION 23: PROTECTION AGAINST MULTIPLE DISABILITY FOR
PROTECTION SYSTEMS

The effects of adverse conditions to which redundant channels or protection systems might be exposed in common, either under normal conditions or those of a credible accident, shall not result in loss of the protection function. (Category B)

1000-MWe Criteria

- 23.1 The requirements stated in General Criterion 23 will be met.
- 23.2 The design of the reactor protection systems shall be based on the relevant proposed IEEE criteria for standard nuclear power plant protection systems.

Rationale Supporting the Selection of the 1000-MWe Criteria

The principles on which these criteria are based have been developed in the case of thermal reactor systems and are considered adequate and relevant to fast reactors.

Compliance with the 1000-MWe Criteria

The design has not progressed to the state where an explanation of compliance can be given. It is, however, the intention that components of the protection system will be designed and laid out so that the mechanical and thermal environment accompanying any emergency situation in which the components are required to function does not interfere with that function.

GENERAL CRITERION 24: EMERGENCY POWER FOR PROTECTION SYSTEMS

An emergency power source shall be provided and designed with adequate independency, redundancy, capacity, and testability to permit the functioning of the engineered safety features and protection systems required to avoid undue risk to the health and safety of the public. This power source shall provide this capacity assuming a failure of a single active component. (Category B)

1000-MWe Criteria

- 24.1 The requirements stated in General Criterion 24 will be met.
- 24.2 The capacity of the emergency power source will be based on the requirements of the engineered safety features for the Credible Design Basis Accidents (defined under Criterion 10) concurrent with loss of outside power.
- 24.3 The design of the equipment associated with the operation of the emergency power source will be based on the relevant IEEE criteria for standard nuclear plant protection systems.

Rationale Supporting the Selection of the 1000-MWe Criteria

The first specific criteria specifies the capacity of the redundant power sources in terms of the most demanding emergency.

The last statement relates the design of equipment to current industry standards in this field.

Compliance with the 1000-MWe Criteria

The first source of emergency power is the station auxiliary transformer. If this first source should fail, the final sources of emergency power are two emergency diesel-generator sets. While these sets have not been specified in detail, current Westinghouse practice in this area would include the following features:

Each unit, as a backup to the normal A-C power supply, is capable of sequentially starting and supplying the power requirement of the one set of safeguards equipment required for the Credible Design Basis Accident.

Each emergency diesel is automatically started and can be fully loaded within about half a minute of the initial starting signal. The starting system is completely redundant for each diesel generator.

Other features concerning the testing and operation of this system are discussed in General Criteria 25 and 26.

GENERAL CRITERION 25: DEMONSTRATION OF FUNCTIONAL OPERABILITY OF PROTECTION SYSTEMS

Means shall be included for suitable testing of the active components of protection systems while the reactor is in operation, to determine if failure or loss of redundancy has occurred. (Category B)

1000-MWe Criteria

- 25.1 The requirements stated in General Criterion 25 will be met.
- 25.2 Standards and design bases required for test purposes will be based on those presented in the proposed IEEE criteria for standard nuclear plant protection systems.

Rationale Supporting the Selection of the 1000-MWe Criteria

The principles on which these criteria are based have been developed in the case of thermal reactor systems and are considered adequate and relevant to fast reactors.

Compliance with the 1000-MWe Criteria

The design of the core protection system has not reached the stage where specific design can be discussed in detail. Compliance with the above criteria will, however, be adhered with current Westinghouse PWR practice.

Here, each protection channel in service at power is capable of being calibrated and tripped independently by simulated signals for test purposes, to verify its operation. This includes checking through to the trip breakers which necessarily involves the trip logic. Thus, the operability of each trip channel can be determined conveniently and without ambiguity.

The starting of the diesel-generator sets can be tested from the control room. The ability of the units to start within the prescribed time and to carry load can periodically be checked.

Testing of the diesel-generator starting scheme may be performed from the plant main control board. This generator breaker is not closed automatically after starting during this testing. The generator may be manually synchronized to the 480-volt bus for loading. Complete testing of the

starting of either diesel-generator can be accomplished by tripping the associated 480-volt bus supply breaker and providing a coincident simulated safeguards signal. Blocking the closing of the generator breaker causes the bus tie breaker to close after a time delay sufficient for normal diesel-generator starting.

GENERAL CRITERION 26: PROTECTION SYSTEMS FAIL-SAFE DESIGN

The protection systems shall be designed to fail into a safe state or into a state established as tolerable on a defined basis if conditions such as disconnection of the systems, loss of energy, (e.g. electrical power, instrument air), or adverse environments, (e.g. extreme heat or cold, fire, (steam or water) are experienced. (Category B)

1000-MWe Criteria

26.1 The requirements stated in General Criterion 26 will be met.

26.2 This criterion will be interpreted in the light of the specific criteria presented in this proposed IEEE criteria for standard nuclear power plant protection systems.

Rationale Supporting the Selection of the 1000-MWe Criteria

The principles on which this criterion is based have been developed in the case of thermal reactor systems and are considered adequate and relevant to fast reactors.

Compliance with the 1000-MWe Criteria

Current Westinghouse practice utilizes the following features:

Each reactor trip circuit is designed so that trip occurs when the circuit is de-energized; an open circuit or loss of channel power, therefore, causes the system to go into its trip mode. In a two-out-of-three circuit, the three channels are equipped with separate primary sensors, and each channel is energized from independent electrical buses. Failure to de-energize when required is a mode of malfunction that affects only one channel. The trip signal furnished by the two remaining channels is unimpaired in this event.

The signal for containment isolation of non-vital valves is developed from a two-out-of-three circuit in which each channel is separate and independent and which signals for containment isolation upon loss of power. The failure of any channel to de-energize when required does not interfere with the proper functioning of the isolation circuit. Similar factors apply in the case of two-out-of-four circuits.

Reactor trip is implemented by interrupting power to the magnetic latch mechanisms on each drive, allowing the control rods to insert by gravity. The protection system is thus inherently safe in the event of a loss of power.

Automatic starting of either emergency diesel-generator is initiated by redundant undervoltage relays on the 480-volt bus to which the diesel-generator is connected, or by the safety injection signal. Engine cranking is accomplished by a stored-energy system supplied solely for the associated diesel-generator. The undervoltage relay scheme is designed so that loss of 480-volt power does not prevent the relay scheme from functioning properly.

REACTIVITY CONTROL

GENERAL CRITERION 27: REDUNDANCY OF REACTIVITY CONTROL

Two independent reactivity control systems shall be provided. (Category A)

1000-MWe Criterion

27.1 Two independent reactivity control systems shall be provided. Independence will be achieved by physical separation of the control rods, drive mechanism, and instrumentation associated with each system from those of the other system.

Rationale Supporting the Selection of the 1000-MWe Criterion

In spite of sophisticated design, and sometimes as a result of the complexity of instrumentation needed to "enhance" safety, failure of a control system is credible. In order to ensure reliable control of the fission process, two control systems will be provided, each independent of the other.

There remains some concern that an in-core accident could jam all control rods. It is possible that such an accident (e.g. sudden vaporization, or flashing, of sodium) would lead to a condition (such as meltdown) that could not be mitigated by the current reactivity control system. Further study of such accidents is needed; such study may dictate the need for a different specific criterion.

Compliance with the 1000-MWe Criterion

The reference design has two separate sets of safety control rods, each operated by separate control circuits and drive mechanisms. See Criterion 28 for more information.

GENERAL CRITERION 28: REACTIVITY HOT SHUTDOWN CAPABILITY

The reactivity control systems provided shall be capable of making and holding the reactor subcritical from any hot standby or hot operating condition, including those resulting from power changes. (Category A)

1000-MWe Criteria

- 28.1 Either of the two reactivity control systems shall be capable of making and holding the core subcritical from any hot standby or hot operating condition, including conditions of steady state and changing power.
- 28.2 In normal operation, with both control systems functioning, the shutdown margin shall be at least 3% $\Delta k/k$. In abnormal situations, such as when one control system is inoperative or when the most reactive control rod remains withdrawn, the shutdown margin shall be at least 1% $\Delta k/k$.

Rationale Supporting the Selection of the 1000-MWe Criteria

The rationale supporting the selection of Criterion 27.1 gave the reasons for existence of two reactivity control systems. In order for each of the reactivity control systems to serve its necessary function, it must be possible to make the reactor subcritical from any normal state.

The specification of 3%, or $\beta_{8.11}$, subcritical is a conservative, albeit arbitrary, requirement to ensure that the reactor is very surely in the safe, subcritical configuration. In the abnormal circumstances cited in the criterion, a shutdown margin of 1% is deemed sufficient because the probability of the reactor being in such an abnormal state is small, and the reactor will be left in that abnormal state for only a short period of time.

Compliance with the 1000-MWe Criteria

The various control rod worths are:

<u>Rod Group</u>	<u>One Rod Worth</u>	<u>Rod Group Worth</u>
Safety	\$0.80	\$12.80 (in two groups)
Shim	\$0.42	\$13.47
Regulating	\$0.23	<u>\$ 2.73</u>
	Sum =	\$29.00

Some pertinent control requirements are:

Cold to hot full power	\$2.70
One stuck rod average worth	\$0.80
One stuck rod maximum worth	\$1.83 with all other rods in
3% shutdown margin	\$8.11
1% shutdown margin	\$2.70

Thus, the normal shutdown margin provided by safety rods alone is $\$12.80 - \$2.70 = \$10.10$ (or 3.73% $\Delta k/k$).

If one safety control system is inoperative, the shutdown margin provided by safety rods alone is $\$6.40 - \$2.70 - \$1.83 = \8.27 (or 3.06% $\Delta k/k$).

It should be noted that the shutdown margin for each of the cases just cited would actually be larger, since the shim and regulating rods will have been withdrawn; their subsequent insertion increases the shutdown margin.

GENERAL CRITERION 30: REACTIVITY SHUTDOWN AND HOLDDOWN CAPABILITY

One of the reactivity control systems provided shall be capable of making the reactor subcritical under any credible accident condition (including anticipated operational transients) sufficiently fast to prevent exceeding fuel performance conditions consistent with public health and safety protection. The control system should then be capable of holding the reactor subcritical with the most reactive control rod fully withdrawn. (Category A)

1000-MWe Criterion

- 29.1 Either of the two reactivity control systems shall be capable of making the reactor subcritical under any credible accident condition (including anticipated operational transients), sufficiently fast to prevent exceeding fuel performance conditions consistent with public health and safety. The resultant shutdown margin shall be greater than the worth of the most reactive control rod when fully withdrawn.

During refueling, the reactor will be shutdown with a margin of at least 3% $\Delta k/k$.

Rationale Supporting the Selection of the 1000-MWe Criterion

In addition to placing the reactor in the subcritical condition specified in Criterion 28, it is necessary to ensure that - particularly when operational transients occur - this can be done rapidly enough to avoid endangering public health and safety.

This criterion specifies that the subcritical condition must be reached even if one control rod is stuck in the fully withdrawn position.

The requirement that the shutdown margin during refueling be at least 3% $\Delta k/k$ is intended to ensure that insertion of fuel in the wrong location or dropping of a fuel assembly cannot lead to a reactivity excursion.

Compliance with the 1000-MWe Criterion

Refer to the compliance section of Criterion 28 and observe that 1% $\Delta k/k$ shutdown margin is obtained even when one control system is inoperative and the most reactive control rod is stuck out, since the shutdown margin provided by safety rods alone is in this case: $\$6.40 - \$2.70 - \$0.80 = \2.90 (or 1.07% $\Delta k/k$). Similarly, it can be seen that the shutdown margin of 3% $\Delta k/k$ during refueling can be met. Since anticipated operational transients will make the reactor supercritical by much less than \$1, it is clear that a single control system can also cope with operational transients.

Thus, the reference design meets the requirement on shutdown magnitude. However, the shutdown rate cannot yet be said to be correct. Analyses of credible operational transients are needed in order to ensure that fuel performance conditions consistent with public health and safety are not exceeded. A preliminary analysis of flow coastdown indicates that the scram rate is adequate to protect the core from damage; but, additional analyses are clearly needed.

GENERAL CRITERION 31: REACTIVITY CONTROL SYSTEM MALFUNCTION

The reactor protection systems shall be capable of protecting against any single malfunction of the reactivity control system, such as unplanned continuous withdrawal (not ejection or dropout) of a control rod, by limiting reactivity transients to avoid exceeding acceptable fuel damage limits.

1000-MWe Criterion

31.1 The requirements stated in General Criterion 31 will be met.

Rationale Supporting the Selection of the 1000-MWe Criterion

The general criterion follows current Westinghouse commercial practice.

Compliance with the 1000-MWe Criterion

Reactor scram shutdown with rods is completely independent of the normal control functions, since the trip breakers completely interrupt the power to the rod mechanisms regardless of existing control signals.

Design of the absorber rod control system and of the worths of individual rods has been carried out so as to restrict the size of reactivity excursion possible as a consequence of malfunctions in the reactivity control system. Reactor trip systems based on neutronic and thermal detection systems will automatically operate the scram shutdown system.

The design characteristics of the reactor protective system are discussed in Criteria 20 through 27.

GENERAL CRITERION 32: MAXIMUM REACTIVITY WORTH OF CONTROL RODS

Limits, which include reasonable margins, shall be placed on the maximum reactivity worth of control rods and on rates at which reactivity can be increased to ensure that the potential effects of a sudden or large change of reactivity cannot (a) rupture the reactor coolant boundary or (b) disrupt the core, its support structures, or other vessel internals sufficiently to lose capability of cooling the core. (Category A)

1000-MWe Criterion

- 32.1 The maximum reactivity worth of a control rod and the maximum rate at which it can increase reactivity shall be such that any operation or credible malfunction of the control rod or its drive system cannot cause a reactivity transient which could rupture the reactor coolant boundary, or disrupt the core, support structure, or vessel internals.

Rationale Supporting the Selection of the 1000-MWe Criterion

The reactivity worth of the control rods and their rate of movement should be limited so that, if a credible maloperation or a malfunction occurred, the reactor would not suffer damage that could endanger the public health and safety.

Compliance with the 1000-MWe Criterion

Without extensive safety and kinetic analyses, the specific magnitudes and rates required to meet the criterion cannot be specified. However, the reactor design is conservative, with a maximum control rod worth of \$0.80 and a maximum control rod reactivity insertion rate of \$0.04/sec. The reliable magnetic jack mechanisms and separate control systems increase the probability that, when kinetic and safety analyses have been performed, this criterion can be met.

REACTOR COOLANT BOUNDARY

GENERAL CRITERION 33: REACTOR COOLANT BOUNDARY CAPABILITY

The reactor coolant boundary shall be able to accommodate, without rupture, the static and dynamic loads imposed on any boundary component as a result of any credible inadvertent and sudden release of energy to the coolant. As a design reference, this sudden release shall be taken as that which would result from a sudden reactivity insertion such as rod motion.
(Category A)

1000-MWe Criteria

- 33.1 The reactor vessel and all primary pipework will be designed to accept all operational loads and anticipated transient conditions imposed by the plant. Such loads will include those generated by liquid flow, piping reactions, differential thermal expansion, static weights and any dynamic loads the internals may produce.
- 33.2 The reactor vessel and all primary pipework will be designed to accept all anticipated additional loads imposed by geological and climatic conditions at the site of the plant.
- 33.3 The structural design of the vessel and pipework will accept areas of high loading that can be anticipated to occur locally within the circuit (e.g., at inlet and outlet nozzles).
- 33.4 The design of the vessel and primary pipework will also be capable of accommodating any credible inadvertent and sudden energy release to the coolant. As a design reference, this energy release will be taken to be that which would result from a sudden reactivity insertion that might arise from control rod motion

Rationale Supporting the Selection of the 1000-MWe Criteria

Criterion 33 is concerned with the requirement that the reactor vessel and primary pipework should be capable of withstanding, without rupture, all operational and anticipated transient conditions. These specific criteria therefore list the normal loadings that might occur in a reactor system arising from the operation of the plant, from its siting, and from credible accidents. Specific note is taken of the fact that the vessel does not act as a containment of the worst credible meltdown accident excursion, although credit may be taken of the fact that it acts as a first energy absorption barrier. Quantitative maximum loadings and energy releases will need to be specified in the Title I design.

Compliance with the 1000-MWe Criteria

The reactor coolant boundary, including the reactor vessel, primary piping system, and intermediate heat exchanger, will be analyzed to insure that it is capable of accepting, without failure, all expected operational loads and transient conditions, imposed by normal operation, design seismic and climatic conditions, expected energy releases caused by sudden core reactivity increases, and all other static and dynamic loads that are expected or deemed credible. However, thorough analysis of the system during these situations were not performed during the conceptual design stage. These loadings will be analyzed as the preliminary and final design stages develop.

GENERAL CRITERION 34 (35): REACTOR COOLANT BOUNDARY RAPID PROPAGATION
FAILURE PREVENTION

The reactor coolant boundary shall be designed to reduce to an acceptable level the probability of rapidly propagating type failures. Consideration shall be given (a) to the provisions for control over service temperature and irradiation effects including operating restrictions where appropriate, (b) to the design and construction of the reactor vessel in accordance with applicable codes and standards, including those which establish requirements for energy absorption within the elastic strain energy range and for absorption of energy by plastic deformation, and (c) to the design and construction of reactor coolant boundary piping and equipment in accordance with applicable codes and structures. (Category A)

1000-MWe Criterion

34.1 The criterion will fulfill the scope and intent of the general criterion above.

Rationale Supporting the Selection of the 1000-MWe Criterion

Criterion 34 (35) is concerned with the requirement to establish thermal and neutron irradiation limits and to design the vessel and pipework according to established codes to prevent the possibility of rapid propagation failure of the coolant boundary. As we are not here dealing with a high pressure system such as a PWR, the same importance does not apply to rapid propagating failure. However, the principles of protection against vessel failure (and thereby loss of coolant) still apply.

Compliance with the 1000-MWe Criterion

The reactor vessel for the 1000-MWe reference concept is completely surrounded by four inches of thermal insulation. This thermal insulation is located on the inner surface of the steel safety tank. It is a calcium silicate (anhydrous) composition known as thermobestor. The reactor vessel is also surrounded by a radial neutron shield having an overall thickness of 24-1/2 inches. This shield is designed to reduce secondary sodium activity to acceptable levels and to suppress the neutron activation of primary system components.

The reactor vessel is also contained in a concrete vault that supplies additional primary system shielding.

Radial neutron reflectors within the vessel and thermal shielding inside the core barrel protect the core barrel and vessel wall from excessive irradiation.

The reactor vessel internals are designed so that the vessel wall will be maintained at coolant inlet temperature. The cold inlet flow is directed circumferentially around the upper core barrel and downward in an annulus surrounding the core barrel to the inlet plenum. In this way, the vertical portion of the vessel is protected against the high-temperature creep and stress effects.

The self shielding effects of the vessel internal structures and the core radial reflector protect critical vessel areas from structurally prohibitive doses of radiation.

Conceptual design does not allow a vessel analysis based on an expected number of transients during plant lifetime. However, the vessel and the system designs will be evaluated as required by the applicable codes to determine the effects of low cycle fatigue, and cumulative usage factors will definitely be less than one at all points.

The reactor vessel, piping system, and all other system boundary vessels will be designed according to the applicable portions of the nuclear piping code, power piping code, and the ASME design code as a minimum requirement.

GENERAL CRITERION 36: REACTOR COOLANT BOUNDARY SURVEILLANCE

Reactor coolant boundary components shall have provisions for periodic inspection of selected areas. These areas will provide the representative sample of the entire pressure boundary, necessary to evaluate the structural and leakage integrity of all areas where failure would cause a loss of coolant accident. A material surveillance program will be provided, if justified, by a lack of sufficient information necessary to assure that the vessel material design properties will not be adversely affected by the expected radiation levels and environmental conditions. (Category A)

1000-MWe Criteria

- 36.1 The vessel and associated plant will be designed for a 30-year life, and the capability to perform periodic inspection of critical areas will be provided to assess the structural and leakage integrity throughout life.
- 36.2 The inspection areas will be chosen to provide a representative sample of the entire coolant boundary, reactor vessel, and pipework, to evaluate structural and leakage integrity of all areas where failure would cause undesirable loss of coolant.
- 36.3 A material surveillance program will be provided, if justified, by a lack of sufficient evidence obtained by other means to ensure that the vessel material design properties will not be adversely affected by thermal and neutron irradiation levels.
- 36.4 Visual inspection of seals, upper vessel interior, bolts, flanges, and shield plug will be available when the plant is in its refueling cycle.
- 36.5 Means of monitoring for loss of sodium coolant will be provided.
- 36.6 Means of monitoring for loss of cover-gas pressure will be provided.

Rationale Supporting the Selection of the 1000-MWe Criteria

Criterion 36 is concerned with the requirement for a reactor vessel and primary pipework surveillance program. The specific criteria are written in order to ensure a sufficient inspection procedure based on critical areas used as a representative sample rather than being based on inspecting the entire circuit. The material surveillance program, if considered necessary, would have to conform to the intent of applicable inspection codes.

Compliance with the 1000-MWe Criteria

The design of the plant piping and equipment layout, the system insulation that will be used, and the containment design, all allow access for primary coolant boundary inspection. The necessity for a specific structural surveillance or material surveillance program is not determined in the conceptual design stage. The necessity for these programs will be evaluated, and specific requirements will be set down as the plant design proceeds through the preliminary stage

Instrument and protective devices for serving such functions as coolant leak detection and loss of cover gas are covered under other criteria.

ENGINEERED SAFETY FEATURES
A. General Requirements

GENERAL CRITERION 37: ENGINEERED SAFETY FEATURES BASIS FOR DESIGN

Engineered safety features shall be provided in the facility to back up the inherent safety provided by the core design, the reactor coolant boundary, and their protection systems. Such engineered safety features shall be designed to cope with any credible reactor coolant piping failure. (Category A)

1000-MWe Criteria

- 37.1 Reactor containment or equivalent will be provided. The containment structure will be designed to withstand the worst credible core melt-down accident (CDBA). (See Criterion 10.2)
- 37.2 Emergency core cooling will be provided. It will be of sufficient capacity to keep the fuel below the maximum design temperature at all times following the loss of main coolant flow. (See Criterion 44)
- 37.3 A post-accident atmosphere cleanup system will be provided to remove radioactive particles from the atmosphere.
- 37.4 Inert gas systems will be provided to protect against sodium chemical reactions. These systems will be in operation during all power and refueling operations.
- 37.5 Check valves will be provided, if necessary, to prevent flow reversal following a primary coolant loop pipe rupture.
- 37.6 Protection will be provided against siphoning the sodium coolant below the level of the core.
- 37.7 Blast shielding will be designed to contain the effects of any shock wave generated by the reactor during the worst credible meltdown accident.

- 37.8 Missile protection of engineered safety features, particularly the containment, will be designed to protect against possible missiles generated by the CDBA. (See Criterion 40)
- 37.9 A last ditch cooling system will be provided, if practicable, to cool the molten fuel resulting from a core meltdown.
- 37.10 A mechanism will be provided, if practicable, to prevent a supercritical configuration from forming following a core meltdown.
- 37.11 A safety tank will be provided to insure a sodium level above the core following a reactor vessel rupture.

Rationale Supporting the Selection of the 1000-MWe Criteria

Engineered safety features are defined as "devices or methods, inherent or provided, which prevent, mitigate, or control the consequences of accidents. These safeguards include containment systems, auxiliary cooling, fire fighting, redundancy in safety systems, etc...."*

The criteria for the containment (37.1) and the emergency cooling system (37.2) follow directly from this definition.

An inert gas system (37.4) will not support combustion, and will therefore prevent a sodium fire (CDBA). The concentration of radioactive particles after an accident must be kept within limits that are consistent with the requirements of 10 CFR 100 (37.3).

A primary coolant pipe rupture may cause flow reversal (37.5), siphoning (37.6), or both, and subsequent core drainage.

The core meltdown and compaction accident (CDBA) may lead to some or all of the following: (a) shock waves and dynamic effects (37.7), (b) missiles (37.8), (c) molten fuel leakage to the reactor cell floor (37.9) and (d) secondary criticality (37.10).

In the event of the worst credible meltdown accident, the core material must be contained and cooled. (37.11)

Compliance with the 1000-MWe Criteria

In this stage of the analysis, none of the system designs have been finalized and are subject to modification as the analysis proceeds. Some of the systems have yet to be designed, and are in the early conceptual stages.

* LMFBR Program Plan, Section 10 - Safety, Page 15.

The containment, emergency cooling system, and missile protection are covered in General Criteria 10, 44, and 40, respectively.

The post-accident atmosphere cleanup system is in the early stages of design, and not much can be said quantitatively. The final design will include sonic, electrostatic, filter, or other devices for removing radioactive aerosol from the containment atmosphere, and will include sufficient redundancy based on a design capacity yet to be determined.

Check valves are presently located in the coolant pumps, but may be removed to a point closer to the reactor vessel so they may better cope with the effects of pipe rupture. Bypass check valves are also currently included in the design of the core barrel as a protection against siphoning; however, further analysis is required in this area to determine design parameters of the final system.

Present design incorporates the blast shield with the radial neutron shield. It extends the full height of the reactor cell and is continued underneath the vessel. It consists of three gas cooling annuli, each separated by six inches of serpentine aggregate followed by an outside liner of mild steel. The inner liner of one-inch steel serves as a safety vessel against loss of coolant resulting from reactor vessel rupture. The blast shield may plastically deform during the worst credible meltdown accident, but will not rupture. This statement is based on preliminary calculations that give 3800 pounds of TNT as the maximum energy release during an incredible meltdown of the entire core, and 6000 pounds of TNT as the maximum energy the shield will absorb without rupture.

No conceptual analysis has been done on either the last-ditch cooling system or the core dispersal system. One possible design of the last-ditch cooling system is the incorporation of cooling coils embedded in the reactor cell floor.

The outer safety tank has not been specifically designed; however, general criteria have been defined as: (a) it will completely surround the reactor vessel, and (b) the volume of the open void below the top of the emergency coolant outlet nozzle in the safety tank must not exceed the volume of sodium above the top of the emergency coolant outlet nozzle in the reactor vessel.

GENERAL CRITERION 38: RELIABILITY AND TESTABILITY OF ENGINEERED
SAFETY FEATURES

All engineered safety features shall be designed to provide functional reliability and ready testability as is necessary to avoid undue risk to the health and safety of the public. (Category A)

1000-MWe Criteria

- 38.1 A program of plant testing will be formulated for all equipment systems and system controls vital to the functioning of engineered safety features. The program will consist of performance tests of individual pieces of equipment in the manufacturer's shop where possible, integrated tests of the system as a whole, periodic tests of the actuation circuitry and mechanical components to assure reliable performance, upon demand, throughout the plant lifetime.
- 38.2 Routine periodic testing of the engineered safety features components is required.

Rationale Supporting the Selection of the 1000-MWe Criteria

The initial tests of individual components and the integrated tests of the system as a whole complement each other to assure performance of the system as designed and to prove proper operation of the actuation circuitry.

Compliance with the 1000-MWe Criteria

During the conceptual design period, when features of the plant are being continuously modified and further defined as time proceeds, inspection and performance tests have not yet been planned, either during manufacture or during plant lifetime.

However, components and systems of engineered safety features will be subject to strict quality and performance controls. Inspection and test procedures will include:

- a. quality control during manufacture;
- b. where appropriate, performance testing before delivery;

- c. performance testing before and during commissioning, when appropriate; and
- d. periodic testing before and during plant lifetime at a frequency consistent with the safety function involved and possibly under reduced conditions.

Such testing will include mechanical components where these are involved, (e.g. valves, dampers, and pumps) and control components where appropriate, (e.g. alarm systems and automatic operation of components). Where in situ passive features are involved (e.g. core dispersion device), a material surveillance program may be necessary.

The following engineered safety features may be subject to periodic testing during plant lifetime:

- a. Containment: See compliance to Criteria 54 to 57.
- b. Air Cleanup System (and atmosphere cleanup system): See compliance to Criterion 62. The post-accident atmosphere cleanup systems will be subject to similar test programs.
- c. Emergency Core Cooling: See compliance to Criterion 45.
- d. Check Valves: Which may be tested during downtime by observing the pressure transients that arise following single-loop flow operation. This will be done at low flows to avoid sodium-hammer effects.
- e. Aerosol - Settling Device: Such a device has not yet been designed; but, any electrostatic, sonic, or mechanical device may be tested during plant lifetime. This will be considered in the detailed design.
- f. Inert Gas System: Will be subject to a full operational test program.

Other engineered safety features that are not subject to periodic testing during plant lifetime are:

- a. Siphon Breakers, and
- b. Last ditch cooling system.

These features have not been subject to detailed design yet; it is therefore impossible to define any inspection and test program that would demonstrate compliance with the criteria.

It is expected that detailed description of test procedures of engineered safety features will be part of the design task.

GENERAL CRITERION 39: EMERGENCY POWER FOR ENGINEERED SAFETY FEATURES

A plant auxiliary power distribution system shall be provided with an emergency power source under the control of the operator, and shall be designed with sufficient redundancy and capacity to permit the functioning of the engineered safety features required to avoid undue risk to the health and safety of the public. This auxiliary power system will operate in the event of the failure of any element in the primary power system which results in the loss of primary power. (Category A)

1000-MWe Criteria

- 39.1 An auxiliary power system will be provided using diesel generation equipment. This, together with associated power distribution circuitry, will be under the control of the operator; although, automatic control may be added, and further safety protection thereby gained.
- 39.2 The auxiliary power system will operate in the event of failure of any single element of the primary power system that results in the loss of primary power.
- 39.3 The emergency cooling system will be driven by the auxiliary power system.
- 39.4 Certain redundant protective instrumentation channels may be powered by the auxiliary diesel-generated power system, either habitually or in the event of an accident unassociated with a loss of off-site power.
- 39.5 In the event of a loss of off-site power, instrumentation and control will be powered by the auxiliary power systems. Battery power supplies will be available for the immediate instrumentation requirements until diesel-generation equipment can be put into operation.
- 39.6 Certain redundant protective instrumentation channels will be powered by battery supplies throughout operation to provide the redundancy.

Rationale Supporting the Selection of the 1000-MWe Criteria

Criterion 39 is only concerned with supplying emergency power to the engineered safety features in the desired interval of time. Some items are not needed from a safety point of view, and thus have no emergency power provisions. The next category of items are those that must have power, but can stand a finite amount of time (~ 10 seconds) before obtaining it. These items are powered by diesel generators that are not running at the time of normal power failure. The next category of items are those that must have emergency power immediately upon recognition of a main power failure, but, that can survive a switching transient. These items derive their emergency power from batteries that are on constant charge from the normal unfailed power system, or diesel generators that are kept running in a ready condition. The last, and most critical category, are the items that must not suffer a switching transient on loss of normal power and, therefore, are normally kept connected to circuits that are powered by large station batteries that are kept charged by the normal power. Upon failure of normal power, these items continue to function, without transients, until the batteries are depleted.

Compliance with the 1000-MWe Criteria

The 1000-MWe design will comply with the criteria in that an elaborate reliable power distribution system connected to a multiple, emergency power source system is proposed. Redundant diesel generators are specified, both for the "running-ready" condition and the "available within (~ 10 sec)" condition. In addition, station batteries will be provided for both the "transient allowed" switch-over system and the "transient free, always connected" requirement.

The normal source of auxiliary power during plant operation is the main plant turbine-driven generator. Power is supplied via the unit auxiliary transformer that is connected to the main generator switch gear.

Standby power required during plant startup, shutdown, and after reactor trip is supplied from the local electric utility system directly to the station auxiliary transformer.

All diesel-driven generating equipment will be capable of remote starting from the main control room for testing purposes, in addition to the automatic-start-on-demand feature. All diesel-driven generators will be started and tested under load on a fixed maintenance schedule.

All station batteries will be carefully and periodically maintained and rigorously checked to guarantee their availability.

GENERAL CRITERION 40: MISSILE PROTECTION

Adequate protection for those engineered safety features, the failure of which could cause an undue risk to the health and safety of the public, shall be provided as necessary against dynamic effects and missiles that might result from plant equipment failure. (Category A)

1000-MWe Criteria

- 40.1 Missile protection for engineered safety features will be provided, as necessary, against missiles resulting from reactor plant failures. Protection of an engineered safety feature is necessary only if the failure to provide the protection results in an undue risk to the health and safety of the public.
- 40.2 To the extent practicable, all equipment will be designed to eliminate the possibility of missile generation.

Rationale Supporting the Selection of the 1000-MWe Criteria

By initially designing to eliminate all sources of missiles, an offensive rather than defensive position is taken. Missile shields then become a redundant form of protection rather than the primary line of defense.

Compliance with the 1000-MWe Criteria

Core meltdown and compaction accident or other plant equipment failure might result in dynamic effects or missiles. For such engineered safety features as are required to ensure safety in the event of such an accident or equipment failure, protection from these dynamic effects or missiles will be considered in the layout of plant equipment and any missile barriers. Consideration will be given during the design to the following potential sources of missiles: valve stems and bonnets, instrument thimbles including installed sensors, bolts, complete control rod drive shafts and/or mechanisms, and the reactor vessel shield plug.

GENERAL CRITERION 41: ENGINEERED SAFETY FEATURES PERFORMANCE CAPABILITY

Engineered safety features shall provide sufficient performance capability to accommodate any single failure of an active component and still function in a manner to avoid undue risk to the health and safety of the public. (Category A)

1000-MWe Criteria

- 41.1 Engineered safety features such as air cleanup and emergency cooling systems will be designed to perform their function with a safety margin to cover any calculational uncertainties and any deterioration in performance.
- 41.2 Any single failure of an active component in any safety feature will not endanger the function of the safety feature. Sufficient redundancy will be included in the design to accommodate for single failures of active components.

Rationale Supporting the Selection of the 1000-MWe Criteria

The engineered safety features will not only be designed to cope with a component failure, but forethought must be given to the possible decrease in efficiency due to equipment aging or equipment wear.

Compliance with the 1000-MWe Criteria

During the conceptual design period, when features of the plant are being continuously modified and further defined as time proceeds, engineered safety features have not been fully defined. In some cases, (e.g. last-ditch cooling system and a mechanism to prevent secondary criticality) no design yet exists, although the Title I design may include such features.

Each engineered safety feature will be designed with margins to cover calculational uncertainties. Such margins will be assessed at two or three standard deviations of the calculational error in the main variables of interest. These variables are pressure and temperature in the case of the containment, rupture rates in the case of siphon breakers or check valves, air volume rates in air cleanup systems, heating levels in cooling system (emergency and last ditch), and failure mechanism rates in devices to prevent secondary criticality.

Each engineered safety feature will have additional design margins to cover deterioration during plant lifetime. In particular, this applies to containment penetration seals, check valves, pumps, fans, and dampers in air cleanup systems, and any moving part. The failure of any single component will not endanger any safety function.

- a. Containment: See compliance to Criterion 53.
- b. Air cleanup system and post-accident atmosphere cleanup system: See compliance to Criterion 62. Also, where necessary, redundancy in control, valves, filters, and fans and dampers is built into the system.
- c. Emergency Core Cooling: See compliance to Criterion 44.
- d. Check Valves: The reference design includes a check valve in each pump, but it is likely that this valve will be removed and placed closer to the vessel inlet to cope with a pipe rupture more efficiently.
- e. Siphon Breakers: There will be more than one siphon breaker in the system, each with a performance safety margin.
- f. Inert Gas System: There will be adequate redundancy in the system by doubling active components or even the entire system if the design shows the need.

GENERAL CRITERION 42: ENGINEERED SAFETY FEATURES COMPONENTS CAPABILITY

Engineered safety features shall be designed so that the capability of these features to perform their required function is not impaired by the effects of a credible accident to the extent that there would be undue risk to the health and safety of the public. (Category A)

1000-MWe Criteria

42.1 Components of engineered safety features that are vital to the operation of the safety feature, such as emergency cooling pumps, instrumentation, auxiliary power supply generators, battery power, air cleanup blowers, motors, cables, penetrations, etc., that are located inside the containment will be selected to meet the most adverse accident conditions to which they may be subjected. These items will be designed to withstand, without failure, exposure to the worst combination of temperature and pressure expected during the required operational period.

Rationale Supporting the Selection of the 1000-MWe Criteria

Each component of a safety system must be capable of withstanding the pressure and temperature effects of a CDBA, if this is when the system is expected to operate. The supporting electrical leads and control equipment must also be of the same quality.

Compliance with the 1000-MWe Criterion

During the conceptual design period of the 1000-MWe plant, when features are being continuously modified, the engineered safety features have not been fully defined. In some cases, (e.g. last-ditch cooling system, etc.) no design exists, although the final plant design may include such features.

Most engineered safety features, the containment and the last-ditch cooling system, the inert gas system, the safety vessel, blast shielding, and missile protection, are designed to mitigate against the consequences of the worst credible core meltdown accident (Criterion 10.5) and they are designed to withstand the peak calculated transient pressure and temperature during that accident. See the compliance to Criterion 49 for containment details. The air clean system and post-accident atmosphere clean system and their components are designed to operate under all credible accident conditions, including the credible design basis accident. (Criterion 10.5)

Emergency core-cooling components, pumps, control, generators, etc., are designed to withstand all conditions up to and including those arising from the most severe pipe rupture -- the double-ended, circumferential break. They will, therefore, be designed to withstand any sodium hammer transients arising from such a rupture.

Check valves and siphon breakers will be designed to operate in the case of a pipe rupture; therefore, their design will be subject to the similar conditions as are applied to emergency core-cooling components. The aerosol settling device will be designed to operate in the conditions and environment arising from the most severe sodium fire that could arise.

Where control is required in an engineered safety feature, as in the air and atmosphere cleanup systems, the emergency cooling pump and the aerosol settling device, cables, control electronics, and instrumentation will be designed to operate under peak CDBA calculated temperatures and pressures.

ENGINEERED SAFETY FEATURES
B. Emergency Core Cooling

GENERAL CRITERION 44: EMERGENCY CORE COOLING CAPABILITY

A core cooling system, to provide adequate emergency core cooling taking into account sufficient safeguard margins, shall be provided. (Category A)

1000-MWe Criteria

- 44.1 Emergency core cooling capability will be designed to provide adequate cooling to remove decay heating following loss of main cooling.
- 44.2 The emergency core cooling method utilized will be unaffected by main cooling system malfunctions and will be capable of operation following loss of normal on-site auxiliary power.
- 44.3 Sufficient redundancy shall be included in the design of emergency cooling to accommodate for single failure of active components, such components to include valves and pump components.
- 44.4 The emergency cooling will be designed so that it is not inactivated by the same fault that resulted in a loss of main cooling to the core. It will be designed to employ separate components where possible, in pipework, pumping and power supply, and it will be designed to contain its coolant even when the primary piping network external to the core has been drained.

Rationale Supporting the Selection of the 1000-MWe Criteria

Criterion 44 is concerned simply with the provision of emergency core cooling under all credible conditions. It might, for example, require two loops entirely reproducing each other before this is achieved. On the other hand, it could more probably be achieved with a single emergency core-cooling loop, into which sufficient redundancy has been built. It is also required that the emergency core cooling capability should be retained in the event of a rupture of the pipework of the main cooling circuit.

Compliance with the 1000-MWe Criteria

An auxiliary core cooling system (ACS) has been conceptually designed. Its cooling capacity was based on the prevention of sodium boiling in the core in the event of a simultaneous pump seizure in one loop and loss of pumping power in the other. The design is conservative for this accident. Analysis of the catastrophic double-ended pipe rupture was not performed. However, it is expected that the system will prevent significant core damage during this accident.

The system consists of a cooling circuit completely independent of the main coolant systems, except for the reactor vessel interface that is surrounded by a safety tank. Redundant emergency power supplies are provided for the pumps and air blowers in addition to their normal on-site power supply. The primary ACS loop contains pump discharge check valves to prevent backflow. Two full size valves in parallel are provided for redundancy. The circuit pumps are the electromagnetic type with no moving parts. The primary ACS vessel penetrations are below the level of the main cooling system inlet and outlet nozzles to allow ACS operation with both main loops drained. The ACS piping system and intermediate heat exchanger will be designed in accordance with applicable portions of the nuclear piping code, power piping code and the ASME vessel design code.

GENERAL CRITERION 45 (46 to 48): INSPECTION AND TESTING OF SYSTEM
WHICH PROVIDES EMERGENCY CORE COOLING

Design provisions shall, where practical, be made to facilitate physical inspection of all critical parts of the system which provides emergency core cooling. A capability shall be provided (a) to test periodically the operativeness of the system up to a location as close to the core as is practical, and (b) to test initially, under conditions as close as practical to design, the full operational sequence that would bring the system into action. (Category A)

1000 MWe Criteria

- 45.1 Provision will be made to physically inspect emergency core-cooling components such as valves and pumps.
- 45.2 The operation of active components of the system will be tested at regular intervals during the lifetime of the system, such components including valves, pumps, and diesel generating sets.
- 45.3 Periodic inspection of critical areas will be made to assess the structural and leakage integrity throughout life, by choosing such inspection areas to be a representative sample of the entire coolant boundary of the emergency core cooling system.

Rationale Supporting the Selection of the 1000-MWe Criteria

Criterion 45 (46 to 48) is concerned with the testing (assurance that the emergency core cooling capability is always in functional order is naturally of prime importance) and inspection of the system. Specific criteria are written with the idea that assurance of functional operability will be obtained by using the emergency cooling system during shut-down periods.

A value for the percentage of normal cooling flow that must be provided for emergency cooling will be specified before the Title I design.

Compliance with the 1000-MWe Criteria

The auxiliary core-cooling system is completely independent of the main heat transport systems except for the reactor vessel interface. The pumps and air blowers in the intermediate loop can be operationally tested at any time. The primary side pump can be energized at any time, though flow cannot be attained while the main coolant pumps are running due to the ACS pump discharge check valves. These valves will be tested for operability each time the reactor is shut down and the main coolant pumps are reduced to pony motor flow.

The necessity for a structural integrity inspection program will be determined at a later time; however, access to all equipment is provided should an inspection program be necessary.

ENGINEERED SAFETY FEATURES

C. Containment

GENERAL CRITERION 49: REACTOR CONTAINMENT DESIGN BASIS

The containment structure, including access openings and penetrations, and any necessary containment heat-removal systems shall be designed so that the leakage of radioactive materials from the containment structure, under conditions of the pressure and temperature resulting from the maximum credible accidental energy release, will not result in undue risk to the health and safety of the public. The maximum credible accidental energy release shall be determined from an analysis of the worst credible core meltdown and compaction accident (Criterion 10) and the maximum credible sodium reaction accident. (Category A)

1000-MWe Criteria

- 49.1 Containment will be provided to limit radioactivity release to the environment. This release will not exceed the limits described in 10 CFR 20 for normal operation and for transient situations that might reasonably be anticipated to occur and 10 CFR 100 for potential accidents which have a very low probability of occurrence.
- 49.2 The containment building will be designed to withstand the peak over-pressure that could occur in the building as a result of the most severe credible reactor accident such as the worst credible core meltdown and compaction accident, or as a result of the most severe credible sodium reaction. The design will take into account any environmental loadings, earthquake, high winds, etc. that the site, Middletown, U.S.A., might make necessary, in addition to normal static loads. (Criterion 10.2).

Rationale Supporting the Selection of the 1000-MWe Criteria

The specific criteria result from requirements expressed in Criteria 10, 40, and 70.

Compliance with the 1000-MWe Criteria

In calculating the upper bounds of pressure and temperature accidents, the core meltdown and sodium fire accidents were used. These accidents could not occur simultaneously since the containment is inert during power operation and refuelling. Only during major maintenance would air be allowed in the containment. During major maintenance the reactor is secured in a shutdown condition.

The pressure and temperature loadings, obtained by analyzing credible core meltdown and sodium reaction accidents, when combined with operating loads and maximum wind or seismic forces, do not exceed the load-carrying capacity of the structure, its access opening(s) or penetrations.

The containment will be constructed to prevent any leakage from normal and direct dose radiation from exceeding 10 CFR 100 under accident conditions and 10 CFR 20 under normal operation.

GENERAL CRITERION 50: NDT REQUIREMENT FOR CONTAINMENT MATERIAL

The selection and use of containment materials shall be in accordance with applicable engineering codes.
(Category A)

1000-MWe Criteria

- 50.1 The selection and use of containment materials will comply with the applicable codes and standards.
- 50.2 The concrete part of the containment will not be susceptible to low-temperature brittle fracture.
- 50.3 The containment ambient temperature during operation and testing will be such that the minimum service metal temperature of the containment lines or barriers is 30°F above the NDT temperature.
- 50.4 Containment penetrations that can be exposed to the environment must be designed to the NDT + 30°F criterion.

Rationale Supporting the Selection of the 1000-MWe Criteria

Designing to NDT + 30°F represents a safe compensation for the variability in homogeneous materials and provides a method of designing to the crack arrest properties of the materials involved. This is current practice, and the LMFBR requirements, at this stage, do not dictate a change.

Compliance with the 1000-MWe Criteria

The selection and use of containment materials will comply with applicable codes and standards. The outer containment will not be susceptible to low-temperature brittle fracture.

The inner steel containment vessel is enclosed within the outer containment and is not exposed to the temperature extremes of the environment. The containment temperature during operation will be well above the NDT temperature of the inner steel vessel material. Primary containment penetrations will also be designed to the NDT + 30°F criterion.

GENERAL CRITERION 51: REACTOR COOLANT BOUNDARY OUTSIDE CONTAINMENT

If part of the reactor coolant boundary is outside the containment, features shall be provided to avoid undue risk to the health and safety of the public in case of an accidental rupture in that part. (Category A)

1000-MWe Criterion

This criterion does not directly apply, since the reactor and primary coolant system of the 1000-MWe plant will be entirely enclosed within the reactor containment building. (Criterion 10.1)

GENERAL CRITERION 52: CONTAINMENT HEAT REMOVAL SYSTEMS

Where an active heat-removal system is needed under accident conditions to avoid exceeding containment design pressure, a system with adequate reliability and capacity shall be provided. (Category A)

1000-MWe Criteria

52.1 A heat-removal system for the containment will be provided if the containment has been designed to withstand a pressure less than the maximum transient pressure attained during the Credible Design Basis Accidents.

52.2 If a heat removal system is provided for the containment, the system will be designed to have adequate reliability and capacity.

Rationale Supporting the Selection of the 1000-MWe Criteria

The specific criteria conform to the general criteria.

Compliance with the 1000-MWe Criteria

The containment will be designed to withstand the maximum transient pressure attained during the Credible Design Basis Accidents. Therefore no heat-removal system will be required.

GENERAL CRITERION 53: CONTAINMENT ISOLATION VALVES

Penetrations that require closure for the containment isolation function shall be provided with redundant valving and associated apparatus or systems.
(Category A)

1000-MWe Criteria

- 53.1 Redundant valving for containment isolation in the event of an accident will be provided.
- 53.2 Valve capability and the sequence of operations leading to isolation of the containment will be tested periodically.
- 53.3 Isolation valves, on loss of power, will fail-safe either to an open or shut position, depending on which is the safest configuration.
- 53.4 Each line leading from the primary coolant system or containment volume to an outside environment will be provided with two independent isolation valves in series, each capable of automatic operation following high radioactivity signals, with a manual operation capability as a backup.
- 53.5 Each line leading either from the containment to a closed volume that is not the outside environment or from a volume inside the containment, not connected to the main containment volume, to the outside environment needs at least one isolation valve capable of automatic closure, with a manual operation capability as a backup.
- 53.6 One way inlet lines do not need automatically operated valves, but be provided with manually operated isolation valves as a minimum.

Rationale Supporting the Selection of the 1000-MWe Criteria

Criterion 53 is concerned with the isolation of the containment in the event of an accident that might result in a radioactive containment atmosphere. The specific criteria are written to avoid such a radioactive atmosphere from reaching the outside environment, automatically. Thus, the only lines that do not need automatic isolation valves are inlet lines that can be guaranteed to remain inlet lines under accident conditions.

Compliance with the 1000-MWe Criteria .

In addition to satisfying containment isolation criteria, the valving is designed to facilitate normal operation and maintenance of the systems and to ensure reliable operation of other engineered safety features. Systems design is such that failure of one valve to close does not prevent isolation, and no manual operation is required for immediate isolation. Automatic isolation is initiated by the containment isolation signal. Containment radioactivity level is measured by an activity monitoring system consisting of an atmosphere particulates detector and a radiogas detector. Output of the radiogas detector is recorded in the control room, and a high activity signal from either detector actuates an alarm in the control room and actuates the valves to the closed position. The redundant containment high activity channels meet the single component failure criterion. The basic isolation valve arrangements used to provide two barriers between the primary coolant system or containment atmosphere and the environment are described in the following paragraphs.

Normally operating outgoing lines connected to the primary coolant system are provided with at least one automatically operated trip valve and one manual isolation valve in series. In addition to the isolation valves, each line connected to the primary coolant system is provided with a remotely operated valve located near its connection to the primary coolant system.

Normally operating outgoing lines not connected to the primary coolant system are provided with at least one automatically operated trip valve or one remotely operated stop valve. Manual isolation valves in series with the trip or remotely operated valves are also provided unless the line is connected to a closed system outside containment.

Incoming lines connected to open systems outside the containment are provided with a check and a remotely operated valve.

Incoming lines connected to closed systems outside containment are provided with at least one check valve and manual isolation valve.

Because of their size, the containment or hot cell atmosphere conditioning and handling ducts are each equipped with two, tight-sealing butterfly type valves. These valves can be closed either manually or automatically upon a signal of high radioactivity level in the containment or by the containment isolation signal.

Lines that penetrate the containment and that may be opened to the containment atmosphere, but that are normally closed during reactor operation are provided with two isolation valves in series or one isolation valve and one blind flange.

In the detailed design of the nuclear plant systems, certain lines may require minor modification to the arrangements defined by the above descriptions, in order to implement the basic redundant barrier criterion.

GENERAL CRITERION 54 (55): CONTAINMENT LEAKAGE RATE TESTING

Containment shall be designed so that an integrated leakage rate testing can be conducted at the peak calculated accident pressure after completion and installation of all penetrations, and the leakage rate can be determined by test at reduced pressures during the plant lifetime. (Category A)

1000-MWe Criteria

- 54.1 The guaranteed leakage rates for the containment building and all its penetrations following isolation of the containment after the Credible Design Basis Accidents shall be such that there is no undue risk to the health and safety of the public. Licensing standards for radiation doses will be applied to the particular site of the plant.
- 54.2 Integrated leak testing of the isolated containment at the peak calculated accident pressure will be conducted after construction to verify the containment conformance with required performance.
- 54.3 Provision will be made in the design so that leak testing can be conducted on the overall containment and all penetrations at a reduced pressure at periods during life to verify the performance. The relation between test pressure and acceptable leak rate will be established during the first tests immediately after installation.
- 54.4 Access air-locks to the containment will be designed so that in depressurizing the space between air-lock doors, the fission products or other radioactivity will not be released to an area immediately surrounding the air-lock exit.

Rationale Supporting the Selection of the 1000-MWe Criteria

Criterion 54 requires the leak rate of the containment at peak calculated pressure to be verified experimentally initially and the capability provided for leak testing at reduced pressures during plant lifetime.

These requirements should provide a sufficient check of the containment integrity.

Compliance with the 1000-MWe Criteria

After completion of the total containment structure and installation of all penetrations, an initial integrated leakage rate test will be conducted at the peak calculated accident pressure (30 psig) and maintained for a minimum of 24 hours to verify that the leakage rate is no greater than 0.1% of the containment volume per day.

The absolute method will be used, and the test continued at one reduced pressure.

Integrated leak testing of the isolated containment using the same method as the initial leak rate test, but at reduced pressures, can be performed at any time during the operational life of the plant to verify its performance, provided that the plant is shut down and secured, and that precautions are taken to protect instruments and equipment from damage.

GENERAL CRITERION 56: PROVISIONS FOR TESTING OF PENETRATIONS

Provisions shall be made, to the extent practical, for periodically seals or expansion bellows to permit leak tightness to be demonstrated at the peak calculated accident pressure. (Category A)

1000-MWe Criteria

- 56.1 Prior to initial operation of the plant, penetrations that have resilient seals and/or bellows will be tested for leak tightness at the peak calculated accident pressure.
- 56.2 Provision will be made in the design for the leak testing of penetrations that have resilient seals or bellows at periods during plant lifetime to verify their performance. Such testing will be performed at reduced pressure using a relation between acceptable leak rate and test pressure established during the first tests immediately after installation.

Rationale Supporting the Selection of the 1000-MWe Criteria

The specific criteria merely fulfill the requirements of the general criterion.

Compliance with the 1000-MWe Criteria

A monitoring system will be provided such that all penetrations may be periodically checked for leak tight integrity during the operating life of the plant.

GENERAL CRITERION 57: PROVISIONS FOR TESTING OF ISOLATION VALVES

Provisions shall be made, to the extent practical, to test the valves and associated apparatus essential to the containment isolation function to determine if failure has occurred and to determine if valve leakage is within acceptable limits during periods of reactor shutdown. (Category A)

1000-MWe Criteria

- 57.1 Provision will be made for testing isolation valves individually throughout plant lifetime, to the extent practical, to check valving capability and to determine whether valve leakage is within acceptable limits.
- 57.2 Provision will be made to test the operational sequence of the automatic isolation function.

Rationale Supporting the Selection of the 1000-MWe Criteria

Criterion 57, requiring the testing of valves and their automation, is separated into the testing of the mechanical operation of the valves themselves and the testing of the sequence of automatic operations that cause their closure (between the reception of a high radioactivity signal and the isolation function).

Compliance with the 1000-MWe Criteria

Capability is provided, to the extent practical, for testing the functional operability of isolation valves and associated apparatus during periods of reactor shutdown.

Isolation valves will be pressure tested to measure leakage. Pressure tests of isolation valves in series will be performed in such a manner that leakage through either valve alone will be detected. The containment isolation control system employs circuits designed so as to allow checking of the operability and calibration of one channel at a time.

ENGINEERED SAFETY FEATURES

D. Containment Pressure Reducing Systems

GENERAL CRITERION 58: INSPECTION OF CONTAINMENT PRESSURE-REDUCTING SYSTEMS

If the containment has a pressure-reducing system, design provisions shall be made, if practicable, to facilitate the periodic physical inspection of all important components of the containment pressure-reducing systems; such as, pumps, valves, spray nozzles, torus, and sumps.
(Category A)

1000-MWe Criteria

Presently, the 1000-MWe design does not employ a containment pressure-reducing system; therefore, there are no specific criteria.

GENERAL CRITERION 59 (60): TESTING OF CONTAINMENT PRESSURE-REDUCING
SYSTEMS COMPONENTS

If the containment has a pressure-reducing system, the system shall be designed, if practicable, so that active components, such as pumps and valves, can be tested periodically for operability and required functional performance. (Category A)

1000-MWe Criteria

Presently, the 1000-MWe design does not employ a containment pressure-reducing system; therefore, there are no specific criteria.

GENERAL CRITERION 61: TESTING OF OPERATIONAL SEQUENCE OF CONTAINMENT
PRESSURE-REDUCING SYSTEMS

If the containment has a pressure-reducing system, a capability shall be provided, if practicable, to test initially under conditions as close as practical to the design and the full operational sequence that would bring the containment pressure-reducing systems into action, including the transfer to alternate power sources. (Category A)

1000-MWe Criteria

Presently, the 1000-MWe design does not employ a containment pressure-reducing system; therefore, there are no specific criteria.

ENGINEERED SAFETY FEATURES
E. Air Cleanup Systems

GENERAL CRITERION 62 (63 to 65): INSPECTION AND TESTING OF AIR CLEANUP SYSTEMS

Provisions in the design of the air-cleaning system shall be made, to the extent practical, (a) to facilitate the physical inspection of all critical parts such as ducts, filters, fans and dampers, (b) to periodically test active components such as fans and dampers, (c) to ensure that filter bypass paths have not developed and that filter and trapping materials have not deteriorated beyond acceptable limits, and (d) to test initially under conditions, as close as possible to design and the full operational sequence which would bring the air cleanup systems into action, including the transfer to alternate power sources to determine if air flow delivery is acceptable. (Category A)

1000-MWe Criteria

- 62.1 Provisions will be made where practicable to allow inspection of critical parts of the air-cleanup system, such as ducts, filters, fans, and dampers at all times during reactor plant lifetime.
- 62.2 Periodic testing of fans and dampers will be required.
- 62.3 Filter inspection will be possible at all times, and testing for filter by-passes, that may have developed, will be carried out.
- 62.4 Provision will be made to test the air-cleanup systems under conditions as close to design as possible. The test would include the transfer of the system to alternative power supplies, and would be repeated periodically throughout the life of the plant.

Rationale Supporting the Selection of the 1000-MWe Criteria

Criterion 62 refers to the necessity for having reliable air cleanup systems on hand at all times and particularly under accident conditions. The air-supplies referred to relate to any breathing supply available to

personnel (control room, manned access areas, etc.) and to any air supplies that might be normally exhausted to the outside environment, unless these are covered by isolation procedures, in the event of an accident.

Compliance with the 1000-MWe Criteria

Provisions will be made to inspect and test the air cleanup systems. This will be done initially under conditions as close to design and full operation as possible. The test will include transfer of the system to alternative power supplies, and it will include air flow measurements. The test may be repeated periodically throughout the life of the plant.

FUEL AND WASTE STORAGE SYSTEMS

GENERAL CRITERION 66: PREVENTION OF FUEL STORAGE CRITICALITY

Criticality in new and spent fuel storage shall be prevented by physical systems or processes; such means as a geometrically safe configuration and neutron absorbers shall be emphasized over procedural controls. (Category B)

1000-MWe Criteria

- 66.1 Where practical, criticality within new fuel and spent fuel handling storage areas will be prevented by the geometric design of fuel assembly storage positions and shipping casks.
- 66.2 Where possible, neutron absorbing materials will be used within new and spent fuel handling and storage areas to provide additional safeguards against criticality; in particular, the possibility of using neutron absorbers within structural materials will be considered.
- 66.3 Strict procedural controls will be enforced to ensure that fuel storage positions are used correctly, that an accurate inventory and a record of movement of fuel is kept, and that operators are aware of their responsibility.
- 66.4 A single fuel element will be designed to remain subcritical at all times, even when totally immersed in water.

Rationale Supporting the Selection of the 1000-MWe Criteria

Although the general criterion states that the prevention of criticality by geometry and by the use of neutron absorbers should be emphasized over procedural controls, nevertheless, all three methods will be applied.

Compliance with the 1000-MWe Criteria

New fuel is received from the fabrication plant in sealed containers that are temporarily placed in storage racks within the nonirradiated fuel storage vault. The container geometry will prevent criticality under all

conditions. The new fuel assemblies are de-canned one-by-one and moved into the fuel storage tank.

Within the fuel storage tank, fuel is stored in three racks, each containing a square array of 17 x 15 storage positions providing under-sodium storage for 765 fuel elements. The racks are made of stainless steel. The fuel sits approximately seven feet within the rack (approximately 10-foot fuel assembly lengths). The fuel area of each core element is completely surrounded by poison, but not the upper or lower axial blankets of the core assemblies.

All racks are poisoned throughout, thus obviating the need for administrative procedures to separate core and blanket subassemblies. Fuel positions are in a 6.7-inch square array. A 1.4-inch channel between the fuel subassemblies is made of 0.69-inch thick, 65% dense, B₄C clad in stainless steel. The poison plates are fabricated individually, then secured in the fuel storage racks. Fuel pit sodium accounts for the additional 0.46 inch of space between the subassemblies. In addition, a 2-foot x 4-foot rack is positioned along the east wall of the fuel tank and contains space for 72 new or used control rods.

Spent fuel assemblies are removed one-by-one and sealed in cans prior to shipping to the reprocessing plant. The can - shipping cask geometry and materials preclude inadvertent criticality.

An accurate record of the location and history of all fissile material on a site is mandatory. An automatic data logging and recording system provides a means of record-keeping along with providing assurance that the refueling operation was accomplished as planned.

A system under present consideration consists of a programmed input compared to the actual machine operations. A printout unit prints out the programmed code and, immediately below this, prints out the actual machine operations (locations assumed, sequence of operation, etc.). Any discrepancy between programmed input and actual operation would automatically alarm and stop operations until reset or errors are corrected. Such an automatic data logging and recording system would in turn interface with a fuel-handling data processing system for record keeping purposes.

Verification of fuel handling machine operations and data logging is performed by operators. Suitable training and testing programs assure operator competence.

The 1000-MWe fuel assembly design precludes criticality when fully immersed in water.

GENERAL CRITERION 67: FUEL AND WASTE STORAGE DECAY HEAT

Reliable decay heat removal systems shall be designed to prevent damage to the fuel in storage facilities that could result in radioactivity release which would result in undue risk to the health and safety of the public. (Category B)

1000-MWe Criteria

- 67.1 Decay heat removal cooling capability will be provided within spent fuel storage areas to prevent damage to the fuel. When the spent fuel is stored within sodium, the heat removal system should be capable of maintaining the sodium temperature at 300 to 400°F.
- 67.2 Decay heat removal capability must also be provided during spent fuel transfer, during fuel handling, and during shipping by cask.
- 67.3 Waste storage areas will be provided with provision for cooling capability.
- 67.4 All cooling will be supplied by circulating inert gases, by circulating sodium or NaK, or by providing large structural heat sinks.

Rationale Supporting the Selection of the 1000-MWe Criteria

Criterion 67, which requires the prevention of fuel damage that might result in a release of radioactivity by keeping the fuel relatively cool, is here separated into more specific sections. No particular problem is assumed to arise because the reactor coolant is sodium, except for the need to exclude water and oxygen.

Compliance with the 1000-MWe Criteria

Transfer of spent fuel from the reactor to the fuel storage tank is accomplished under primary sodium. As a result, no cooling provisions are required in the design of the fuel-handling equipment. The "canless" design of the fuel assemblies permits effective natural convection cooling in the horizontal position.

Cooling of spent fuel within the fuel storage tank is accomplished by circulating NaK through cooling coils immersed in the sodium. The NaK cooling coils form a part of the NaK service system which provides a completely redundant capability.

Argon cooling of spent fuel is provided during removal and transfer from the spent fuel storage tank and in preparation for canning and shipping. Spent fuel will be shipped to the reprocessing plant in casks designed in compliance with 10 CFR 71.

Cooling capabilities are provided as required in waste storage tanks and areas.

GENERAL CRITERION 68: SHIELDING AND WASTE STORAGE RADIATION SHIELDING

Adequate shielding for radiation protection shall be provided in the design of spent fuel and waste storage facilities as required to meet the requirements of 10 CFR 20. (Category B)

1000-MWe Criteria

- 68.1 While spent fuel is in storage, adequate gamma shielding will be designed to be included within the structure of the storage area to prevent excessive radiation levels outside the area.
- 68.2 During fuel transfer, adequate shielding will be provided in the design to prevent excessive radiation levels.
- 68.3 Casks that are used to transport spent fuel and solid wastes outside of containment shielding will be designed to provide adequate radiation shielding.
- 68.4 Waste storage tanks for solid and liquid wastes awaiting disposal will be adequately shielded for radioactivity protection.
- 68.5 Radiation in all areas close to spent fuel storage or waste storage facilities will be limited so that the equivalent dose to personnel in those areas would always be less than a maximum of one rem per 13 week quarter.

Rationale Supporting the Selection of the 1000-MWe Criteria

Criterion 68, requiring radiation shielding for spent fuel and radioactive wastes, is further detailed by the specific criteria. Quantitative limits of radiation values will be further defined in the Title I design, but are, at present, unavailable.

Compliance with the 1000-MWe Criteria

The fuel storage pit is provided with a seven-inch-thick steel cover. The cover and the reactor shield plug are sized to allow personnel access to the hot cell with the covers in place, during reactor operation. A gas-tight seal is provided to prevent fission products from escaping into the hot cell during operation, and also allows an infrequent, but necessary, conversion of the hot cell atmosphere from argon to air without the danger of sodium fire.

During fuel-handling operations and when the covers are removed from the reactor vessel and spent fuel pit, personnel access to the refueling cell is not permitted. The six-foot-thick cell walls are sized to reduce radiation outside the cell to acceptable levels.

Permanent and temporary shielding is provided, as required, in other portions of the fuel handling and waste storage systems. Shielding for the spent fuel shipping cask is designed to comply with 10 CFR 71.

GENERAL CRITERION 69: PROTECTION AGAINST RADIOACTIVITY RELEASE FROM THE
SPENT FUEL AND WASTE

Provisions shall be made in the design of fuel and waste storage facilities to avoid release of radioactivity which would cause undue risk to the health and safety of the public. (Category B)

1000-MWe Criteria

- 69.1 Adequate shielding and leak integrity will be provided for the storage areas. (Criterion 68.)
- 69.2 Continuous monitoring of fuel and waste storage facilities will be provided. Automatic visual and audible displays of high radioactivity signals will be provided, and cleanup facilities will be made available.
- 69.3 Transfer of spent fuel and waste from one storage facility to another will be made under strict procedural controls, with adequate radiation shielding and remote handling methods.
- 69.4 Waste materials, be they gaseous, liquid, or solid, should be subject to strict inventory controls up to the time when they are finally disposed of through treatment plants.

Rationale Supporting the Selection of the 1000-MWe Criteria

Criterion 69, to avoid radioactivity release from fuel and waste storage facilities, is further detailed by the specific criteria. These criteria are seen to be inclusive of Criterion 68. Quantitative levels for radioactivity limits will require specification in the Title I design, since at the present stage of the conceptual design, they are not defined.

Compliance with the 1000-MWe Criteria

All fuel storage and waste handling and storage facilities are contained, and equipment is designed so that any release to the atmosphere is continuously monitored and will not exceed the limits of 10 CFR 100. Displays and cleanup facilities are provided as required.

The reactor refueling cell contains a welded steel liner and is operated at a negative pressure with respect to the atmosphere to preclude outleakage of radioactive contaminants. Except during fuel-handling operations, leakage is further controlled by cover seals on the reactor vessel and fuel storage tank.

Inventory controls are provided for all radioactive materials on the reactor site.

Shielding is discussed under Criterion 68.

PLANT EFFLUENTS

GENERAL CRITERION 70: CONTROL OF RELEASES OF RADIOACTIVITY TO THE ENVIRONMENT

The facility design shall include those means necessary to maintain control over the plant radioactive effluents, whether gaseous, liquid, or solid. Appropriate holdup capacity shall be provided for retention of gaseous, liquid, or solid effluents, particularly where unfavorable environmental conditions can be expected to require operational limitations upon the release of radioactive effluents to the environment. In all cases, the design for radioactivity control shall be justified (a) on the basis of 10 CFR 20 requirements for normal operations and for any transient situation that might reasonably be anticipated to occur, and (b) on the basis of 10 CFR 100 dosage level guidelines for potential reactor accidents of exceedingly low probability of occurrence. (Category B)

1000-MWe Criteria

- 70.1 Liquid, gaseous, and solid waste disposal facilities will be designed so that discharge of effluents and off-site shipments are in accordance with applicable governmental regulations.
- 70.2 The design will include provisions for the retention of high activity gaseous products within the primary coolant treatment loop and gas storage tanks.
- 70.3 Provision will be made for the retention and/or control release of all high activity solid, liquid, and gaseous products resulting from normal or accident conditions.
- 70.4 Radioactivity control will be on the basis of 10 CFR 20 requirements for normal operation and for transient situations which might reasonably be anticipated to occur and on the basis of 10 CFR 100 for potential accidents that have a very low probability of occurrence.

Rationale Supporting the Selection of the 1000-MWe Criteria

The ability to retain, process, and release in a controlled manner all high activity products, even under accident conditions, provides absolute control over the dosage received at the site boundary. This retention ability guarantees that under normal operating conditions, the requirements of 10 CFR 20 will be met, and that under accident conditions, 10 CFR 100 will not be exceeded. With this type of holdup system, there is a good possibility of adhering to 10 CFR 20 under accident conditions.

Compliance with the 1000-MWe Criteria

Liquid, gaseous, and solid waste disposal facilities will be designed so that discharge of effluents and off-site shipments are in accordance with applicable governmental regulations.

Radioactive fluids entering the waste disposal system will be collected in sumps and tanks until determination of subsequent treatment can be made. They will be sampled and analyzed to determine the quantity of radioactivity with an isotopic breakdown if necessary. Before any attempt is made to discharge, they will be processed as required and then released under controlled conditions.

The systems design and operation will be characteristically directed toward minimizing releases to unrestricted areas. Discharge streams will be appropriately monitored, and safety features will be incorporated to preclude excessive releases.

Radioactive gases will be pumped by compressors through a manifold to one of the gas decay tanks where they will be held a suitable period of time for decay. During normal operation, gases may be discharged intermittently at a controlled rate from these tanks through a monitored vent.

Liquid wastes will be processed to remove most of the radioactive materials. The spent resins will be packaged and stored on site until shipment off-site for disposal.

All solid waste will be placed in suitable containers and stored on-site until shipment off-site is made for disposal.

Part 2

SUMMARY OF DIFFERENCES FROM AEC GENERAL CRITERIA

INTRODUCTION

This section contains a summary of the differences between the AEC-proposed General Design Criteria for Nuclear Power Plant Construction and the general design criteria proposed by the Westinghouse Advanced Reactors Division for Liquid Metal Fast Breeder Reactor Power Plants. The changes in the criteria are based upon design experience gained on the 1000-MWe LMFBR Follow-On Study Program and upon comments on the AEC-proposed criteria by the Westinghouse Atomic Power Divisions* and the Atomic Industrial Forum Inc.**

GENERAL DIFFERENCES

Some of the changes are general and apply to several of the criteria. These changes are as follows:

- a. The phrase "acceptable fuel damage" that appears in many of the AEC criteria implies that safety margins are too low and that the fuel can be damaged under acceptable operational conditions. The phrasing "without exceeding fuel conditions consistent with public health and safety protection" is used in the LMFBR criteria.
- b. In all references to the reactor coolant pressure boundary, the word "pressure" has been deleted because the LMFBR is a low-pressure system, and reference to a pressure boundary connotes a high-pressure system.
- c. Some of the AEC criteria have been written more concisely in the LMFBR criteria without changing the intent of the AEC criteria.

*Comments on AEC-Proposed "General Criteria for Nuclear Power Plant Construction Permits," attachment to a letter from J. C. Rengel, Vice-President Westinghouse Atomic Power Divisions, to Secretary U. S. Atomic Energy Commission, September 8, 1967.

**Comments of Forum Committee on Reactor Safety on AEC's Proposed Construction Permit Criteria, attachment to a letter from Edwin A. Wiggen, Committee Secretary AIF, to Secretary U. S. Atomic Energy Commission, October 2, 1967.

SPECIFIC DIFFERENCES

Specific differences between the AEC-proposed general design criteria and the proposed LMFBR general design criteria are listed below. In order to avoid lengthy explanations, we will assume that the reader has the AEC-proposed criteria for comparison with the LMFBR criteria. Therefore, only the differences will be discussed.

Criterion 1

In the first sentence, we have modified "accidents" with "nuclear" to make it clear that the criterion deals with nuclear accidents that could cause undue risk to the health and safety of the public. In the last sentence, we have eliminated the word "sufficiency". We do not believe that it should fall upon the applicant to show the sufficiency or adequacy of a code or standard. We strongly feel that the question as to sufficiency or adequacy of codes and standards should be taken up with the appropriate codes or standards committee, and modifications of such codes and standards should be through the machinery provided by professional and technical societies in cooperation with the United States of America Standards Institute. Note, however, that we have added a sentence requiring a showing of adequacy where there is no applicable code.

Criterion 2

The word "additional" was deleted to avoid the implication that the applicant should consider simultaneously or cumulatively, the forces of more than one extraordinary natural phenomenon.

Criterion 4

This criterion, as originally drafted, being negative in nature, implies that there is something basically wrong with equipment sharing. It also imposes an unreasonable restriction on sharing of equipment if safety is any way impaired without regard to the efficiency of the resulting system. Our proposed revision restates the criterion in a positive sense and relates the question of sharing or not sharing equipment to the requirement of no undue risk to the health and safety of the public.

Criterion 5

We have modified this criterion to require that the reactor operator assure the maintenance of essential records, but to allow for the fact that the actual records may be on file with the vendor or designer in many cases. We have also added a phrase to define "essential" as those that are necessary to avoid undue risk to the health and safety of the public.

Criterion 6

In the first sentence of this criterion, we have added a reference to the control and protection, since the reactor core, by itself, cannot be designed to meet the criteria. The definition of acceptable fuel damage limits, we believe, should be a part of supplementary criteria.

Criterion 7

As in Criterion 6, we have added reference to the control and protection systems that are necessary to comply with this criterion.

Criterion 8

The AEC criterion requires that the power coefficient be nonpositive; whereas, the LMFBR criterion requires a nonpositive coefficient only for reactivity changes associated with a rapid increase in power. This change permits greater flexibility in the design of the reactor and its control system without diminishing the capability of the system to control against potential nuclear accidents.

Criterion 9

We believe that very low probability is more appropriate and reasonable than exceedingly low probability. One might interpretate low probability to mean that each design must have a lower probability than each preceding design, for example. We also believe that the use of the term "abnormal leakage" would be more appropriate than "significant leakage".

Criterion 10

The title of this criterion was changed to "reactor containment" and the phrase "reactor containment or equivalent protection" was included in the first sentence, both to avoid ambiguity in the term "containment" as well as to allow for the possibility of future development of other means of providing the same protection. The intent of this criterion has not been changed; however, it was necessary to change the design requirements to suit the potential accidents of the LMFBR plant.

Criterion 11

As originally drafted, this criterion could be interpreted to require a second control room. We do not believe it is practical nor in the interest of safety to have such a requirement. Accordingly, we have deleted the last sentence in the criterion. We have also deleted the reference to 10 CFR 20 limits to radiation exposure. This requirement is not consistent with current practice nor is it appropriate or reasonable for highly unlikely, though credible, accident situations.

Criterion 12

We have modified the variables to be those that are essential to avoid undue risk to the health and safety of the public.

Criterion 13

This criterion has been modified to make it clear that continuous monitoring and continuous control are not always necessary, but that the frequency of measurement and exercise of control should be related to the requirements imposed by anticipated rates of change of those variables being monitored or controlled. The example given in the last sentence "...and concentration of soluble reactivity control poisons." was deleted because it is not applicable to a LMFBFR.

Criterion 14

The word "automatically" was deleted. We believe that manual action in some cases will be adequate and, in fact, even desirable, and that the requirement for automatic control action should be judged on the merits of each application relative to avoiding undue risk to health and safety of the public.

Criterion 20

The last sentence of the AEC general criteria has been deleted. It would appear preferable to provide duplicates of the test system or component rather than going to an inferior system or component based on a different principle.

Criterion 21

We have deleted this criterion since it is more of a definition than a criterion, and since the implied requirement is adequately covered by Criterion 23.

Criterion 22

In the AEC general criteria, this criterion could be interpreted to require redundant protection, assuming failure of all common instrumentation. It has been modified to state "or any one of those common to control..."

Criterion 25

The reason for the changes here is that the licensee should be given some latitude in determining when and how such tests should be carried out. Further, he should be required only to test the active components of a protection system in contrast, for example, to a rupture diaphragm that could only be tested at the expense of destroying it. Also, certain tests might permit the licensee to determine if failure or loss of redundancy has occurred; but, they might not permit him to demonstrate it.

Criterion 27

We have eliminated the words "at least" from this criterion. Since these criteria are essentially minimal requirements, the phrase "at least" is redundant. Also, there is a strong implication that really more than two independent reactivity control systems are desired.

Criterion 28

Deletion of the preface phrase, "at least two of" is based on a comment made in Criterion 27. We have deleted the requirement for fast shut-down, since this is covered in Criterion 29.

Criteria 29-30

Since these two criteria are so closely related, they were combined into a single criterion for the sake of conciseness. Deletion of the preface phrase, "at least", is consistent with the comments on Criteria 27 and 28. Also, the word "core" was replaced by the word "reactor" which is better suited to a fast breeder reactor. The other editorial changes are for purposes of clarification.

Criterion 31

We have reworded this criterion to reflect what we believe to be the intent of the criterion, recognizing that the reactor protection system is provided to protect against reactivity control system malfunctions.

Criterion 32

We have modified the first sentence to replace the word "considerable" with "reasonable" which we feel more accurately reflects the intent of the criterion. In the last sentence, we have changed "to impair the effectiveness of emergency core cooling" to the phrase "to lose capability to cool the core," which we again believe to be a more accurate statement of the intent of the criterion and consistent with current practice.

Criterion 33

We have deleted the phrase "and with only limited allowance for energy absorption through plastic deformation." We believe that the phrase "accommodating without rupture" is sufficient and that the designer should be allowed to define the margin to rupture on the basis of the particular situation with which he is dealing. If limits are to be applied to the amount of plastic deformation to be permitted, they should be dealt with in supplementary criteria. Also, we have inserted the word "credible" to make it clear that the reactor coolant boundary will be designed to accommodate without rupture the consequences of a credible accident, i.e. it will not be designed to accommodate the core meltdown and compaction accident without rupture.

Criteria 34-35

These criteria have been reworded and combined into a single criterion. Where the requirements of this criterion need to be specified in more detail than in the suggested redraft, this should be done in supplementary criteria. In the first sentence we have replaced the word "minimized" with "reduced to an acceptable level", which we believe has more meaning.

Criterion 36

It should not be necessary to inspect or maintain surveillance over all portions of the coolant boundary; hence, we have inserted the phrase, "of selected areas." Also, we believe that both the applicant and the AEC are in a better position to take advantage of developing technology and code refinement if these general design criteria referred to "current applicable codes" rather than to specifically designated codes.

Criterion 37

We have deleted the phrase "as a minimum" since this is the general intent of the criteria as a whole and, therefore, is unnecessary. Also, we have reworded the criterion to imply that any credible coolant piping break should be accommodated, but that the circumferential rupture of any pipe with unobstructed discharge from both ends is not necessarily credible--for example, in concrete pressure vessel integral designs.

Criterion 38

We have deleted the word "high" in "high functional reliability" and have inserted the phrase "as is necessary to avoid undue risk to the health and safety of the public" after the word "testability" in order to more adequately define the degree of reliability and testability necessary. We have eliminated the remainder of the criterion because it is a statement of philosophy that does not appear to be necessary as a part of this criterion.

Criterion 39

We have reworded this criterion so that it does not arbitrarily rule out the use of an off-site source of emergency power and that source of power is under the control of the operator and has sufficient redundancy and capacity. We have also eliminated reference to application of the single failure criteria to off-site power sources other than the emergency power source in that it is impractical to require that the operator provide off-site power connections to his station that can sustain any single failure. If it were really practical to achieve this objective with respect to off-site power, then perhaps there would be no need for provision of additional emergency power.

Criterion 40

We have reworded this criterion to make it more clear that protection of the engineered safety features is necessary only if the failure to provide the protection results in an undue risk to the health and safety of the public. For example, if an engineered safety feature were to be damaged by a missile, but that missile was not associated with any situation that would require the operation of that engineered safety feature to protect the public, then protection against the effects of the missile would not be necessary.

Criterion 41

We have modified this criterion for clarity and simplicity by substituting the failure of any single active component for partial loss of installed capacity and redefining the safety function in terms of risk to the health and safety of the public.

Criterion 42

Although it would appear extremely difficult, if not impossible, to design engineered safety features in such a way that a credible accident will cause no impairment of the capability of any component or system, it is possible to design them to meet the requirements of this criterion as it has been rewritten.

Criterion 43

The intent here was simply to state the criterion in a more positive way.

Criterion 44

We have reworded this criterion to eliminate the arbitrary requirement for two emergency core cooling systems. We strongly believe that one emergency core cooling system incorporating adequate redundancy of active components and designed to provide protection over the full range of postulated pipe breaks such that adequate reliability is assured is sufficient. With the criterion as proposed, two active systems could be supplied that meet the criterion, while a single passive system, that could do the same function far more reliably, could not meet the criterion. Also, the word "system" has been deleted from the title. By this deletion, we wish to imply that the core may have emergency cooling capability without necessarily having a system that is specifically an emergency core-cooling system. This philosophy is carried over into Criteria 45-48.

Criteria 45-48

Since all of these criteria apply to the inspection and testing of the system that provides emergency core cooling, they were combined for conciseness. The changes in the criteria are as follows:

- a. In the first sentence, we have added the phrase "where practical" to recognize the fact that there can be cases where such provisions as called for in Criterion 45 are not feasible, or they compromise some other more necessary provision. We have also modified the wording to clarify what we believe was an intent to insure that emergency core-cooling systems would be interpreted as including parts of other systems which perform necessary functions with respect to emergency core cooling.
- b. Testing the "operativeness" in contrast to the "delivery capability" of the emergency core-cooling system "up to" rather than "at" a location close to the core more accurately reflects the art of the possible and should provide for as adequate a test of reliability.
- c. With respect to testing the full operational sequence of emergency core cooling, the only change here, and a significant one we believe, is insertion of the word, "initially." Although we concur that a capability to test the operational sequence of the emergency core-cooling system should be provided, the test as a practical matter would not be carried out frequently and possibly not more than once -- prior to start-up.

Criterion 49

The objective of this criterion, in our opinion, should be that under the circumstances of an accident, the integrity of the containment should be such as to prevent leakage of radioactive material that would result in an undue risk to the health and safety of the public. Since the maintenance of containment integrity is based on effective functioning of the system that provides emergency core cooling, it appears unreasonable in this criterion, to assume the complete failure of the cooling system; hence we have assumed the failure of a single active component. Consistent with this assumption, we believe that the pressure and temperature to be withstood should be characteristic of those anticipated from the maximum credible energy release resulting from the worst credible accidents such as core meltdown accident (Criterion 10) and the maximum credible sodium reaction accident.

Criterion 50

It appears to us that the specific requirements of this criterion, as originally drafted, were not in keeping with the intent of general design criteria.

Criterion 51

We have modified the first sentence of this criterion to be consistent with the philosophy of avoiding undue risk to the health and safety of the public. The last sentence has been deleted on the basis that it is unnecessary since it merely restates the requirement to avoid undue risk to the health and safety of the public.

Criterion 52

This criterion has been reworded to require a single containment heat removal system with adequate reliability and compacity. This is consistent with our revisions to Criterion 44.

Criterion 53

In this criterion we have inserted the word "isolation" to more clearly define the containment function referred to and have restated the requirement so that redundant valving shall be provided.

Criteria 54-55

These criteria have been combined since they both refer to containment leakage rate testing. We have substituted "the peak calculated accident pressure" for "design pressure," since these criteria should reflect minimal requirements. Note also that it is only the initial testing that will be

conducted at the peak calculated accident pressure. A requirement calling for periodic leak testing at design pressure would impose an unnecessary and impractical design requirement on the plant. Therefore, we have stated that periodic leak testing will be done at reduced pressures throughout the plant lifetime.

Criterion 56

We have inserted the word, "periodically", to avoid an interpretation that we do not believe was intended, namely a requirement for "continuous" testing. Also, we have added the phrase "to the extent practical" as in comments on earlier criteria. In this criterion, we have related the test conditions for penetrations to the peak calculated accident pressure rather than to the designed pressure as in Criteria 54 and 55.

Criterion 57

As in Criterion 56, we have added the phrase "to the extent practical." We believe it sufficient to be able to perform this testing during periods of reactor shutdown, and have modified the criterion accordingly. We have also changed the wording to more clearly identify the containment function as the containment isolation function and to indicate that the purpose of the test is to determine the status of the isolation valves.

Criteria 58-61

Although the containments of current LMFBR designs do not have pressure reducing systems, such systems may be feasible, so these criteria were left in. Terms that apply specifically to water reactors were deleted. Also, we have added the phrase "if practicable". The word practicable seems appropriate here because practicable, by definition, applies to that which has not yet been worked out or fully tested, but seems feasible.

Criteria 62-65

To be more concise, these criteria were combined into a single criterion. We have added the phrase "to the extent practical" as in comments on earlier criteria. Regarding the testing of the full operational sequence, we have inserted the word "initially", since such a test would be carried out very infrequently and probably not more than once.

Criterion 67

We have substituted "which would result in undue risk to the health and safety of the public" for "to plant operating areas or the public environs" since we believe the first phrase more accurately describes the responsibility of the licensee.

Criterion 68

The suggested change permits the criterion to accommodate radiation limits as may be specified which may differ from those set forth in 10 CFR 20.

Criterion 69

We have modified the wording in this criterion to allow the designer flexibility to choose how he shall control the release of radioactivity by substituting "provisions to avoid the release of radioactivity which could cause undue risk to the health and safety of the public" for the word "containment."

Criterion 70

We have deleted the qualification on condition (b) namely, "except that reduction of the recommended dosage levels may be required where high population densities or very large cities can be effected by the radioactive effluence." This qualification is not helpful and could be subject to misinterpretation by the uninformed public.

Part 3

SURVEY OF MALFUNCTIONS

INTRODUCTION

A preliminary safety review of the 1000-MWe reference concept was carried out, and the results are presented in this section. This review centered principally around the development of a fault tree analysis to identify faults or malfunctions that could lead to reactor core damage.

A fault tree analysis is a procedure for logically working backward from a particular end condition or event (damage reactor core) to determine all possible causes of the end condition or event. The fault tree display in Figures 1 through 12 graphically presents the causes, consequences, and interrelationships for faults that can lead to core damage. The procedure of subdividing or branching downward on the fault tree was continued until a unique malfunction, failure, or operational error was identified that corresponded, in a level of detail, to the available information on the 1000-MWe reference plant.

Also, as a part of the preliminary safety review, the probable sequence of events following each fault was defined, and the safety considerations that affect the outcome of the accident were reviewed. These safety considerations included (a) safety related assumptions made during the conceptual design of the plant, (b) the effect of inherent safety features, and (c) the action of core protective systems that are a part of the reference design. For each fault, one or more equivalent "Initiating Conditions for Reactor Accidents" was defined.* The results of this review are summarized in Table 1. Note that the items in the list of malfunctions are keyed to the fault tree.

*An "Initiating Condition for Reactor Accident" is defined as a unique perturbation to an intact operating reactor (considering only the reactor core and primary vessel internals), resulting from a malfunction or fault, which if uncorrected could cause irreversible damage to the reactor core. For example, a pump failure would be classified as a "malfunction," whereas the corresponding "Initiating Condition for Reactor Accident" would be loss of coolant flow.

SEE FIGURE 12
FOR LEGEND

PRELIMINARY FAULT TREE - 1000 MWe LMFBR
FOLLOW-ON STUDY

2058-1

Figure 1

(Figure 1)

2 053-2

Figure 2

Figure 3

(Figure 3)

2053-5

Figure 5

Figure 7

Figure 8

(Figure 1)

2053-9

Figure 9

Figure 11

SOURCE ERROR
SOURCE FAILURE
SOURCE PROBLEM
ETC

CATAGORIZATION
TITLE BLOCK FOR
FAILURE GROUP OR
PROBLEM GROUP

EITHER EVENT IS
SUFFICIENT
FOR PROPAGATION
OF FAILURE MODE

BOTH EVENTS ARE
NECESSARY FOR
PROPAGATION OF
FAILURE MODE

AN ADDITIONAL
CONDITION ASSOCIATED
WITH A FAILURE MODE

LEGEND FOR FAULT TREE

2053-12

TRANSFER NUMBERS IN THE "OR" - "AND" -
"FLAG" GATES IMPLIES THAT THE FAILURE
MODE THAT HAS ACCUMULATED UP TO THIS
POINT WILL BE BORROWED AS AN INPUT TO
ANOTHER PART OF THE FAULT TREE.

INPUT ARROW WITH TRANSFER NUMBERS
IMPLIES THAT THE REFERENCED CONDITIONS
ARE BORROWED FROM ELSEWHERE IN THE
FAULT TREE AND INSERTED HERE.

Figure 12

TABLE 1

SAFEGUARDS REVIEW

MALFUNCTION	RELATED MALFUNCTION	INITIATING CONDITION FOR REACTOR ACCIDENT	SAFEGUARDS
Primary Coolant System Rupture (Figure 2)		A pipe rupture as a single event lowers the core sodium level and reduces core coolant flow. With the additional failure of the sodium level reactor trip the cladding will exceed temperature limits and core damage will occur.	Sodium released by such an event will be retained within an inert gas envelope surrounding the primary system. Low operating pressure of the sodium coolant eliminates stored energy as a mechanism for damage propagation. The inerted heat exchanger cells and annulus surrounding the core vessel are designed for the limited temperature and gas pressure rise caused by escaping sodium. Core damage due to the transient reduction of coolant flow during a great or small pipe rupture is limited by sodium level trip with back up of temperature trip and sodium flow loss trip. The auxiliary core cooling system nozzle will remain under sodium maintaining sufficient sodium circulation to remove after glow heat.
Inadvertent System Drain (Figure 2)		The removable spool section of the drain line is reassembled and the core is drained with fuel subassemblies in the reactor. Loss of coolant causes the temperature limit of the cladding to be exceeded with possible core damage.	Draining of the reactor as a single event is guarded against by design and procedure. Normal drain service to the primary system connects to low points of the heat transfer system but not to the reactor. Filling service will be by the same or similar lines. Core drain service will not be continuously available, but normally will be blanked off with a spool section removed. Procedure will require assurance of low core heat and low reactivity prior to reconstructing the blanked-off spool section. It is credible that heat transfer loops can be subjected to inadvertent drain, but low sodium level alarms and trip prevents gross damage.
Reactor Vessel Leak and Safety Vessel Leak (Figure 2)		A simultaneous rupture of the lower region of both the core vessel and the safety vessel causes the loss of core sodium with baring of the core and blanket. Due to lack of cooling the temperature limit of the fuel cladding is exceeded and the core is damaged.	A lower region rupture of both vessels is not credible. A rupture of either vessel will not cause gross core damage. The low sodium level reactor trip and temperature protective circuits limit core damage.
One Primary Pump Failure (Figure 2)	Check Valve Failure	At power, one primary pump fails while the other primary pump continues to pressurize the reactor inlet sodium plenum. Also, the check valve on the inoperative loop fails to close against backflow from the inlet plenum. Piping, heat exchangers, and outlet nozzles of the inoperative loops are subjected to a thermal cycle. Cold sodium mixes with outlet sodium. Reduction of normal sodium flow through the reactor causes increased cladding temperatures and core damage if the protective systems do not function.	Simultaneous failure of one pump and check valve operation must occur to achieve reverse flow. In addition, to achieve gross core damage the pump rpm vs. demand protective channel must fail as well as the sodium outlet temperature protective channel.
Automatic Control Failure (Figure 2)			Automatic control failure as a single event is not a sufficient condition for core damage. Not only must the control system fail to maintain temperatures within the control band, but one or more temperature protective channels must fail in addition to an independent fault that leads to inadequate cooling.
Manual Control Failure (Figure 2)			Manual control failure as a single event is not a sufficient condition for core damage. Not only must maloperation allow temperature to exceed limits, but temperature protective channels also must fail.

MALFUNCTION

RELATED MALFUNCTION

INITIATING CONDITION
FOR REACTOR ACCIDENT

SAFEGUARDS

Rod Drop-Cutback Failure
(Figure 2)

Failure of all cruciforms to drop is hypothetical. Physical separation and fail safe redundancy of control ensures activation. Failure of one cruciform to drop due to mechanical hang up and/or failure of one set to drop due to control abnormality still allows adequate shut down ($-1\% \delta k/k$) with the remaining cruciforms. Cutback activation is backed up by reactor trip. As a single event, rod drop or cutback failure is not a sufficient condition for core damage. Overtemperature protective channels must fail in addition to other independent faults to achieve core damage by inadequate cooling.

Over Temperature Message Failure
(Figure 2)

Regional core channel outlet temperatures will be displayed and will alarm at preset values well within the operation limit. Other temperature protective channels will function if one fails.

Loss of Feedwater Steam
System Rupture
(Figure 3)

Feedwater Underpressure Message
Failure
Turbine Trip Message Failure

Heat sink failure due to inadequate feedwater supply or rupture of the steam generator allows the intermediate sodium return leg and primary sodium return temperature to increase. An increase of core inlet temperature allows an increase of fuel cladding temperature and core damage.

Reactor trips actuate prior to increase of the core inlet sodium temperature. As a back-up safety feature the core outlet temperature protective trips actuate. The negative overall core temperature coefficient limits reactivity increase.

Carbon Input Primary
System
Oxide Input Primary
System
(Figure 4)

Primary Sodium Purification
System Failure

Flow blockage of the core or heat exchanger could occur due to gradual buildup of dissolved and particulate impurities. Dissolved impurities tend to precipitate where subjected to a cooling temperature gradient as within the sodium heat exchanger. Oxide is introduced by film deposits during element transfer. Lubricants can introduce carbon during element transfer. Flow blockage will cause cladding temperature increase and core damage.

Cold trapping removes oxygen during start-up and operation. Carbon and oxygen are removed by hot trap during reactor operation. Plugging temperatures are obtained daily to ascertain oxygen level, and sodium sample analyses are made on schedule to ascertain carbon content. There are procedural requirements for specific low oxygen control at phases of startup and operation. High temperature protective channels alarm and provide adequate warning prior to any core damage.

Foreign Object in Primary
System
(Figure 4)

An error of design, fabrication, inspection, or operation introduces an object that blocks flow in some part of the primary system. A foreign object can cause cladding temperature increase and core damage.

Detail design and review of the design minimizes probability of releasing or shifting of an object into the sodium flow path. Quality control during all phases of construction and rigorous operation-maintenance procedure prevent the presence of any foreign object in the primary system. Fuel subassembly inlets have an anti-plugging feature. High temperature and temperature change rate protective channels prevent core damage.

Loss of Primary Sodium
Coolant
(Figure 4)

Outer Vessel Leak and Failure
of Low Sodium Level Trip

(See first three items listed under
Figure 2)

(See first three items listed under
Figure 2)

(Figure 4)
Operation Error is not unique but can initiate independent faults shown elsewhere, e.g., inadvertent system drain, manual control failure, foreign object in primary system, etc.

Loss of coolant, control failure, or foreign object can cause cladding temperature increase and core blockage. Attenuation of primary sodium flow can lead to increased cladding temperature and core damage.

No single maloperation causes unprotected flow loss sufficient for gross core damage. Temperature protective channels, pump rpm monitors, sodium level monitors, and procedure are in effect during power operation.

Primary Pump Gas-Bound
(Figure 4)

Outlet Temperature or Pump RPM
Protective Failure

Accumulated pockets of gas move from one part of the system to the pump impeller and reduce pump effectiveness. The loss of flow can cause an increase of cladding temperature and core damage.

There is not sufficient free surface space within the primary system to accumulate a sizable gas inventory (other than above the gas flow velocity pool surfaces). Gas service systems and other service systems are designed to prevent the introduction of gas into the primary coolant.

Primary Pump Cavitation
(Figure 4)

Outlet Temperature or Pump RPM
Protective Failure

Loss of reactor cover gas pressure reduces head at pump inlet sufficiently for cavitation with effective sodium flow attenuation. Loss of flow can cause an increase of cladding temperature and core damage.

The reactor trips if cover gas pressure is reduced and sodium outlet temperature protective channels limit core damage as a backup.

MALFUNCTION	RELATED MALFUNCTION	INITIATING CONDITION FOR REACTOR ACCIDENT	SAFEGUARDS
Primary Pump Motor Failure (Figure 4)	Temperature-Pump RPM Protective Failure	Loss of pump motor power or pump motor failure causes primary system flow loss with an increase of cladding temperature and core damage.	De-energizing the pump motor actuates a delayed reactor trip, an rpm deviation trip and a core outlet temperature trip. After momentum "coastdown" of sodium flow, the check valves of the de-energized loop close to maintain core heat removal and prevent core flow bypass.
Primary Pump Seizure (Figure 4)	Outlet Temperature or Pump RPM Protective Failure	Seizure of the primary pump shaft or impeller causes primary system flow loss with an increase of cladding temperature and core damage.	Pump rpm deviation or core outlet temperature increase trips the reactor; check valves of the de-energized loop close to maintain core heat removal and prevent core flow bypass.
Carbon Input Intermediate System (Figure 5)		Oil films, grease, and other residue from construction, or lubricants introduced during maintenance contaminate the intermediate sodium. Redistribution of a large input of carbonaceous material to the sodium heat exchanger or steam generator can produce flow blockage.	Quality control and maintenance procedure minimize contaminants. The terminal concentration is too low for sensible physical interference with sodium flow or heat exchange. Heat balance, temperature indication, flow indication, and pressure indication make long-term component damage improbable.
Oxide Input Intermediate System (Figure 5)	Intermediate Sodium Purification System Failure	Introduction of oxide to the intermediate sodium system from: 1) construction residue, 2) maintenance operations, 3) diffusion from surfaces, and 4) redistribution within the system causes sodium oxide precipitation and flow blockage in the sodium heat exchanger or steam generator. Attenuation of intermediate sodium flow will cause the primary return flow to the reactor to increase in temperature.	Opportunities for oxide introduction to the intermediate sodium system are not great. Almost continuous operation of the purification system and measurement of the oxide content are a requirement. Heat balance, temperature indication, flow indication, and pressure indication increase operation awareness of long-term plugging accumulations. Cold trap operation will maintain a low oxygen equilibrium.
Foreign Object in Intermediate System (Figure 5)		A foreign object introduced to the intermediate coolant system during construction, maintenance, or a faulty design that enables the release of some component or part. Attenuated intermediate flow will cause the primary return sodium to increase in temperature, and cladding damage is possible.	Quality control during construction and procedure control during maintenance operations prohibit the unaccountable introduction of a foreign object. Design review and identification with historical cases decreases the likelihood of a design error. Hydraulic tests and other startup and/or periodic testing will produce awareness of a flow abnormality. Temperature protective channels will give warning and/or trip the reactor.
(Figure 5) Operation error is not unique but can initiate independent faults as shown elsewhere, e.g., Foreign Object, Loss of Intermediate Sodium Coolant Intermediate Pump Gas Bound, Intermediate Pump Motor Failure, etc.		Attenuation or loss of intermediate sodium flow causes a temperature increase of core inlet sodium through the heat exchanger to the reactor and possible cladding damage.	Design and procedure will be reviewed to define and minimize the potential for malfunction. Alarm and trip actuation on sodium level and core outlet temperature minimize cladding temperature excesses. The negative temperature coefficient limits reactivity increase.
Intermediate System Drain or Rupture (Figure 5)		Inadvertent drain of the intermediate sodium system, leakage, or gross rupture would (with various orders of time) result in partial or complete loss of sodium flow. Temperature gradient in the sodium heat exchanger collapses to higher temperatures and increases the temperature of sodium returning to the reactor. Cladding damage could occur.	Sodium service draining of the intermediate system requires activation of a mechanical valve lock to make it a unique operation. Prior to pump cavitation, sodium level loss will activate alarm and/or reactor trip.
Intermediate Pump Gas Bound (Figure 5)	Outlet Temperature or Pump RPM Protective Failure	Accumulated pockets of gas are swept from one part of the system to the pump impeller and reduce pump effectiveness. The loss of flow causes a temperature increase of core inlet sodium via the heat exchanger with possible cladding and core damage.	There is not sufficient free surface space within the intermediate system to accumulate a sizable gas inventory (other than low velocity pool surface). Gas service systems and other service systems will be designed against the introduction of gas.
Intermediate Pump Cavitation (Figure 5)	Sodium Level or Pump RPM or Outlet Temperature Protection Failure	Loss of system cover gas pressure reduces head at the pump inlet sufficiently for pump cavitation and sodium flow attenuation. Loss of flow causes an increase of cladding temperature and core damage.	The reactor trips if intermediate system cover gas pressure is reduced. Sodium outlet temperature protective channels limit core damage.

MALFUNCTION	RELATED MALFUNCTION	INITIATING CONDITION FOR REACTOR ACCIDENT	SAFEGUARDS
Intermediate Pump Motor Failure (Figure 5)	Pump RPM or Outlet Temperature Protective Failure	Loss of pump motor power or pump motor failure causes sodium flow loss and an increase of core inlet sodium temperature via the sodium heat exchanger.	De-energizing the pump motor actuates a delayed reactor trip or an rpm deviation trip. Inlet temperature deviation at a preset limit trip the reactor and limit core damage.
Intermediate Pump Seizure (Figure 5)	Pump RPM or Outlet Temperature Protective Channels	Seizure of the intermediate pump shaft or impeller causes flow loss with an increase of sodium temperature at the core inlet. Cladding temperature increase and core damage can occur.	Pump rpm deviation, sodium core inlet temperature deviation, and core outlet temperature protective channels trip the reactor and limit core damage.
Set Point Error (Figure 6)	Protective System Failure	The set points for trip actuation are set too high or change in one or more nuclear protective channels. With poor coupling a high set point allows power excess in one quadrant. Similar set point errors in two or three nuclear protective channels allows core power excess. Cladding temperature limits would be exceeded with resultant core damage.	Nuclear coupling between quadrants is high, therefore, set point error in at least two protective channels is required before power limits are exceeded. In addition to power protective channels there are outlet temperature protective channels as well as control instrumentation that limit temperature excesses.
Power Control Failure (Figure 6)	Protective System Failure	A malfunction of the load-following controllers or subassembly demands power increase or flow reduction with attendant core temperature increase. Cladding temperature would exceed limits with core damage.	Automatic controller change rate limits and control range feedback limits return the reactor to manual control prior to temperature excesses. All the temperature and power protective channels as well as control instrumentation limit temperature excesses.
Carbon Input Primary System or Oxide Input Primary System (Figure 7)	Primary Sodium Purification System Not Operating or Primary Sodium Purification System Not Adequate	Oil films remaining from construction or lubricants introduced during element transfer operations introduce carbon to the primary sodium. Oxides are introduced by: 1) element transfer operations, 2) sodium transfers to-and-from service systems, and 3) long-term diffusion from system surfaces. Failure of the hot traps or cold traps allow carbonaceous or oxide deposits to form on the cladding or in the core channels. The increase of local heat transfer impedance or channel blockage causes excessive cladding temperatures and possible core damages.	Cold trapping removes oxygen during start-up and operation. Carbon and oxygen are removed by hot trap during reactor operation. Plugging temperatures are obtained daily to ascertain oxygen level, and sodium analyses are made on schedule to ascertain carbon content. There are procedural requirements for specific low oxygen content at phases of startup and operation. High temperature protective channels will alarm and provide adequate warning prior to core damage.
Foreign Object (Figure 7)		A foreign object is introduced to the primary coolant system during construction, maintenance, or by faulty design. Attenuation of flow in one or more core channels or flow blockage in one of the main heat exchange systems causes increase of the cladding temperature and possible core damage.	Design review minimizes opportunity for the release of internal components into the flow path. Quality control and discipline during fabrication, construction, and maintenance prohibit any residue or foreign objects within the finished complex. The lower end of the fuel subassembly extends into the core grid plate and communicates into the core sodium inlet supply plenum. This extension functions as a cage to prevent flow blockage by loose objects. Temperature abnormality produces awareness of channel blockage. Gross blockage will actuate temperature protective trips.
Fuel Element Misalignment in Channel (Figure 7)		The fuel pin within a fuel subassembly bows toward other neighbor pins and chokes cool- and flow between pins. A hot spot develops that exceeds the cladding temperature limits.	Review of the fuel subassembly design and testing of prototype elements for support grid spacing optimizes overall function and minimizes any opportunity for bowing or regional cooling loss.
Excess Fuel Swelling (Figure 7)		If the swelling rate of the pellets is greater than the empirically confirmed prediction, the bond gap between cladding and pellet can hold fission gas. Cracking of pellets or radial displacement of pellets also can act to retain fission gas in the bond annulus. Sizable voiding of sodium bond reduces heat transfer to coolant and produce further bond voiding and possible cladding failure.	The swelling rate will be confirmed by in-pile tests. Compatibility of pellets to bond and cladding will be verified by in-pile testing of prototypes.

MALFUNCTION

RELATED MALFUNCTION

INITIATING CONDITION
FOR REACTOR ACCIDENT

SAFEGUARDS

Plugged Fuel Element Vent
(Figure 7)

The fuel pin vent tube extension that communicates and "breathes" to the core cover gas region can possibly plug with sodium oxide or extraneous material introduced during fabrication or installation. During irradiation, fission gas pressure can rupture the cladding.

Quality control and procedure control minimizes any opportunity for the introduction of oxide or foreign substance within the vent tube or fuel pin. Subassemblies are examined on-site for damage as they enter the loading cycle.

Cladding Crud
(Figure 7)

Surface accumulation of sodium oxide, or carbon compounds reduces heat transfer and cause a hot spot. The overtemperature condition leads to cladding failure and core damage.

Oxygen and carbon purification systems operate to maintain acceptable impurity concentrations. Subassembly inspection enables evaluation of the outer heat transfer surface of the cladding.

Gas Bubbles Outside
Cladding
(Figure 7)

Cover gas or other gas entrained or dissolved in the sodium coolant enters the core lattice as bubbles that temporarily mask the outer cladding surface and impedes heat transfer. If bubble residence time in one locale is long enough, or if there is a gas streaming condition, the cladding temperature limit will be exceeded, with core damage possible.

The primary heat transfer system is designed without gas accumulation pockets. Entrained gas in the coolant will be of minor size, and core coolant velocity does not allow local gas accumulation in the core.

Gas Bubbles in Sodium
Bond
(Figure 7)

Fission gas that normally diffuses from the fuel pellet surface rises through the sodium bond annulus to vent relief. However, if the space is restricted, the bubble may not rise but remain to coalesce with other bubbles to form a thermal impedance hot spot. The cladding temperature limit will be exceeded, with possible core damage.

The critical size for bubble mobility will be empirically verified. The required clearance for the sodium bond at the end of life is a criteria to be optimized with the predicted fuel swelling.

Loss of Sodium Bond
(Figure 7)

Plugging of the fuel pin vent is a mechanism for loss of bond. If a cladding leak or minor cladding failure also occurs, the bond sodium can be displaced by stored fission gas. Temperature increase of the isolated fuel pellets can be a source of additional core damage.

Loss of bond is initiated by plugged fuel vent and safeguards of the plugged fuel vent case apply.

Fuel Charged to Wrong
Position
(Figure 8)

Loading of an over-enriched fuel subassembly increases k by more than the shutdown margin or reduces the shutdown margin. This combined with routine start-up safety rod withdrawal could lead to a power excursion with core damage.

Fuel production with accountability for fissile material reduces probability for greatly over-enriched material. No special fuel or experimental fuel with large fissile inventory is planned. Loading of the most enriched fuel subassembly into a sodium-filled channel is worth approximately +1.5%. During loading with all control rods in, the shutdown margin is greater than 4%. Normal startup procedure, and startup procedure with an unknown or changed core is rigorous with regard to initial count rate vs. count rate increase. The count rate at down time is a matter of record; any gross deviation of the subcritical count rate constitutes an abnormal condition that will be investigated. During startup, excessive flux rate change (period) always will trip the reactor.

Criticality Prediction Loading Procedure Error
Error
(Figure 8)

If a calculation error indicates that critical loading is much greater than actual, and also if in violation of procedure, the loading exceeds the approved intervals as determined by inverse flux plot, the reactor may exceed the critical condition as control rods are withdrawn. Core damage could result.

The prediction of criticality always is determined by more than one responsible person. With an unknown or changed core, the inverse count plot either confirms or refutes the prediction. Loading and rod withdrawal intervals are conservative such that the predictions are checked against the empirical with a safety margin on the measurement conditions. During startup, excessive flux rate change (period) always trips the reactor.

FHM Mechanical Failure
or
Early Release Procedure
Error
(Figure 8)

Damage to the fuel subassembly occurs by misalignment with the core lattice or by dropping of the subassembly into the core. Damage to the fuel pins or subassembly causes inadequate regional cooling at power. Core damage can result.

The reactor is subcritical with all control rods in during loading changes; uncontrolled insertion of a fuel subassembly does not cause a reactivity increase beyond the subcritical condition. The gripper fingers of the element grapple are positive actuating with cam rod motion. Cam rod position is indicated. Gripper finger tips are self-securing with load. Weight indication is a required procedure check condition.

MALFUNCTION	RELATED MALFUNCTION	INITIATING CONDITION FOR REACTOR ACCIDENT	SAFEGUARDS
Primary Pump Energize Error (Figure 8)	Drive Latch Failure or Extension Rod Failure	The tantalum control rod poison sections are pushed up by the pressure of core inlet sodium if a sodium pump is fully energized. The control rod rests in the core by gravity when the holddown rods are removed for element transfer operations. Also if the drive latch mechanism breaks, the 1) control rod, 2) extension rod, and 3) ratchet bar could be forced up against gravity by the core pressure gradient. In the first case, the reactivity increase with ejection of numerous control rods will result in core damage.	Sodium pumps are interlocked against energizing by more than minimum circulation rate at shutdown. Prior to removal of the shield plug and extension rods, the main pump motor power supply is removed from service. At times other than element transfer the control rod and extension rod assembly is held in place by the magnetic jack mechanism and weight of the combined assembly. Failure of one or more at shutdown and ejection of one rod does not exceed the subcritical condition.
Inadvertent Startup of Stand-by Sodium Loop (Figure 10)		An inactive primary loop (a main loop or auxiliary core cooling loop) is accidentally activated and the cold coolant in the loop is pumped into the reactor inlet plenum. The core inlet temperature drops and the core power increases due to negative temperature coefficients.	The auxiliary core cooling loop is maintained isothermal at core inlet temperature by designed reverse flow (slight core bypass) through a check valve. Inadvertent energization of the auxiliary primary pump initially returns sodium at inlet temperature to the core inlet plenum so there will be no void effect. If auxiliary flow is unchecked, hot outlet sodium is introduced to the core inlet plenum but the overall negative temperature coefficient will actually decrease power. Startup of an inactive heat transfer system with a full temperature gradient across the core is procedurally prohibited.
Feedwater Heater Loss (Figure 10)	Protective System Failure	a) A sudden decrease in feedwater temperature is produced by a failure of the feedwater heater. This temperature change causes a transient overcooling of the steam generator. A temperature transient is produced in the primary and secondary coolant loops. b) A similar situation is produced by a sudden increase in feedwater flow from a part flow to a maximum flow condition.	With the reactor protection system operating, the reactor plant is able to accommodate this transient without damage. The sodium inlet temperature protective instrumentation trips the reactor.
Fuel Element Malfunction (Figure 10)	Poor Fuel Workmanship and Limited Fuel Inspection or Fuel Design Error or Long Term Irradiation Damage	Fuel element instability leads to the phenomena of divergent oscillation and extensive core damage.	Design scrutiny, analysis, and design review ensures a stable design commensurate with the state-of-the-art. Hydraulic testing of prototype fuel pins, pre-neutron and partial power testing (transfer function) confirms the design. Protective systems check damage.
Core Structure Malfunction (Figure 10)	Core Component Poor Workmanship and Limited Core Component Inspection or Core Component Design Error or Long Term Irradiation Damage	Core component instability leads to the phenomena of divergent oscillation and extensive core damage.	Design scrutiny, analysis, and design review ensure a stable design. Pre-neutron testing, hydraulic testing, plus low power flow, pressure and temperature test (transfer function) confirm the design.
Spectral Shift (Figure 10)	Moderator Material Input and Primary Sodium Purification System Failure or Partial Core Sodium Loss	Partial core voiding leads to a positive reactivity insertion since the voiding coefficient of reactivity is positive in the central region of the core. Addition of moderator material such as carbon or hydrogen from an unknown source softens the spectrum causing a negative reactivity effect.	The primary system is designed to prevent loss of primary sodium by draining. Both reactor inlet and outlet nozzles are above the core and a safety vessel is located around reactor vessel to prevent draining in the event of a vessel rupture. Low sodium level and temperature protective channels limit core damage. Addition of moderator material is a conservative change in respect to neutron spectrum. Bubble formation and transport is limited by design.
Gas Entrainment (Figure 11)	Reactor Sodium Surface Vortex or Pump Vortex or Equilibrium Gas Pocket Accumulation	A vortex forms at the sodium cover gas interface in the reactor vessel or in the pump. A gas bubble is introduced into the coolant stream and it is carried around the loop and introduced into the core. A large gas bubble is accumulated in some part of the primary loop due to dis-entrainment of small bubbles or changes in gas solubility. At some instant the entire bubble is released and transported through the core. Due to the positive partial voiding coefficient of reactivity, reactivity insertion may be produced and a power excursion may result.	A flow baffle in the outlet plenum of the reactor vessel is designed to prevent entrainment of cover gas. No vortexing is expected in the pump. The primary loop piping and components are designed to prevent accumulation of sizable gas bubbles.

MALFUNCTION	RELATED MALFUNCTION	INITIATING CONDITION FOR REACTOR ACCIDENT	SAFEGUARDS
Hydraulic Ejection (Control Rod) (Figure 11)	Full Sodium Pump Head and Rod Drive Holding Latch Failure or Extension Rod Failure	The highest worth control rod, which is fully inserted into the core, is suddenly ejected from the core causing the reactor to experience a power transient.	The maximum control rod worth is limited such that prompt criticality is prevented. The rod drive mechanisms are designed to minimize the possibility of this incident. Period and power level scram would stop the transient before reactor damage is produced.
Sodium Boiling in Core (Figure 11)	Boiling in Bond or Boiling in Coolant	Boiling in the core introduces a positive reactivity effect due to the local positive sodium voiding coefficient. Boiling in the bond can be expected to occur first and assist cladding failure along with a positive sodium voiding coefficient.	The reference plant is designed on the assumption that the reactor will be scrammed before the boiling has propagated to the extent that a damaging reactivity insertion is created.
Startup Error (Figure 11)	Incorrect Procedure and Operation Error	During startup, reactivity is inserted at a faster than normal rate and a reactor power excursion is produced.	Period and power level scrams effectively stop the transient before reactor damage is produced. Rod withdrawal is limited by design and procedure.
Control Rod Rapid Withdrawal (Figure 11)	Operation Error and Interlock Failure Spurious Energization	The highest-worth group of control rods is withdrawn at the maximum rate. The incident may begin at any reactor power level or at any subcritical configuration.	Control rod worths, withdrawal rates and grouping schemes are such that the maximum reactivity insertion rate is limited to a safe value. Rod controllers are programmed to actuate one rod at a time; power supply capacity is adequate only to energize one rod mechanism at a time. Period and power level trips stop the transient before damage occurs.