CONF-790816--60

SAFETY APPROACH TO THE SELECTION OF DESIGN CRITERIA FOR THE CRBRP REACTOR REFUELING SYSTEM

C. J. Meisl, G. E. Berg, and N. F. Sharkey

Atomics International Division
Energy Systems Group
Rockwell International
8900 De Soto Avenue
Canoga Park, California 91304

ABSTRACT

The selection of safety design criteria for Liquid Metal Fast Breeder Reactor (LMFBR) refueling systems required the extrapolation of regulations and guidelines intended for Light Water Reactor refueling systems and was encumbered by the lack of benefit from a commercially licensed predecessor other than Fermi. This paper describes the overall approach and underlying logic that were used while developing safety design criteria for the reactor refueling system (RRS) of the Clinch River Breeder Reactor Plant (CRBRP). The complete selection process used to establish the criteria is presented, from the definition of safety functions to the finalization of safety design criteria in the appropriate documents. The process steps are illustrated by examples.

INTRODUCTION

The selection of safety design criteria for the Clinch River Breeder Reactor Plant (CRBRP) Reactor Refueling System (RRS) is different from that of the Light Water Reactors (LWR) due to the CRBRP RRS configuration.

The basic features of the RRS configuration are: through the head, under the shield, in-reactor vessel handling; movable fuel transfer machine to transfer fuel in an inert atmosphere between reactor and ex-vessel storage; ex-vessel spent fuel storage under sodium; and spent fuel shipping cask loading in an inerted hot cell. The RRS is described in more detail in [1] and [2].

The selection of safety design criteria requires an extension of government regulations and industry standards applicable to LWR. Because the CRBRP will be the first fully licensed LMFBR in the U.S. since the Fermi Power Plant, no recent precedence exists with regard to the acceptability of RRS Safety design criteria to the licensing authority.

"Safety design criteria" in the context of this paper are those criteria for the construction, operation, and maintenance of RRS equipment and facilities which consider radiological protection for the public and for the plant operators.

SAFETY DESIGN CRITERIA SELECTION PROCESS

The philosophy and logic used to select safety design criteria can best be portrayed by the flow diagram shown in Figure 1. The major steps in

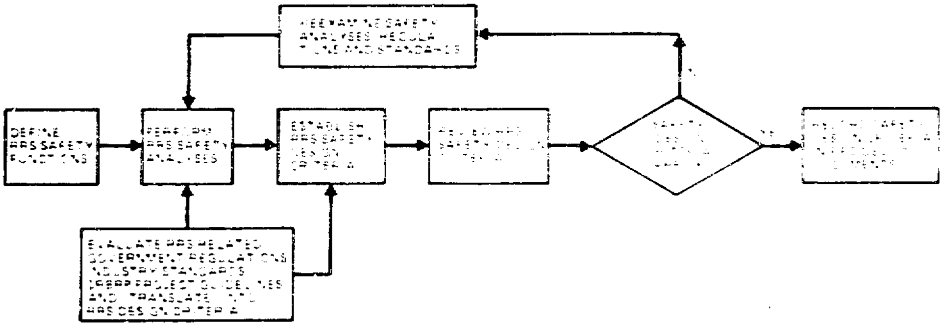

Figure 1. Safety Design Criteria Selection Process

the criteria selection process are as follows, listed in approximate chronological order:

1) Define RRS safety functions, i.e., those functions important for the radiological protection of the public and of the plant operators.
2) Perform RRS safety analyses covering normal operations and unusual events.
3) Evaluate government, industry, and project regulations and guidelines. Interpret these and translate them into specific safety design criteria.
4) Establish and review safety design criteria. Reexamine the results of the safety analyses and reassess regulations and guidelines in response to comments from project participants and to Nuclear Regulatory Commission (NRC) inquiries.
5) Finalize and baseline the safety design criteria in RRS design documents.

An iterative process was used until a final consistent set of design criteria evolved. Each of the listed steps is discussed as follows.

DEFINITION OF RRS SAFETY FUNCTIONS

Safety functions of RRS equipment and facilities are defined here as those which, if not provided, could lead directly or indirectly to excessive radiological exposure of the public or of the plant operators. They are based mainly on the General Design Criteria 61, 62, and 63 of 10 CFR 50, Appendix A. The following five top-level safety functions were established for RRS equipment and facilities:

1) <u>Provide Containment of Radioactive Materials</u> (Criteria 61, 63) — This function is specifically directed to containing radioactive gases and sodium, and to controlling the spread of radioactive contamination.
2) <u>Provide Biological Shielding</u> (Criterion 61) — The radiation shielding function is required for operator protection mainly. This function provides the basis for ALARA considerations.

3) Maintain Subcriticality (Criterion 62) — Subcriticality considerations are important for on-site storage of new and spent fuel.
4) Remove Residual Heat from Spent Fuel (Criteria 61, 63) — This function expresses the necessity for adequate decay heat removal to protect the integrity of the containment structures, and to maintain the structural integrity of spent fuel cladding.
5) Prevent Loss-of-Safety Function of Other Components (Criterion 61) — This function is important for the definition of design criteria of equipment interfacing with, or adjacent to the RRS. It is the basis for criteria such as prevention of moving equipment collision, crane hoisting and rigging requirements, seismic and impact loads, safety interlocks, and provision for emergency electrical power.

SAFETY ANALYSES FOR RRS

The next step in the safety design criteria selection process is to perform safety analyses for all RRS components with potential for loss of safety function. Figure 2 presents an activity flow chart delineating major activity sequences that are discussed below.

At first, a list of postulated "top-level undesired events" is prepared. The sources of this list include the results of previous RRS safety studies, accidents listed in Chapter 15 of U.S. NRC Regulatory Guide 1.70 (see Table I), reviews of applicable LWR and LMFBR historical experiences (e.g., as reported in [3]), results of LMFBR component development tests, and evaluations by design and safety experts. The list includes the following postulated events:

1) Loss or degradation of spent fuel cooling capability
2) Release of radioactive inert cover gas
3) Dropping of a fuel assembly
4) Spill or leakage of radioactive sodium
5) Immobilization of a spent fuel assembly during transfer operations
6) Collision between, or drop of heavy equipment involving spent fuel transfer machines, spent fuel shipping cask, or spent fuel storage facilities
7) Accidental criticality of new or spent fuel.

Separate analyses were conducted for each RRS component to evaluate its response to individual events. The resulting list of undesired events associated with specific RRS components was checked for completeness, and was searched for those events which could produce potentially large consequences or which had an element of commonality for many RRS items.

Using semi-quantitative or scoping analyses, the event consequences were categorized as insignificant or potentially significant. For example, the safety consequences of dropping a new fuel assembly are considered insignificant. This early screening procedure substantially reduced the amount of analysis to be undertaken and freed efforts for safety analyses with potentially significant or unknown consequences.

The bulk of effort with regard to RRS safety analyses consisted of constructing fault trees and safety assurance diagrams, and of conducting

TABLE I

Key Regulations and Standards Considered in Developing RRS Safety Design Criteria

Federal Regulations	
10 CFR 20	Standards for Protection Against Radiation
10 CFR 50	Licensing of Production and Utilization Facilities
10 CFR 70	Special Nuclear Material
10 CFR 71	Packaging of Radioactive Material for Transport
10 CFR 73	Physical Protection of Special Nuclear Material
10 CFR 100	Reactor Site Criteria
NRC Regulatory Guides	
1.13	Spent Fuel Storage Facility Design Basis
1.25	Assumptions Used for Evaluating the Potential Radiological Consequences of a Fuel Handling Accident in the Fuel Handling and Storage Facility for BWR's and PWR's
1.26	Quality Group Classification and Standards for Water, Steam, and Radioactive-Waste-Containing Components of Nuclear Power Plants
1.29	Seismic Design Classification
1.70	Standard Format and Content of SAR's for Nuclear Power Plants (LMFBR Edition)
1.104	Overhead Crane Handling Systems for Nuclear Power Plants
NRC Standard Review Plans	
RDT Standards	
F1-2T	Preparation of System Design Descriptions
F8-6T	Hoisting and Rigging of Critical Components and Related Equipment
F9-2T	Seismic Requirements for Design of Nuclear Power Plants and Nuclear Test Facilities
C16-1T	Supplementary Criteria and Requirements for RDT Reactor Plant Protection Systems
Industry Standards	
ASME	Boiler and Pressure Vessel Code: Section III, Divisions 1 and 2 Section VIII, Divisions 1 and 2
ANSI B31.1	Power Piping
ANSI N15.8	Guide to Practice Nuclear Material Control System for Nuclear Power Reactors
ANSI N16.5	Guide for Nuclear Criticality Safety in the Storage of Fissile Materials
ANSI N18.2	Nuclear Safety Criteria for the Design of Stationary PWR's
ANSI N18.8	Design Basis Criteria for Safety Systems in Nuclear Power Generating Stations
ANS 54.1	General Safety Design Criteria for an LMFBR Nuclear Power Plant
IEEE 279	Criteria for Protection Systems for Nuclear Power Generating Stations
IEEE 323	General Guide for Qualifying Class I Electric Equipment for Nuclear Power Generating Stations

failure mode and effects analyses, common cause failure analyses, and in-depth quantitative consequence computations. The analyses considered the detailed chronological sequences of events initiated by faults, malfunctions, component failures, and human errors leading to potentially significant consequences. Most analyses were inter-disciplinary, covering the fields of applied mechanics (mainly stress and deformation analyses), heat transfer and thermodynamics, nuclear physics, and radiological release analysis.

The use of safety assurance diagrams, see Figure 3 for an example, proved to be a particularly valuable tool in accident progression analyses. These diagrams not only illustrate malfunctions and accident sequences, they also delineate clearly and specifically the lines of defense which inhibit or stop accident progression (indicated by slashes).

An example for an in-depth quantitative consequence analyses is shown in Section 15.7.3.1 of [2]. The analysis concerns the postulated, extremely unlikely event of a Core Component Pot (CCP) sodium leak while the CCP resides in the Ex-vessel Transfer Machine (EVTM), and while it contains a high-decay heat spent fuel assembly. The postulated event was found to result in potential off-site doses which are within the limits of the "enveloping" RRS event. The "enveloping" RRS event is a postulated mechanistic event producing the highest off-site doses. It was determined to be an event in which all fission gases from one spent fuel assembly with the shortest decay time are released into the EVTM containment and are subsequently allowed to diffuse through the EVTM elastomer seals into the reactor containment building while it is in the refueling configuration. The maximum site boundary dose from this event is a thyroid dose in the amount of ~1% of the plant guideline exposure during construction-permit review.

In addition to the consequences, expected frequencies of occurrence were estimated for each event for which a quantitative analysis was performed. The frequency of occurrence considered the combined effects of fuel handling equipment use time, component failure probabilities, operator error probabilities, and off-normal plant condition probabilities.

Operation of RRS equipment and facilities is limited to their relatively short use time during reactor refueling, spent fuel shipping, and new fuel receiving; therefore, use time is important when estimating expected event frequencies.

Probability data for failures of components which are specifically a part of an LMFBR refueling system are rare since limited operating experience exists with this kind of reactor system. However, many of the components which make up the RRS are not operating in a liquid sodium environment, but rather in argon or air, and are of more or less conventional commercial design. A list of failure probabilities for these components and references of their data origin is contained in [4].

Due to the sparsity of operational data for LMFBR-type refueling equipment, general error rate estimates from LWR's were used, including those presented in [5].

Off-normal plant conditions affecting the RRS are mostly seismic and loss-of-power events. The frequency of occurrence for these events used in the RRS safety analyses was based on data given in [5] and [6].

The results of the safety analyses, consisting of consequences and expected frequency of occurrence of postulated events, were compared to the damage severity limits at a given frequency class, shown in Table II. (The basis for this table is discussed under the next heading.) If the calculated consequences of an event were found to exceed the damage severity limit at the estimated frequency of event occurrence, design changes or

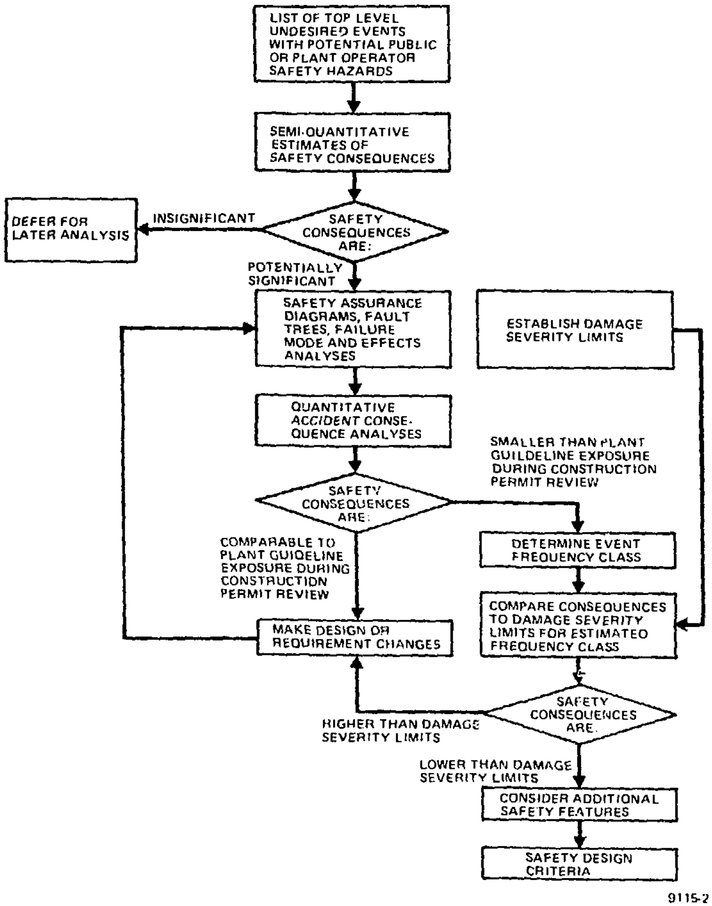

Figure 2. Safety Analysis Flow Chart

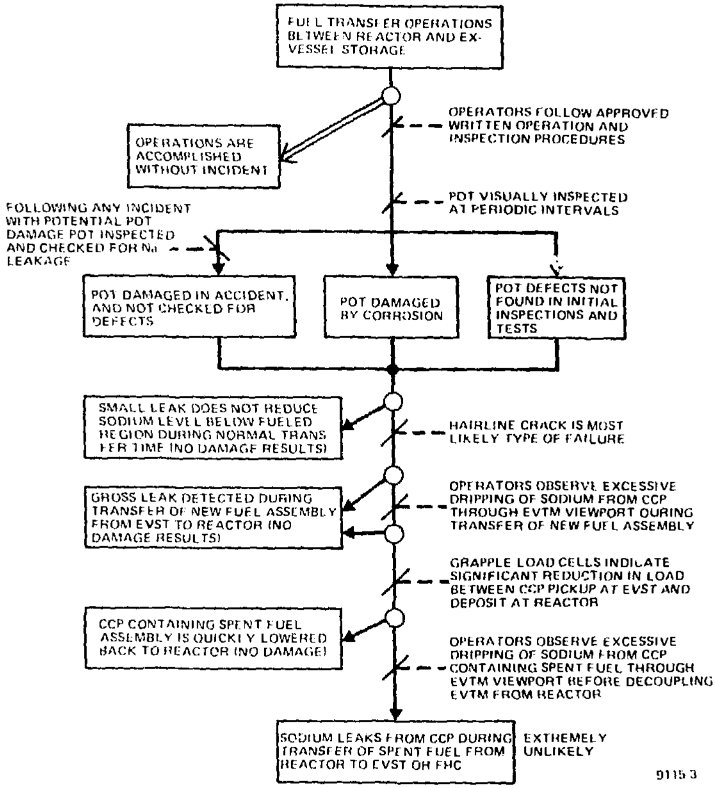

Figure 3. Protection Against Leak in Core Component Pot

TABLE II

Definition of Expected Frequencies and Damage Severity Limits of Events for Reactor Refueling System

Postulated Plant Condition (Similar ASME "Operating Conditions" in parentheses)	Expected Frequency of Event Occurrence		Damage Severity Limit of Events				Level of Design Protection or Plant Against the Postulated Plant Condition
	Qualitative (Frequency Class)	Quantitative (Probability of Occurrence per Reactor Year)	Event Category	Fuel Damage	Plant Equipment Damage	Radioactivity Release Limits for Restricted and Unrestricted Areas[a]	
Normal Operation (Normal)	Normal	1.0 (Includes normal transients)	No Damage	1) No reduction in new fuel lifetime 2) No reduction in new fuel power capability 3) No additional cladding strain in spent fuel	1) No equipment damage or operational impairment 2) No automatic or manual protective action required	Restricted area: As low as reasonably achievable (ALARA) Airborne radioactivity in Zone I <0.02 mrem/hr Total RRS operator exposure <125 mrem/quarter Unrestricted area: ALARA (10 CFR 50 App. I)	1 (Intrinsic features of design)
Off-Normal Condition Anticipated Fault (Upset) Example: OBE	Anticipated (One or more times during the life of the nuclear power unit)	3×10^{-2} to 1.0	Operational Incident	1) As above 2) As above 3) As above	1) As above 2) No loss of effective component lifetime	<10 CFR 20 for restricted and unrestricted areas	
Off-Normal Condition Unlikely Fault (Emergency)	Unlikely (Individually not expected in plant lifetime; integrated over all plant components may occur a number of times)	10^{-4} to 3×10^{-2}	Minor Incident	1) Reduction in new fuel life or power capability 2) Clad failures in almost all fuel rods of one spent fuel assembly, but insignificant fuel release	Plant or equipment damage leading to considerable plant down time, but no unrepairable or unreplaceable gross structural damage	Restricted area: <10 CFR 20 quarterly dose per incident Unrestricted area: <10 CFR 20 per incident	2 (Protective Systems)
Off-Normal Condition Extremely Unlikely Fault (Faulted) Example: SSE	Extremely Unlikely (Not expected to occur during plant lifetime)	10^{-7} to 10^{-4}	Major Incident	Substantial fuel clad failure with gross release of fuel for new or spent fuel assemblies	1) Plant or equipment damage that may preclude future plant operation 2) No loss of safety function	Restricted area: <10 CFR 20 annual dose per incident Unrestricted area: Less than Plant Guideline Exposures set for Construction Permit Review	3 (Protective Systems)

[a]Restricted Area: Reactor Containment Building, Reactor Service Building
Unrestricted Area: Site Boundary and beyond

operational changes were investigated to either eliminate the event or to limit its consequences. This process was iteratively repeated several times until the safety influencing design or operating conditions were judged to be covered satisfactorily by safety design criteria. In a number of cases where it has been possible to significantly reduce the consequences from an event, design changes were made even though the consequences did not approach the allowable limit.

Besides establishing actual safety design criteria, the results of the safety analyses were as follows:

1) Identification of postulated events with potentially large consequences for inclusion in the Preliminary Safety Analysis Report, [2].
2) Establishment of design basis accidents for equipment safety classification, identification of needs for safety interlocks, and for safety-related emergency power.
3) Definition of specific design features to decrease event consequences or event frequencies.

EVALUATION OF GOVERNMENT REGULATIONS AND INDUSTRY STANDARDS

The evaluation of applicable Federal, industry, and project regulations and guidelines yielded a set of design criteria which were independent of specific RRS safety analysis; for example, the requirement to provide two means of decay heat removal for spent fuel. It also resulted in criteria which expressed event damage severity limits as a function of frequency of event occurrences, against which the consequences and frequencies of the postulated RRS events, calculated in the safety analyses, could be measured.

The severity limits versus event frequencies specifically developed for RRS design are shown in Table II. The entries in Table II were determined partly from more general plant design groundrules, partly from ANS and industry publications. The probability ranges shown in Column 3, for example, were derived from several sources, including [6].

Difficulty was encountered in trying to apply Federal, industry, and project regulations and guidelines to the CRBRP RRS. The regulations and guidelines, although appropriate for light-water reactor RRS's or for LMFBR reactor design, were often not directly applicable for LMFBR fuel handling and storage facilities. Design criteria relating to spent fuel cooling, fuel storage criticality control, or radiation shielding were found to be well defined in the existing regulations and guidelines. However, criteria for selection of construction codes of equipment other than pressure vessels, for hoisting and rigging standards, for facility impact loads, for seals, etc, were found to be inadequately covered. In these cases, the intent was extracted from related regulations and guidelines, and logic diagrams were constructed to yield the required criteria.

The main sources considered for developing RRS safety design criteria were CRBRP project rules and the Federal and industry documents listed in Table I.

The selection of construction codes and standards, and of seismic categories for RRS equipment and facilities required a major effort. The approach followed was to establish a logical procedure which could be used to select existing codes, standards, and categories for all RRS equipment and facilities. Emphasis was placed in the selection of codes and standards currently in use, rather than development of specific construction and inspection rules for each RRS item by taking advantage of the extensive experience gained with their use. This generally provides more assurance of quality and completeness than do newly developed codes and standards.

The logic diagrams which graphically depict the method followed for the selection of construction codes and standards and of seismic categories for RRS components are shown in Figures 4 and 5, respectively. Basically, it is a graduated classification system which matches the construction code and the seismic category with the importance of the safety or economic function performed by each RRS component. The method expands the classification systems of NRC Regulatory Guides 1.26 and 1.29, and of RDT Standard F9-2T (see Table I), to include economic considerations. The threshold values for the economic criteria were obtained by consensus of Atomics International (AI) expert opinions. The classification method summarized in Figures 4 and 5 was successfully applied for all RRS equipment and facilities down to a key component level.

Similar methodologies were developed to determine hoisting and rigging design requirements for crane-handled RRS and maintenance loads, RRS facility impact load design requirements, and optimum number of electrical interlocks for protection of RRS equipment and facilities.

ESTABLISHMENT AND REVIEW OF SAFETY DESIGN CRITERIA

The steps described above led to a set of system-oriented safety design criteria which were available as a guide to the equipment and facility designers at an early stage of the design process. Table III summarizes some of the key RRS safety design criteria. The criteria have been reviewed by the CRBRP project participants through formal Design Reviews, and by NRC via the PSAR in which the RRS design criteria appear as Design Bases in Chapter 9.1, [2]. In developing the criteria, considerable iteration within the design team and with the NRC has been necessary to establish an agreed upon basis for the design.

SAFETY CRITERIA DOCUMENTATION AND IMPLEMENTATION

The final step in the described process consisted of documenting and baselining the RRS design criteria. The criteria were entered into two categories of documents: The RRS top-level requirement document, the System Design Description (SDD), contains design criteria in a general form to facilitate the dialogue with the customer and to be applicable to all RRS equipment designs. The next tier of documents (e.g., Equipment Specifications and Interface Documents) spell out detailed design criteria, specifically tailored to the needs of individual hardware design and to the explicit language required by designers.

Table IV presents some of the key safety features of RRS equipment and facilities as a direct consequence of safety design criteria. This list is not exhaustive; its intent is to show the traceability of design features to design criteria sources.

ACKNOWLEDGEMENT

This work was performed under Contract No. 54-7AO-192907 BP.

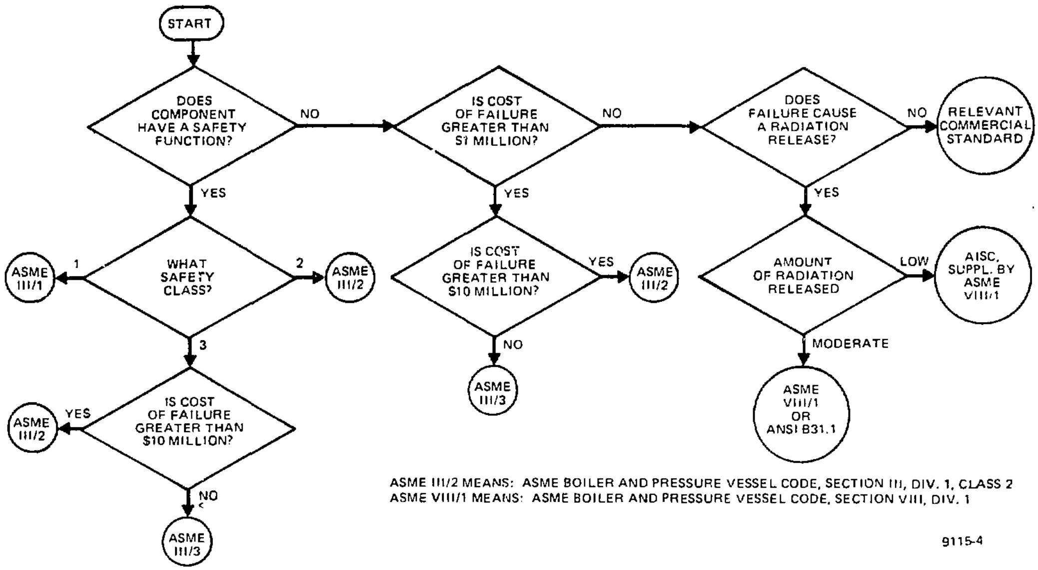

Figure 4. Construction Code and Standard Selection Process

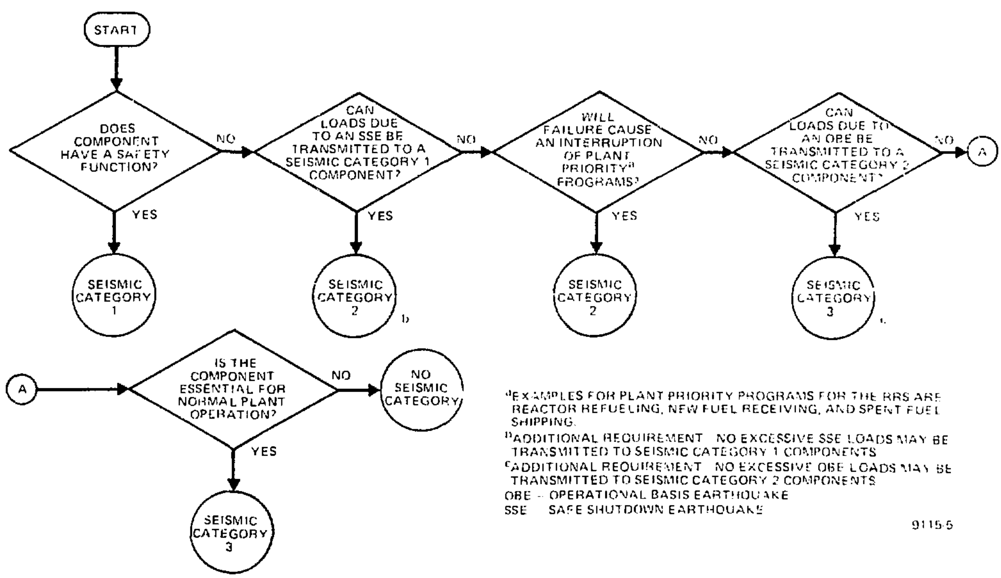

Figure 5. Seismic Category Selection Process

TABLE III

Reactor Refueling System Key Safety Design Criteria

1. Safety Functions
   - A. Provide containment of radioactive material
   - B. Provide biological shielding
   - C. Maintain subcriticality
   - D. Remove residual heat from spent fuel
   - E. Prevent loss-of-safety functions of other components
2. Correlation Between Event Frequency of Occurrence and Consequence Limits
3. Unusual Events to be Considered in Design of All RRS Equipment and Facilities
4. Prevention of Criticality
   - A. $K_{eff} < 0.95$, preferably by use of geometrically safe configuration
   - B. Meet requirements of 10 CFR 70
5. Shielding
   - A. Radiation zone criteria for facilities in accordance with plant criteria
   - B. Equipment not to exceed the lower of:

     125 mrem/quarter integrated dose or a maximum accessible surface dose rate of 200 mr/h
   - C. Streaming at penetrations up to three times that permitted at surface of bulk shielding; but general area dose rate increase at work location limited to 1.2 times the level without penetrations.
   - D. ALARA rules for radiation exposure minimization
6. Gas Sealing
   - A. If release would exceed 10 CFR 20 limits for restricted areas:
     - 1) Dynamic Seals — double and buffered, continuously monitored
     - 2) Static Seals — double, periodic leak check
   - B. If release would not exceed 10 CRF 20 limits for restricted areas:
     - 1) Dynamic or Static Seals — double: no routine leak check, but capability provided
7. Cooling of Spent Fuel
   - A. Two means of cooling
   - B. Guard Tanks

TABLE IV

RRS Safety Design Criteria and Safety Features

Criterion	Safety Feature
Prevent Loss of Cooling of Irradiated Core Assemblies	Cooling Loop Redundancy and Diversity
	Guard Tank for Sodium-Filled Fuel Storage Vessel
	Antisiphon Devices
Protect Fuel from Mechanical Damage	Fuel Storage Covered by Heavy Shields
	Redundancy and Failsafe Design of all Drives and Grapples
	Suitable Interlocks
	Single Failure Proof Design of Building Cranes and Hoisting and Rigging
	Travel and Lift Restraints for Crane, Gantry, and Trolley
Limit Off-Site Exposures	Closed and Sealed Fuel Storage and Fuel Handling Equipment
	Spent Fuel Stored Under Sodium (Limits Iodine Release)
	Storage Facilities Have Gas Clean-up Systems
	Double and Buffered, or Double Seals
	Steel Lining of Vaults and Cells
Inspection Capability	Periodic Inspection of all Moving Parts and Visual Inspection of the Exterior of Vessels Containing Sodium
Prevent Criticality in Fuel Storage	Geometrically Safe Spacing of Fuel Assemblies or Provision for Neutron Poison
	No Contact of Fuel with Moderating Fluids
Radioactivity Release Less Than Project Guidelines in Case of Seismic Events	Selection of Appropriate Seismic Categories for Analysis and Construction
	Seismic Restraints and Supports
Choose Quality Standards Commensurate with Importance to Safety	Selection of Appropriate Construction Codes and Standards
Provide Systems which Detect Loss of Cooling and Excessive Radiation	Radiation Levels are Monitored
	Liquid Sodium Levels are Monitored
	Coolant Outlet Temperatures are Monitored
	Sodium Leak Detectors Between Fuel Storage Vessel and Guard Tank

REFERENCES

1. K. W. Foster, "Clinch River Breeder Reactor Project Fuel Handling System Features and Experience," Proceedings of 23rd Conference on Remote Systems Technology, ANS Winter Meeting, San Francisco, November 1975.

2. Clinch River Breeder Reactor Preliminary Safety Analysis Report, April 1975.

3. "Nuclear Power Experiences," B. J. Verna Publisher, P.O. Box 544, Encino, California 91316.

4. CRBRP-1, "CRBRP Risk Assessment Report," March 1977.

5. WASH-1400 (NUREG-75/014), "Reactor Safety Study," U.S. NRC, Appendix III, October 1975.

6. J. Graham, L. E. Strawbridge, and P. Bradbury, "Safety of the Clinch River Plant," Nuclear Engineering International, 19, 221 (1974).