

# **NUCLEAR SAFETY CRITERIA AND SPECIFICATIONS FOR SPACE NUCLEAR REACTORS**

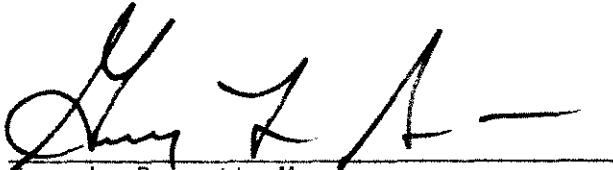


AUGUST 1982

**U.S. DEPARTMENT OF ENERGY**

**OFFICE OF SPACE NUCLEAR PROJECTS  
WASHINGTON, D.C. 20545**

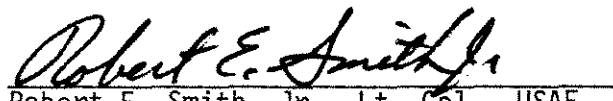
APPROVED BY THE OFFICE OF SPACE NUCLEAR PROJECTS:



Gary L. Bennett, Manager  
Safety and Isotope Fuels

8-11-82

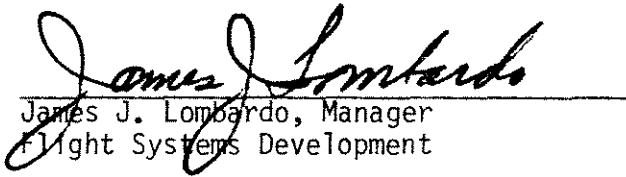
Date



Robert E. Smith, Jr., Lt. Col., USAF  
SP-100 Program Manager

11 August 1982

Date



James J. Lombardo, Manager  
Flight Systems Development

August 18, 1982

Date



B. J. Rock, Acting Director  
Office of Space Nuclear Projects

August 12, 1982

Date

# NUCLEAR SAFETY CRITERIA AND SPECIFICATIONS FOR SPACE NUCLEAR REACTORS

## TABLE OF CONTENTS

### Part A - Nuclear Safety Criteria for Space Nuclear Fission Reactors

	<u>Page</u>
1.0 General	A-1
1.1 Purpose	A-1
1.2 Objective	A-1
1.3 Scope	A-1
1.4 Implementation and Deviations	A-2
2.0 Definitions	A-3
3.0 Applicable Documents	A-4
4.0 Safety Documentation	A-5
4.1 General	A-5
4.2 Contents of Safety Analysis Reports	A-5
4.3 Schedule of Safety Analysis Reports	A-7
5.0 Safety Requirements	A-8
5.1 Safety Philosophy	A-8
5.2 Radiation Protection Safety Criteria	A-8

### Part B - Nuclear Safety Specifications for the SP-100 Space Nuclear Reactor Power System Technology Program

1.0 General	B-1
1.1 Purpose	B-1
1.2 Objective	B-1
1.3 Scope	B-1
1.4 Implementation and Deviations	B-1
2.0 Safety Design Requirements	B-2
3.0 Safety Specifications	B-3
3.1 Reliability and Quality Assurance	B-3
3.2 Safety Test and Analysis Program	B-3
3.3 Design/Manufacturing Testing and Inspection Program	B-3
3.4 Functional Requirements	B-4
3.4.1 Reactor Control System	B-4
3.4.2 Reactor Protection System	B-4
3.4.3 Reentry Core Dispersal Capability	B-5
3.4.4 Orbital Altitude Boost System	B-5
3.4.5 Spacecraft Attitude Control System	B-5
3.4.6 Reactor Control and Safety Systems	B-5
Communication System	
3.4.7 Independent Electric Power	B-5
3.4.8 Instrumentation System	B-6
3.4.9 Core Cooling System	B-6
3.5 Normal Operational Environments	B-6
3.6 Accident Environments	B-7
3.7 Design Margins	B-7

PART A  
NUCLEAR SAFETY CRITERIA  
FOR  
SPACE NUCLEAR FISSION REACTORS

1.0 GENERAL

The policy of the United States for all U.S. nuclear power sources in space is to ensure that the probability of release of radioactive material and the amounts released are such that an undue risk is not presented, considering the benefits of the mission.\*

1.1 Purpose

The purpose of this document is to define safety criteria which must be met to implement the U.S. policy. These criteria provide the bases for decisions on the acceptability of specific mission and reactor design proposals.

1.2 Objective

The objective of this document is to provide safety criteria which a mission/reactor designer can use to help ensure that the design is acceptable from a radiological safety standpoint.

1.3 Scope

These criteria encompass mission design, reactor design, and radiological impact limitation requirements for safety, and the documentation required. They do not address terrestrial operations, occupational safety or system reliability except where the systems are important for radiological safety. Specific safety specifications based on these criteria shall also be generated and made part of contractual requirements.

\*The U.S. approach to nuclear safety has been spelled out in a number of documents, e.g., 10CFR20 notes that in accordance with recommendations of the Federal Radiation Council, approved by the President, persons engaged in licensed activities should "make every reasonable effort to maintain radiation exposures, and releases of radioactive materials in effluents to unrestricted areas, as low as is reasonably achievable" taking into account the state of technology and the economics of improvement and other factors. DOE Order 5480.1A states that it is the policy of the DOE to "assure protection of the environment, the safety and health of the public, and Government property against accidental loss and damage." In a U.S. working paper submitted to the U.N. Working Group on the Use of Nuclear Power Sources in Outer Space (Paper A/AC.105/C.1/WG.V/L.8, dated 23 January 1980), it is stated that "the primary safety design objective is to minimize the potential interactions of the radioactive materials with the populace and the environments so that exposure levels are within limits established by international standards."

#### 1.4 Implementation and Deviations

These criteria are to be used as requirements on the reactor and spacecraft systems contractors. Proposed deviations to these criteria must be approved by the Department of Energy and reflected in contract modifications.

## 2.0 DEFINITIONS

In general, reference should be made to the American National Standard, "Glossary of Terms in Nuclear Science and Technology," ANS-9/ANSI-N1.1-1976 for acceptable definitions. For the purpose of these criteria and specifications, the following terms have the meaning indicated:

Common cause failure--An event in which more than one system, subsystem, structure, component or feature are rendered incapable of performing their functions because of a single, more basic triggering condition.

Design basis event--A postulated abnormal condition used in the design of a space reactor to establish the performance requirements of the reactor systems, subsystems, structures, components and features (including engineered safety features).

Engineered safety feature--A system, structure, component, or feature of a space nuclear reactor that has been designed to perform a specific safety function; in particular to prevent or control a design-basis event or mitigate its consequences.

Long-lived orbit, high orbit--An orbit with an altitude such that reentry of the reactor would not occur for 300 or more years.

Nuclear subsystem--Encompasses the reactor core, reactor control systems, heat transport systems, engineered safety features of the reactor, reflector, and shield.

Power conversion system (or subsystem)--That part of the reactor power system that converts fission-generated thermal energy to other useful forms of energy.

Short-lived orbit, low orbit--An orbit with an altitude such that reentry of the reactor would occur in less than 300 years.

Space reactor, reactor, or nuclear reactor--A device in which a self-sustaining nuclear fission chain reaction can be maintained and controlled. For the purposes of this document it is assumed that the reactor is put on a spacecraft.

### 3.0 APPLICABLE DOCUMENTS

The following documents are applicable to project safety requirements. If there is any conflict between these documents, the order of precedence is in the order listed:

- o DOE Orders on Nuclear Safety\*
- o This document
- o Project safety specifications
- o Nuclear subsystem specification

The documents listed below should be reviewed by the reactor systems contractor for any applicable criteria to be used in developing the specific safety specifications for flight reactors. It is recognized that these documents were not intended for space nuclear reactors.

- o Overall Safety Manual (1974, revised in 1981)
- o DOE 5480.1A, Environmental Protection, Safety, and Health Protection Programs for DOE Operations.
- o 10 CFR 50, Appendix A, General Design Criteria for Nuclear Powerplants

Documents referenced in DOE 5480.1A should also be used as appropriate.

The reactor systems contractor should prepare a detailed technical safety specification for the design and operation of the space reactor using this document and the appropriate parts of DOE 5480.1A and 10 CFR 50, Appendix A, as requirements.

\*For a specific mission and launch vehicle, the pertinent safety documents will also apply. These documents will be identified by the mission and launch agencies.

## 4.0 SAFETY DOCUMENTATION

### 4.1 General

Each space mission involving the launch of a nuclear reactor shall be formally analyzed by the reactor systems contractor to assess the potential radiological risk of the mission. These safety analyses, which are described in more detail in the Overall Safety Manual, shall begin at the initiation of the design concept and shall continue through the launch safety approval process. These safety analyses shall be formally reported to the Department of Energy in safety analysis reports at a minimum of three major points during the development and fabrication of the space reactor system (see also the Overall Safety Manual for additional description of the safety documentation). These safety analysis reports shall include: a Preliminary Safety Analysis Report (PSAR), an Updated Safety Analysis Report (USAR), and a Final Safety Analysis Report (FSAR). These reports will be reviewed by the Department of Energy and the Interagency Nuclear Safety Review Panel (INSRP).

### 4.2 Contents of Safety Analysis Reports

For ease of comparison, these reports should be of similar format. Each safety analysis report shall include volumes on:

Reference Design Document. This part of the safety analysis report shall contain a description of:

- o Mission and Flight System Summary
- o Nuclear Reactor (including type of fuel, design requirements, reactor materials and materials properties, radiation field at launch and during operation)
- o Power conversion subsystem
- o Ground support equipment
- o Spacecraft (including location and attachment of nuclear reactor)
- o Mission Profile
- o Launch Vehicle (including flight safety and tracking plans)
- o Reference Trajectory and Flight Characteristics (including launch conditions)
- o Launch Site (including demographic, topographic, and meteorological characteristics)



- o Range and Radiological Safety Operations
- o Safety-related systems, subsystems, and components (engineered safety features)

Accident Model Document. This part of the safety analysis report shall contain a description of:

- o Accident and Radiological Models and Data (including test data and verified and validated computer codes that support the analysis)
- o Vehicle and Reactor Failure Mode Analysis (from prelaunch through final disposition; with a description of the potential accident environments and flight contingency options)
- o Nuclear Reactor Response to Accident Environments (including prelaunch, launch, ascent, reentry, breakup, impact, post-impact--both land and water)
- o Mission Failure Evaluation (includes accident probabilities and quantity of radioactive material potentially released to provide a risk profile).

Nuclear Risk Analysis Document. This final part of the PSAR, USAR and FSAR shall be a probabilistic description of the potential radiological risk of those potential accidents which could involve the space reactor. The extent to which this final part will be included in the PSAR will be a function of the maturity of the mission data.

In general, the safety analysis reports shall consider the following types of accident environments (categorized by mission phase):

Prelaunch, Launch, and Ascent Phases

- Explosion overpressure
- Projectile impact
- Land or water impact
- Liquid propellant fire
- Solid propellant fire
- Sequential combination of the above

Orbit and/or Flight Trajectory Phases

- Reentry
- Land or water impact or collisions in space (meteroids, space debris)
- Post impact environment (land or water)

#### 4.3 Schedule of Safety Analysis Reports

The PSAR shall be issued soon after a design concept is selected for a given mission and shall include a description of the space reactor system and mission as well as probabilistic radiological risk assessments as supported by the available conceptual design data base. The USAR shall be issued as soon as practical after the design freeze. The USAR shall include updated information on the mission, the failure modes analysis, and the radiological risk assessment. The FSAR will normally be issued about 1 year before the scheduled launch. The FSAR shall provide a description of the final system, mission, and the radiological assessment data, including the results of any tests that support the safety analyses and an updated probabilistic risk analysis.

## 5.0 SAFETY REQUIREMENTS

### 5.1 Safety Philosophy

A system of dose limitation is required, the main features of which are:

- o no practice shall be adopted unless its introduction produces a positive net benefit;
- o all exposures should be kept as low as reasonably achievable, economic, technical, and social factors being taken into account;
- o the risk to individuals shall not exceed the limits specified for the appropriate circumstances.

The restriction of the exposure which is caused by the release of radioactive materials into the environment depends on appropriate arrangements for reducing the probability of accidents giving rise to releases of radioactive materials into the environment and for limiting the magnitude of these releases, should they occur.

### 5.2 Radiation Protection Safety Criteria

These criteria consist of radiological risk limits to individuals and populations. These risk limits are related to the assumed probability of the accident event chain leading to the radionuclide release. These criteria are to be used in assessing the consequences of the hypothetical accident.

#### Risk Limits for Individuals

- o A specific analysis shall be prepared as part of the safety approval process to demonstrate that the individual risk is as low as reasonably achievable, economic, technical and social factors being taken into account.

#### Risk Limits for Populations

- o The calculated annual population dose expectation is determined as follows: The spectrum of potential accidents and their estimated probabilities and consequences shall be identified. Then, the probability of each postulated accident is to be multiplied by the dose associated with that accident. This product ("risk index") is to be summed over the range of postulated accidents. A specific analysis shall be prepared as part of the safety approval process to demonstrate that the risk index is as low as reasonably achievable, economic, technical, and social factors being taken into account.

PART B  
NUCLEAR SAFETY SPECIFICATIONS  
FOR THE  
SP-100 SPACE NUCLEAR REACTOR  
POWER SYSTEM TECHNOLOGY PROGRAM

1.0 GENERAL

These nuclear safety specifications provide functional requirements for the SP-100 Program in meeting Part A, Nuclear Safety Criteria for Space Nuclear Fission Reactors.

1.1 Purpose

Nuclear safety specifications are to provide the reactor and mission designer with minimum requirements for engineered features regarded as important to radiological safety.

1.2 Objective

The objective of this document is to provide the necessary bases by which the nuclear safety criteria will be met. Sufficiency of the design in meeting these safety criteria will be assessed in the safety review process.

1.3 Scope

These specifications are applicable only to the SP-100 Program and the spacecraft on which the SP-100 reactor is used. Application of the SP-100 to unmanned short-lived orbit, long-lived orbit and Earth-escape trajectory missions is covered. These specifications do not address terrestrial operations, occupational safety or system reliability except where the systems are important for radiological safety. The requirements of these specification include:

- Documentation and Quality Assurance
- Testing and Inspection
- Functional Components
- Normal and Accident Environments,

relative to systems important to safety.

1.4 Implementation and Deviations

These specifications are to be used as contractual requirements on the reactor and spacecraft systems contractors. Proposed deviations to these specifications must be approved by the Department of Energy and reflected in contract modifications.

## 2.0 SAFETY DESIGN REQUIREMENTS

In consideration of safety objectives and risk limitations contained in this document, it has been determined that the following reactor design and mission design requirements are necessary, but not sufficient, in order to comply:

- o The reactor shall be designed to remain subcritical if immersed in water or other fluids (such as rocket propellants) to which it may be exposed.
- o The reactor shall have a significantly effective negative power coefficient of reactivity.
- o The reactor shall be designed so that no credible launch pad accident, range safety destruct actions, ascent abort or reentry from space resulting in Earth impact could result in a critical or supercritical geometry.
- o The reactor shall not be operated (except for zero power testing yielding negligible radioactivity at the time of launch) until a stable orbit or flight path is achieved and must have a reboost capability from low-earth orbit if it is operated in that orbit.
- o Two independent systems shall be provided to reduce reactivity to a subcritical state. They shall not be subject to common cause failure.
- o The reactor shall be designed to ensure that there is an independent shutdown heat removal system or independent heat removal paths within the heat transport system to provide decay heat removal.
- o The unirradiated fuel shall pose no significant environmental hazard.

Whenever the concept of independence is used in these specifications it shall be taken to mean an absence of any predicted, tested or analyzed susceptibility to common cause failures.

### 3.0 SAFETY SPECIFICATIONS

#### 3.1 Reliability and Quality Assurance

The engineered safety features shall be designed and built in conformance to STS-1, Quality Assurance Program Requirements and STS-2, Reliability Engineering Program Requirements. The engineered safety features shall be shown (by conservative analysis and/or test) to meet Part A, Nuclear Safety Criteria for Space Nuclear Fission Reactors.

#### 3.2 Safety Test and Analysis Program

The reactor systems contractor shall conduct a safety test and analysis program to assess the response of the SP-100 reactor to postulated credible accidents. The results of the safety test and analysis program will form the technical basis for the safety analysis reports.

The reactor systems contractor will prepare a safety test and analysis program plan which will address these criteria and specifications. The plan will include:

- o Objectives
- o Background (with justification for types of tests and analyses)
- o Program Management and Implementation
- o Analytical Program
- o Test Program (including correlation with analytical efforts through pre- and post-test analyses to show reason for each test), schedule and funding plan.

After completion of the test program, a test report shall be issued containing results, conclusions, and recommendations.

#### 3.3 Design/Manufacturing Testing and Inspection Program

The development of the SP-100 shall be accompanied by a design/manufacturing test and inspection program to verify the design concept, to show conformance to safety specifications and to provide the data for the quality control of the manufacture of the engineered safety features.

A design/manufacturing testing and inspection plan shall be developed by the reactor systems contractor, and approved by the Department of Energy. The approval agency is the DOE Program Office. The plan shall contain rationale, test objectives, and procedures.

After completion of the test program, a test report shall be issued which contains results, conclusions, and recommendations.

### 3.4 Functional Requirements

The following safety related systems/functions shall be provided.

#### 3.4.1 Reactor Control System

Positive coded telemetry shall be required to start up the reactor. Thus, the reactor shall have a reactor control system which, in addition to the design requirement of being capable of initiating reactor start-up, shall be capable of controlling power escalation to full power level and of reducing power to a full shutdown mode. The system shall be capable of being operated in a directed positive shutdown mode and of restarting the reactor following a shutdown.

#### 3.4.2 Reactor Protection System

A reactor protection system which includes two independent systems not subject to common cause failure to reduce reactivity to a subcritical state shall be provided. This system, which is one of the engineered safety features, shall be capable of sensing conditions which would call for reactor shutdown and of automatically shutting the reactor down, with restart capability. Except for the neutron absorber/reflector elements and their activators, the protection system shall be independent from the control system. Conditions calling for automatic reactor shutdown by the protection system are:

- o Failure of the reactor control system
- o Failure of the spacecraft attitude control system
- o Exceeding of fuel design temperature limits
- o Failure of Earth/spacecraft reactor control and/or safety systems communications system.

The reactor protection system shall have fault detection sensors and shall be designed to be able to be tested while the reactor is operating (without actually shutting the reactor down). It shall be capable of performing this function, assuming a single system failure, and shall not be subject to common cause failures with systems/conditions upon which it is called to activate in case of their failure. The reactor protection system shall be designed such that any failure of the system puts the reactor in a safe condition. The reactor systems contractor shall specify in the detailed technical safety specification (subject to DOE approval), the minimum shutdown reactivity during

- assembly/testing
- ground handling/storage
- transportation
- launch

### 3.4.3 Reentry Core Dispersal Capability

For short-lived orbit missions, a reentry core dispersal capability shall be provided. This capability will ensure that the reactor core and activated structural elements will be dispersed such that the Nuclear Safety Criteria for Space Nuclear Fission Reactors (Part A) are not exceeded. This capability shall be provided such that the reentry environment of the reactor separate from the launch vehicle will initiate and cause the required dispersal with no active systems required to operate.

### 3.4.4 Orbital Altitude Boost System

An orbital altitude boost system shall be provided by the mission agency (short-lived orbit missions only). This system shall be capable of boosting the reactor to a high orbit following completion of the mission or upon mission failure such that the radiation protection safety criteria of Section 5.2 of Part A are met. Typically, an orbital lifetime of at least 300 years will be required. This system shall be interlocked with the spacecraft attitude control system such that it will not operate if attitude is not controlled.

### 3.4.5 Spacecraft Attitude Control System

A spacecraft attitude control system shall be provided on the spacecraft by the spacecraft system contractor such that spacecraft attitude can be controlled to permit communication with the reactor control and safety related systems and (for short-lived missions) to permit the orbital altitude boost system to perform its function.

### 3.4.6 Reactor Control and Safety Systems Communication System

A reactor control and safety systems communication system shall be provided such that reactor, reactor control system, power conversion system, and safety systems status may be monitored and controlled. Two independent systems shall be provided.

### 3.4.7 Independent Electrical Power

An independent source of electrical power shall be provided such that the reactor control system, the reactor protection system and the reactor control and safety systems communications systems can operate independently of reactor operating mode or reactor power conversion system operation. This secondary source of power shall be capable of providing power for safety related systems operation and reactor restart capability for a minimum of 24 hours following failure of the reactor power conversion system during the spacecraft mission lifetime.



### 3.4.8 Instrumentation System

An instrumentation system shall be provided which provides, through the reactor control and safety systems communication system, signals to allow continuous determination of:

Reactor power level (and rate of change)

Fuel Temperature

Control/Reflector Element positions

Status of:

- Reactor control system
- Reactor protection system
- Power conversion system
- Spacecraft attitude control system
- Orbital altitude boost system (short-lived orbit missions only)
- Independent electrical power source.

### 3.4.9 Core Cooling System

Following a shutdown the core cooling system shall be capable of providing adequate heat removal from the core with sufficiently independent shutdown heat removal paths or with an independent shutdown heat removal system to prevent the fuel temperature limit from being exceeded and safety systems from being rendered inoperable.

## 3.5 Normal Operational Environments

Safety Systems shall be designed to withstand, without loss of capability to perform their safety functions, the effects of normal operational environments, including those present during the following mission phases:

Storage  
Ground Handling  
Launch and Ascent  
Duration of Mission

Environments of storage and ground handling are to be defined commensurate with the ground operations involved in manufacture, testing, shipping, and installation onto the launch vehicle of the SP-100.

Launch and ascent environments are to be those appropriate to the launch vehicle/payload configuration. These environments include:

Vibration  
Shock  
Acceleration  
Acoustic noise  
Pressure

Environments of the duration of the mission include the radiation field created by reactor operation plus that of space. They also include micrometeoroids and fine particulates which could jam mechanical linkages.

### 3.6 Accident Environments

The SP-100 shall be designed such that the risk limits in Section 5.2 of Part A, Nuclear Safety Criteria for Space Nuclear Fission Reactors are not exceeded.

The accident probabilities and environments which must be considered are those of the specific launch vehicle and spacecraft propulsion systems which are to be part of a proposed mission.

The safety requirements of Section 5.0 of Part A, Nuclear Safety Criteria for Space Nuclear Fission Reactors are to be met.

### 3.7 Design Margins

Design margins are derived quantities, usually of a deterministic nature, which depend on or are evaluated against system reliability goals and radiological risk limitation goals. They must reflect consideration of normal mission operation system failure rates and accident probabilities and environments.

Structures, subsystems, components, and features shall be designed to withstand with margin and without loss of their capability to perform their safety functions or to meet the safety requirements of Section 5.0 of Part A the effects of:

- o operation
- o maintenance
- o testing
- o postulated accident conditions for which their response is required
- o storage
- o ground handling
- o launch and flight vibration
- o acceleration and shock
- o temperature
- o nuclear and solar radiation
- o micrometeoroids
- o overpressure
- o acoustic noise
- o humidity

The expected mission levels and conditions of these parameters will be defined by DOE for each mission, as well as the required margin, and made a part of contract requirements of the reactor systems contractor. The reactor systems contractor will prepare detailed technical safety specifications for the nuclear reactor and submit them to the Department of Energy for approval.