TID-27265

SYSTEM SAFETY PROGRAM PLAN
FOR THE
ISOTOPE BRAYTON GROUND
DEMONSTRATION SYSTEM
(PHASE I)

75-311221

September 30, 1975

MASTER

AIRESEARCH MANUFACTURING COMPANY OF ARIZONA
A DIVISION OF THE GARRETT CORPORATION.
PHOENIX, ARIZONA

DISTRIBUTION OF THIS DOCUMENT IS UNLIMITED

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.

NOTICE

This report was prepared as an account of work sponsored by the United States Government. Neither the United States nor the United States Energy Research and Development Administration, nor any of their employees, nor any of their contractors, subcontractors, or 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.

SYSTEM SAFETY PROGRAM PLAN
FOR THE
ISOTOPE BRAYTON GROUND
DEMONSTRATION SYSTEM
(PHASE I)

75-311221

September 30, 1975

Approved by ERDA December 1, 1975
Published December 12, 1975

Prepared by:

L. G. Miller / L.G.M.
L.G. Miller

Approved by:

J. E. McCormick
J.E. McCormick
Project Director,
Mini-BRU Systems

AIRESEARCH MANUFACTURING COMPANY OF ARIZONA
A DIVISION OF THE GARRETT CORPORATION

MASTER

DISTRIBUTION OF THIS DOCUMENT IS UNLIMITED

REPORT NO. 75-311221

TOTAL PAGES 27

ATTACHMENTS:

REV	BY	APPROVED	DATE	PAGES AND/OR PARAGRAPHS AFFECTED
--	ADM	LGM	12-12-75	Initial Issue

AIRESEARCH MANUFACTURING COMPANY OF ARIZONA
A DIVISION OF THE GARRETT CORPORATION
PHOENIX, ARIZONA

TABLE OF CONTENTS

	<u>Page</u>
1.0 GENERAL	1
1.1 Introduction	1
1.2 Scope and Purpose	1
1.3 Application and Implementation	2
1.4 Applicable Documents	2
2.0 SAFETY ORGANIZATION, RESPONSIBILITIES AND AUTHORITY	4
2.1 Prime Contractor Organization	4
2.2 Subordinate (Sub) Contractor Organization	4
2.3 Interface Relationships	4
2.4 Responsibilities and Authority	8
3.0 SYSTEM SAFETY CRITERIA	9
3.1 Definitions	9
3.2 Hazard Level Categories	10
3.3 System Safety Precedence	11
3.4 Special Contractual Requirements	11
3.5 Identification of Techniques for Analysis	11
4.0 SYSTEM SAFETY TASKS TO BE COMPLETED	17
4.1 Schedule	17
4.2 Tasks	17
4.3 Program Review Participation	20
4.4 Design Review Participation	20
5.0 SYSTEM SAFETY DOCUMENTATION	21
5.1 Reports To Be Published	21
5.2 Reports To Be Received	22
5.3 Safety Data Bank	22
5.4 Dissemination of Safety Data	23
6.0 SAFETY PROGRAM CONTROL	25

LIST OF FIGURES

<u>Figure No.</u>	<u>Title</u>	<u>Page</u>
2-1	AIRPHX PROGRAM ORGANIZATION	5
2-2	GE IBS PROGRAM ORGANIZATION	6
2-3	SAFETY LIAISON AND WORKING CHANNELS	7
3-1	PRELIMINARY HAZARD ANALYSIS (FORM)	13
3-2	FAILURE MODES, EFFECTS AND CRITICALITY ANALYSIS WORKSHEET	15
4-1	SAFETY SCHEDULE - PHASE I ACTIVITIES	18
5-1	SAFETY DATA BANK CARD	23

page blank

page blank

AIRESEARCH MANUFACTURING COMPANY OF ARIZONA
A DIVISION OF THE GARRETT CORPORATION
PHOENIX, ARIZONA

Garrett Corporation - Corporate Policy

Administration 1-8

Product Integrity Organization

Production 4-1

Product Quality, Reliability, and
Safety

AiResearch, Phoenix - Operational Procedures

2.57

System Safety Program

10.35

Product Integrity Director and
Committee

AIRESEARCH MANUFACTURING COMPANY OF ARIZONA
A DIVISION OF THE GARRETT CORPORATION
PHOENIX, ARIZONA

2.0 SAFETY ORGANIZATION, RESPONSIBILITIES AND AUTHORITY

2.1 Prime Contractor Organization

AiResearch, Phoenix (AIRPHX) BIPS program organizational structure is depicted in Figure 2-1. The GDS/FS Project Safety Manager is a full time member of the BIPS Program and reports directly to the Project Director.

2.2 Subordinate (Sub) Contractor Organization

General Electric, Valley Forge (GE-VF) program organizational structure is depicted in Figure 2-2.

2.3 Interface Relationships

The safety liaison and working channels are depicted in Figure 2-3. Direct communication is authorized and indeed encouraged between the BIPS Project Safety Manager and all agencies, subcontractors, and elements having a responsibility for contributing to the overall safety effort. Daily contact will be maintained with engineers assigned to the BIPS project. In addition, Program Safety Monitors will be appointed in each functional area to insure adequate coordination. Certain Safety Monitors have been identified (see Figure 2-3); others will be added as the need becomes evident. A separate System Safety staff reporting to the Director of Product Integrity monitors the adequacy of the safety plan and its implementation. Resolution of major points of disagreement takes place within the Product Integrity Committee made up of senior managers of AIRPHX.

AIRESEARCH MANUFACTURING COMPANY OF ARIZONA
A DIVISION OF THE GARRETT CORPORATION

AIRPHX PROGRAM ORGANIZATION
FIGURE 2-1

GE BRAYTON ISOTOPE POWER SYSTEM PROGRAM ORGANIZATION

FIGURE 2-2

AIRESEARCH MANUFACTURING COMPANY OF ARIZONA
A DIVISION OF THE GARRETT CORPORATION

AIRESEARCH MANUFACTURING COMPANY OF ARIZONA
A DIVISION OF THE GARRETT CORPORATION
PHOENIX, ARIZONA

2.4 Responsibilities and Authority

AiResearch Operational Procedures 2.57 and 10.35 specify the organizational responsibilities for Safety at AiResearch.

The Engineering Project is responsible for safety in the product design and has primary responsibility for defining and conducting the System Safety Program as it affects product design. A System Safety Manager has been designated for managing the safety program for the BIPS Project.

The Safety Manager assigned to the program is charged with implementing, maintaining, and controlling the system safety portions of the program described in this document. He reports to the BIPS Project Director.

Other departments are required to appoint system safety monitors for this program with responsibility to work within the scope of the System Safety Program Plan. These monitors will provide information and support upon request from the Project Safety Manager.

The Director of Product Integrity is responsible for monitoring and coordinating all divisional policies and procedures related to System Safety. He is also responsible for the overall effectiveness of the methods for complying with applicable portions of MIL-STD-882.

The Product Integrity Committee is responsible, among other things, for final resolution of major areas of disagreement which may arise within the program concerning safety.

Subcontractors will provide safety data, analyses, and support as determined to be required and as covered by contractual agreement.

3.0 SYSTEM SAFETY CRITERIA

3.1 Definitions (from MIL-STD-882 and other sources)

Safety

Freedom from those conditions that can cause injury or death to personnel, damage to or loss of equipment or property.

System

A composite, at any level of complexity, of operational and support equipment, personnel, facilities, and soft-ware which are used together as an entity and capable of performing and/or supporting an operational role.

System Safety

The maximum degree of safety within the constraints of operational effectiveness, time and cost attained through specific application of system safety management and engineering principles throughout all phases of a system's life cycle.

System Safety Management

An element of program management which insures the accomplishment of the system safety tasks including (a) identification of the system safety requirements; (b) planning, organizing, and controlling those efforts which are directed toward achieving the safety goals; (c) coordinating with other (system) program elements and (d) analyzing, reviewing, and evaluating the program to insure effective and timely realization of the system safety objectives.

System Safety Engineering

An element of systems engineering involving the application of scientific and engineering principles for the timely identification of hazards and the initiation of those actions necessary to prevent or control hazards within the system. It draws upon professional knowledge and specialized skills in the mathematical, physical, and related scientific disciplines, together with the principles and methods of engineering design and analysis to specify, predict, and evaluate the safety of the system.

Hazard

Any real or potential condition that can cause injury or death to personnel, or damage to or loss of equipment or property or contamination of facilities.

Reliability

The probability that the system or some part thereof will perform its intended function for a specified period of time under a set of specified environmental conditions.

Quality Assurance

The planned, systematic set of actions taken to provide adequate confidence that the system, or some portion thereof, will perform satisfactorily when put to use.

3.2 Hazard Level Categories

As stated in MIL-STD-882, a qualitative measure of hazards may be defined in relative terms, and the following hazard levels have been defined and established. These hazard levels will include conditions of personnel error, environment, design characteristics, procedural deficiencies, or subsystem or component failure or malfunction. The hazard levels are:

AIRESEARCH MANUFACTURING COMPANY OF ARIZONA
A DIVISION OF THE GARRETT CORPORATION
PHOENIX, ARIZONA

- (a) Category I - Negligible - . . . will not result in personnel injury or system damage.
- (b) Category II - Marginal - . . . can be counteracted or controlled without injury to personnel or major system damage.
- (c) Category III - Critical - . . . will cause personnel injury or major system damage, or will require immediate corrective action for personnel or system survival.
- (d) Category IV - Catastrophic - . . . will cause death or severe injury to personnel, or system loss.

These Hazard Categories will be used for reliability analyses such as the Failure Mode and Effects Analysis (FMEA) as well as for safety analyses in order to provide standard terminology among project elements.

3.3 System Safety Precedence

Paragraph 5.6 of MIL-STD-882 shall apply.

3.4 Special Contractual Requirements

TBD

3.5 Identification of Techniques for Analysis

During Phase I, the Preliminary Hazard Analysis, Failure Mode and Effects Analysis, and Fault Tree Analysis will be the principle analytical techniques to be utilized. These are discussed in detail in the paragraphs which follow.

3.5.1 Preliminary Hazard Analysis (PHA)

Preliminary Hazard Analyses will be prepared for both the GDS (to include the test facility systems and equipment) and the FS. These will identify and classify the hazards to which personnel and the major components comprising these systems may be exposed. The sample

AIRESEARCH MANUFACTURING COMPANY OF ARIZONA
A DIVISION OF THE GARRETT CORPORATION
PHOENIX, ARIZONA

work sheet, Figure 3-1, will be used in compiling the necessary data. After becoming familiar with each major component envisioned for the system, each component will be checked against a list of possible hazards. Those hazards and undesired events considered possible will then be entered on the PHA worksheet with notation of Program Phase (e.g., tests, ground transport, operation in space, etc.), cause (event creating the hazard), effect (on personnel/equipment), and the category of the hazard. Note the two columns under "Hazard Category" in Figure 3-1. The first column will contain the Hazard Category (see Section 3.2) before "corrective action/minimizing provisions" have been assigned. Once assigned, the revised Hazard Category can then be entered in the second column. Critical and catastrophic hazards will be eliminated or controlled. If these hazards cannot be eliminated or brought to an acceptable level of probability, the matter will immediately be reported to the Project Director for resolution and reporting to the procuring agency (ERDA).

The PHA is, as the name implies, a preliminary analysis and is, by definition, a gross qualitative review. It serves to document the fact that all subsystems/components were initially examined from the viewpoint of safety. From this review, the significant hazards/undesired events can be identified. The probability of occurrence of specific hazards/undesired events can then be determined by means of the Fault Tree Analysis which follows.

3.5.2 Fault Tree Analysis (FTA)

A Fault Tree Analysis will be performed on selected Category III and IV hazards/undesired events identified by the PHA. In brief terms, the FTA method may be described as follows: (a) One first selects the undesired event whose probability of occurrence is to be determined. (b) A "tree" is prepared with the undesired event at the top. Directly below are placed those events which could directly cause the hazard/undesired event. At each succeeding level, one places events

PRELIMINARY HAZARD ANALYSIS

SYSTEM/SUBSYSTEM IDENTIFICATION							
NO.	HAZARD/UNDESIREDEVENT	PROG. PHASE	CAUSE	EFFECT	HAZARD CATEGORY		CORRECTIVE ACTION/ MINIMIZING PROVISIONS

PRELIMINARY HAZARD ANALYSIS

FIGURE 3-1

75-311221

Page 13

AIRESEARCH MANUFACTURING COMPANY OF ARIZONA
A DIVISION OF THE GARRETT CORPORATION
PHOENIX, ARIZONA

which cause or contribute to the events directly above. When completed the diagram is called a "fault tree". (c) The probability of each component failure or event occurrence is determined. These probabilities may come from a number of sources - test data, part failure rates, extrapolation from similar components, etc. (d) These probabilities are then used to calculate the probability of occurrence of the undesired event being investigated. A computer program developed by AiRLA will be utilized for these calculations. (e) Additional analysis may be conducted which shows the number of simultaneous failures which must occur to cause the undesired event. Results of the FTA will be incorporated into the Preliminary System Safety Review.

3.5.3 Failure Mode, Effects and Criticality Analysis (FMECA)

A Failure Mode, Effects and Criticality Analysis will be performed on each major subsystem. While primarily a tool of the reliability engineer, the Program Safety Manager will participate in the preparation of the FMECA and will utilize its data to the maximum extent possible. He will be responsible for completion of the Hazard Classification and Safety Action sections of this analysis. The worksheet shown in Figure 3-2 will be used in compiling the data. Hazard categories as defined in MIL-STD-882 will be used in the FMECA.

In order to conform to the requirements of the ERDA Reliability Specification, SNS-2, dated 17 June 1974, the FMECA worksheet will contain three columns not routinely used in such analyses. These columns, headed A, B, and C, will be used to calculate a relative measure of failure mode and effects criticality in the following manner: (a) The failure mode will be ranked on a relative scale of likelihood from 1 to 100 (with 100 being the most likely) and this number will be placed in column "A". (b) The effect of the failure will be ranked on a scale of 1 to 100 (with 100 being the most likely) and this number will be

AIRESEARCH MANUFACTURING COMPANY OF ARIZONA
A DIVISION OF THE GARRETT CORPORATION
PHOENIX, ARIZONA

SYSTEM _____

COMPLETED BY _____

SUBSYSTEM _____

DATE _____

COMPONENT	FAILURE MODE (S)	PROBABLE CAUSE	EFFECT OF FAILURE	FAILURE MODE MINIMIZATION	*A	*B	*C	HAZ CAT	SAFETY ACTION OR COMMENTS

*A MODE LIKELIHOOD (1 TO 100) - *B EFFECTS IMPACT (1 TO 100) - *C CRITICALITY (A x B)

FAILURE MODES, EFFECTS AND CRITICALITY ANALYSIS WORKSHEET

AIRESEARCH MANUFACTURING COMPANY OF ARIZONA
A DIVISION OF THE GARRETT CORPORATION
PHOENIX, ARIZONA

placed in column "B". (c) Numbers in columns A and B will be multiplied together to produce a criticality ranking, and this number will be placed in column C.

A preliminary FMECA will be performed on the preliminary IBFS design very early in Phase I. It will be completed six months after receipt of order (ARO) and will of necessity be a very preliminary analysis. An FMECA of the GDS (to include the test facility systems and equipment) will receive concurrent attention with the objective being to complete a preliminary FMECA 12 months ARO in order to have it available for the Preliminary Design Review. The final FMECA for the GDS will be completed 18 months ARO.

4.0 SYSTEM SAFETY TASKS TO BE COMPLETED

4.1 Schedule

The schedule for Phase I Safety Activities is depicted in Figure 4-1.

4-2 Tasks

The specific tasks required of the Program Safety Manager follow:

- (a) Establish and maintain liaison with ERDA-DANES, the appropriate National Laboratories (SLA, LASL, Mound Laboratory, etc.), and the subcontractors (GE, AIRLA). The objective of this liaison activity is to coordinate all safety related matters of the project and to collect data pertinent to the safety assessment effort. Information on related programs will be reviewed.
- (b) Identify all applicable safety requirements, including those established by ERDA, NASA, DOD, and OSHA. Appropriate measures will be taken to eliminate or minimize all identified hazards in both the GDS and the IBFS.
- (c) Monitor and review all power system development and test activities for applicability to the safety evaluation. A continuous review will be required to assure that design changes do not adversely affect safety levels previously established.
- (d) Complete the analyses (PHA, FMECA, FTA) as outlined in Sections 3.5.1 through 3.5.3.

AIRESEARCH MANUFACTURING COMPANY OF ARIZONA
A DIVISION OF THE GARRETT CORPORATION

MONTHS AFTER RECEIPT OF ORDER

SAFETY SCHEDULE - PHASE I ACTIVITIES

FIGURE 4-1

AIRESEARCH MANUFACTURING COMPANY OF ARIZONA
A DIVISION OF THE GARRETT CORPORATION
PHOENIX, ARIZONA

- (e) Review SURVSATCOM mission characteristics and determine potential environments to which the IBFS can be exposed. Vehicle and mission information will be extracted from data of previously flown missions and from previous studies of planned missions of a similar nature (e.g., FSAR for the MHW/RTG for LES 8/9).
- (f) Identify and define specific analyses and/or tests not already programmed or completed which will be required as part of the safety assessments.
- (g) Assure that all concerned are apprised of key, critical safety issues and are provided the assistance required to eliminate or minimize identified hazards/undesired events.
- (h) Conduct a Preliminary System Safety Review. This safety review will in general fulfill the requirements of Section 4.2 of the AEC-DANES publication, "Heat Source Safety Design Specification for Space Application" but will be specifically tailored to reflect the tentative status of the preliminary IBFS design during Phase I. It is envisioned to be a somewhat abridged version of the typical PSAR but will serve as a basis for the safety work to be conducted during Phase II. Maximum utilization will be made of studies and data already available on systems which make use of the MHW heat source. The review will be prepared in two stages. The first draft will be available for review by ERDA 18 months after initiation of Phase I. It will basically treat the IBFS but will, in addition, address the safety aspects of the GDS (to include the test facility systems and equipment). The final version of the review will be published after 33 months.

AIRESEARCH MANUFACTURING COMPANY OF ARIZONA
A DIVISION OF THE GARRETT CORPORATION
PHOENIX, ARIZONA

- (i) Sign all reports and safety analyses prepared during Phase I. The Program Safety Manager will conduct a safety review and will personally approve the BIPS design, the GDS facility/support equipment designs, and the GDS test plans and procedures.

4.3 Program Review Participation

The Project Safety Manager will participate in periodic Program Review meetings by providing status summaries of the safety program.

4.4 Design Review Participation

The Preliminary FMECA of the GDS will become a part of the Preliminary GDS Design Review to be conducted at the end of 12 months; similarly, the Final FMECA of the GDS will be a part of the Design Review to be conducted at the end of 18 months.

AIRESEARCH MANUFACTURING COMPANY OF ARIZONA
A DIVISION OF THE GARRETT CORPORATION
 PHOENIX, ARIZONA

5.0 SYSTEM SAFETY DOCUMENTATION

5.1 Reports To Be Published

The following reports will be published during Phase I:

	<u>Months ARO</u>
SSPP (Phase I)	1
PHA - FS	4
PHA - GDS (to include test facility)	5
Preliminary FMECA - IBFS (primarily a Reliability function)	6
Preliminary FMECA - GDS (to include test facility)	12
Final FMECA - GDS (to include test facility)	18
Preliminary System Safety Review (draft)	18
Preliminary System Safety Review (publish final version)	33
Draft SSPP (Phase II) (to include a Ground Safety Program Plan)	33
Safety Input to Final Report	33

The contract will determine which reports are required to be submitted to the procuring agency.

In the event of serious accident, incident, or other reportable occurrence, ERDA Manuals 0502 and 0550 will be used for guidance.

AIRESEARCH MANUFACTURING COMPANY OF ARIZONA
A DIVISION OF THE GARRETT CORPORATION
PHOENIX, ARIZONA

5.2 Reports To Be Received

The following types of reports and data will be obtained from sub-contractors, safety monitors, and project designers:

- o Any existing Safety Analysis Reports on the Heat Source, the Recuperator, the Heat Source Assembly, the Radiator, and other major components.
- o Existing Safety Analysis Reports on similar systems, such as the MHW/RTG LES 8/9 program.
- o Input necessary to complete the PHA and FMECA work sheets.
- o Input, especially failure probabilities, necessary to complete the FTA.

In addition, the Safety Manager will have access to Engineering Specifications, Drawings, Schematics, Quality Assurance Reports, and Test Reports maintained within the Project group.

5.3 Safety Data Bank

A data bank will be accumulated and maintained within the Safety Manager's Office and will be available to other disciplines such as reliability and quality assurance. The data bank will contain the following:

- o Chronological records of actions taken to implement the system safety program.
- o Results of all safety analyses performed

- o Corrective action taken to eliminate or minimize hazards/undesired events
- o Safety specifications and criteria
- o Safety data bank card for each major component and subcomponent (see Figure 5-1)
- o Safety data on similar systems as available.

5.4 Dissemination of Safety Data

Safety data will be distributed to program associates and subcontractors on a case-by-case basis. All active members of the project group will be kept informed by means of published reports in addition to daily contact. Distribution of special reports and notifications will be made as the need arises.

AIRESEARCH MANUFACTURING COMPANY OF ARIZONA
A DIVISION OF THE GARRETT CORPORATION
PHOENIX, ARIZONA

COMPONENT _____ DATE _____

MANUFACTURER _____ PART NO. _____

FUNCTION: _____

USE HISTORY: Failure Rate _____

Reliability Level _____ Actual () Theoretical ()

Test History Available _____

SYSTEM USE: Where Used in System? _____

_____ In What Other System(s) Has It Been Used? _____

TYPES OF COMPONENT FAILURE (What Events [May] Cause Failure?) _____

CONSEQUENCES OF FAILURE TO SYSTEM AND ENVIRONMENT: _____

REMARKS: _____

SOURCE(S) OF INFORMATION: _____

SAFETY DATA BANK CARD

FIGURE 5-1

75-311221

Page 24

AIRESEARCH MANUFACTURING COMPANY OF ARIZONA
A DIVISION OF THE GARRETT CORPORATION
PHOENIX, ARIZONA

6.0 SAFETY PROGRAM CONTROL

Two independent checks of the System Safety Program activities will be made, one by the Program Director and one by the Director of Product Integrity, to provide assurance that the safety program is both adequate in scope and timely in execution.

Final resolution of safety-related conflicts is accomplished by the Product Integrity Committee under the Chairmanship of the Director of Product Integrity.