DDA

(2)

DTIC FILE COPY

AD NO. ____________________
REPORT NO. USACSTA-6572

US ARMY
MATERIEL COMMAND

AD-A184 295

DTIC
ELECTE
SEP 0 4 1987
S D
D

SPECIAL STUDY

OF

GUIDE FOR THE DEVELOPMENT OF

SAFETY ASSESSMENT REPORT (SAR)


MARTIN MOSSA

SAFETY OFFICE

U.S. ARMY COMBAT SYSTEMS TEST ACTIVITY
ABERDEEN PROVING GROUND, MD 21005-5059


AUGUST 1987

DISTRIBUTION STATEMENT A
Approved for public release;
Distribution Unlimited

Prepared for:
U.S. ARMY MATERIEL COMMAND
ALEXANDRIA, VA 22333-0001

DISTRIBUTION UNLIMITED.

87 9 3 087

## DISPOSITION INSTRUCTIONS

Destroy this report when no longer needed. Do not return to the originator.

## DISCLAIMER STATEMENT

The views, opinions, and/or findings in this report are those of the author(s) and should not be construed as an official Department of the Army position, unless so designated by other Official documentation.

Unclassified

SECURITY CLASSIFICATION OF THIS PAGE

A184295

# REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188
Exp. Date: Jun 30, 1986

**1a. REPORT SECURITY CLASSIFICATION**
Unclassified

**1b. RESTRICTIVE MARKINGS**

**2a. SECURITY CLASSIFICATION AUTHORITY**

**2b. DECLASSIFICATION / DOWNGRADING SCHEDULE**
None

**3. DISTRIBUTION / AVAILABILITY OF REPORT**
Distribution Unlimited.

**4. PERFORMING ORGANIZATION REPORT NUMBER(S)**
USACSTA-5472

**5. MONITORING ORGANIZATION REPORT NUMBER(S)**
Not applicable

**6a. NAME OF PERFORMING ORGANIZATION**
U.S. Army Combat Systems Test Activity

**6b. OFFICE SYMBOL** *(If applicable)*
STECS-SO-S

**7a. NAME OF MONITORING ORGANIZATION**
Not applicable

**6c. ADDRESS** *(City, State, and ZIP Code)*
Aberdeen Proving Ground, MD 21005-5059

**7b. ADDRESS** *(City, State, and ZIP Code)*
Not applicable

**8a. NAME OF FUNDING / SPONSORING ORGANIZATION**

**8b. OFFICE SYMBOL** *(If applicable)*

**9. PROCUREMENT INSTRUMENT IDENTIFICATION NUMBER**
Not applicable

**8c. ADDRESS** *(City, State, and ZIP Code)*

**10. SOURCE OF FUNDING NUMBERS**

| PROGRAM ELEMENT NO. | PROJECT NO. | TASK NO. | WORK UNIT ACCESSION NO. |
|---|---|---|---|
| | | | |

**11. TITLE** *(Include Security Classification)*
GUIDE FOR THE DEVELOPMENT OF SAFETY ASSESSMENT REPORT (SAR)

**12. PERSONAL AUTHOR(S)**
Mossa, Martin

**13a. TYPE OF REPORT**
Special Study

**13b. TIME COVERED**
FROM Nov 85 TO Aug 87

**14. DATE OF REPORT** *(Year, Month, Day)*
August 1987

**15. PAGE COUNT**

**16. SUPPLEMENTARY NOTATION**
This report is a product of the U.S. Army Materiel Command Action Committee for System Safety.

**17. COSATI CODES**

| FIELD | GROUP | SUB-GROUP |
|---|---|---|
| | | |
| | | |

**18. SUBJECT TERMS** *(Continue on reverse if necessary and identify by block number)*
Safety Assessment Report (SAR) System Safety
Preliminary Hazard Analysis
Fault Tree Analysis

**19. ABSTRACT** *(Continue on reverse if necessary and identify by block number)*

This report was developed by the Research and Development (R&D) subcommittee of the AMC Action committee for system safety and is intended to provide researchers, combat developers, program managers, contractors, testers and users guidance to develop a comprehensive and effective safety assessment report (SAR).

**20. DISTRIBUTION / AVAILABILITY OF ABSTRACT**
☐ UNCLASSIFIED/UNLIMITED ☒ SAME AS RPT. ☐ DTIC USERS

**21. ABSTRACT SECURITY CLASSIFICATION**
Unclassified

**22a. NAME OF RESPONSIBLE INDIVIDUAL**
Martin Mossa

**22b. TELEPHONE** *(Include Area Code)*
301-278-3898

**22c. OFFICE SYMBOL**
STECS-SO-S

DD FORM 1473, 84 MAR

83 APR edition may be used until exhausted.
All other editions are obsolete.

SECURITY CLASSIFICATION OF THIS PAGE
Unclassified

**AMC ACTION COMMITTEE FOR SYSTEM SAFETY**

**Research and Development**
**Sub-committee**

| | |
|---|---|
| Martin Mossa | USACSTA |
| Doug Paul | USABRDC |
| Charles Garrett | USACRDEC |
| Felix Aguinaga | USAAMICOM |
| Jim Stanley | PM-TRADE |

## TABLE OF CONTENTS

# GUIDE FOR THE DEVELOPMENT OF SAFETY ASSESSMENT REPORT (SAR)

## I. INTRODUCTION:

This report was developed by the R&D subcommittee of the AMC action committee for system safety and is intended to provide researcher, combat developers, program managers, contractors, testers, and users, guidance to develop a comprehensive and effective safety assessment report (SAR). The SAR is a formal, comprehensive safety report that summarizes the safety data that has been collected and evaluated during the life cycle of an item (ref 1). It expresses the considered judgement of the contractor or developing agency regarding the hazard potential of the item and any actions or precautions that are recommended to minimize these hazards and to reduce the exposure of personnel and equipment to them.

## II. RESPONSIBILITIES:

a. Materiel Commanders: AR 385-16 (ref 2) requires that an SAR will be provided to the combat developer and the operational tester, development test agency, and other testing agencies at least 60 days before the start of their respective tests.

b. Heads of operational test (OT) and development test (DT) and evaluation agencies, activities and commands:

1. Use the SAR information to integrate safety into test planning and procedures and for shipping and handling of the system.

2. Ensure that developmental testing will not begin until an SAR has been received, reviewed, and accepted by the test agency.

## III. SAFETY ASSESSMENT REPORT FOR FORMAT GUIDE:

The SAR is a formal summary of the safety data, collected during the design and development of the system, which provides a comprehensive evaluation of safety risks being assumed prior to test or operation of a system or at contract completion. In it, the contractor or material developer summarizes the hazard potential of the item, provides a risk assessment and recommends procedures or other corrective actions to reduce these hazards to an acceptable level.

### 1. INTRODUCTION:

STATE THE PURPOSE OF THE SAFETY ASSESSMENT REPORT.

The purpose of the SAR is to provide a comprehensive evaluation of the safety risks being assumed prior to test or operation of the system or at contract completion. It should identify all safety features of the hardware and system design and procedural hazards that may be present in the system being acquired. It should include, specific procedural controls and precautions that should be followed.

2. SYSTEM DESCRIPTION. Develop by reference other program specifications such as technical manuals, system safety program plans, specifications, etc., as applicable and:

a. State purpose and intended use of item.

The description of the system should begin with its intended use and the mission that it is required to accomplish.

b. Give background information on development of item.

Provide an historical summary of the system's development.

c. Describe the item fully.

Include name, type, model number, presence of any radioactive source, general physical features including size. weight, payload, and specific operational features. Describe major subsystems and components.

d. Describe fully and system that will be tested along with the item.

For example, a weapons system may need to be tested while mounted on a specific vehicle. While the vehicle may already be a fielded item, its interface with the weapons system needs to be evaluated.

e. Provide photos, charts, flow diagrams, or schematics to support the system description, test or operation.

3. SYSTEM OPERATIONS:

a. Present a complete sequence of system operations and emphasize the safety features.

A system is designed, manufactured, and maintained to accomplish a specific mission. It has certain characteristics and limitations within which it will function properly. Procedures which should be followed in sequence for safe operation should be spelled out so that important steps are not by-passed. Hazardous operations should be conducted only in designated areas. Only essential personnel should be permitted within the hazard area during a specific operation. Personnel and organizations should be notified before the operation is begun. Escape routes should be clearly designated.

b. List and describe fully any special procedures needed to assure safe operations, including emergency procedures.

For example, misfire/hangfire/cook-off procedures or warnings should be emphasized for all weapons, as well as load/stow/reload procedures for the smoke grenade and associated launchers.

c. Describe operating environments and specific skills for safe operation, maintenance, or disposal.

d. Describe special facility requirements or personal equipment to support/operate the system.

For example, fire suppression system, climate control, ventilation, ear or eye protection, gloves, clothing, etc.

4. SAFETY ENGINEERING:

a. Include all system safety data and include contractor safety data developed during design and development phases.

The system safety engineering process may begin with known previous experience and knowledge. The lessons learned from previous system developments should be made available for the hazard analysis. Other data available from common resource banks such as government defense and industry should be considered. Accident and incident data should be surveyed for common types of safety hazards.

As long as hazards exist, there is the possibility, no matter how improbable, that an accident will occur. Accidents are possible when the system or its components are being tested during development. However, tests are usually carried out by highly trained personnel who are alert to the possibility that failures at that stage are likely. But when the system becomes operational, the operational personnel may be less skilled, knowledgeable, or capable of meeting emergencies. Designers must therefore assume that in the hands of the ultimate user, the probability of accidents is greater.

b. Show analyses and tests performed to point out hazardous conditions in the item.

Hazard analyses are the heart of the system safety evaluation. The types of analyses that were performed must be stated in this section and the purpose must be clearly defined. Since there are many types of hazard analyses, a specific attempt to understand the system and the need to perform unique types of analyses should be made.

An explanation and instructions on the development of hazard analyses are included in Appendix C of this report. They include preliminary hazard analysis (PHA), subsystem hazard analysis (SSHA), and fault tree analysis (FTA).

(1) Show hazard severity and the effect of hazards on system operation and mission.

Hazard severity and probability of occurrence should be categorized in accordance with procedures in paragraphs 4.5.1 and 4.5.2 of MIL-STD-882B. A reproduction of these tables are included in Appendix C of this report.

(2) Explain system interfaces and associated safety implications.

The human/machine/hazards need to be examined and all of the system's interfaces should be pointed out. Understanding the need for a complete evaluation of hazards to assure that controls are considered in the PHA, is vital. System definition will initialy result in a suitable general design. It is understood that all hazards may not be recognized at this time. However, this analysis should be continuously upgraded as the development phase progresses. Catastrophic hazards should be considered as a source of fault tree analysis so that the events leading to the undesired event can be traced.

(3) Show the results of hazard analysis validation tests.

The method by which safety controls are brought into existence must be stated in a clear, positive policy. It will be necessary to verify that the particular design meets the safety requirements specified. A safety test matrix which identifies the particular areas that were tested, along with the results and actions to abate the hazards should be present.

c. Include surface danger zone data and other range safety data for weapons or explosive items and sources of nonionizing/ionizing radiation.

This section encompasses a wide variety of possible safety hazards which may or may not be an integral part of the system. If the system relates to any of the above, the information must be included. The following data needs to be considered:

(1) General range control precautions, instructions, and danger zones necessary in the firing and other use of ammunition and explosives in all types of test operations utilizing water, airspace, and assigned land areas.

(2) Lasers are an example of nonionizing radiation. Three aspects of laser application which influence the total hazard evaluation are the laser system capability of injuring personnel, the environment in which the laser is used, and the personnel who operate the laser and the personnel who may be exposed.

(3) Any ionizing radiation hazards that may be present within the system or as the result of operating or maintaining the system, must be identified. Methods of safe guards need to be communicated.

d. When the developer states that the test presents no hazard, include the basis for this decision and supporting evidence.

In most cases some form of hazard analysis should be performed before determining that no hazards exist. It is not enough to compare the system in question to some other system that was previously fielded. Copies of all analyses and test reports should be included as evidence.

e. Health hazards (per AMC Suppl 1 to AR 385-16)

(1) Address any known or potential health hazards to test participants as a result of the design or use of the system.

(2) Include results (attach if available) of mandatory health hazards studies made by medical agencies (AR 40-10). Also include results of medical research or consultations made to clarify the nature and degree of the hazard to user personnel.

Examples would include tests for toxic gas concentrations, noise levels (including impulse as well as steady state), and radiation measurements.

c. Indicate whether the restrictions for human use volunteers (AR 70-35) apply.

5. CONCLUSIONS AND RECOMMENDATIONS:

a. State whether the system is completely safe for testing or whether it is safe for testing with exceptions.

It should be remembered that test personnel, both during development testing and operational testing, must operate, fire, evaluate, etc., the materiel to be tested and it is necessary for their safety and the safety of military personnel who will later use the systems, that they understand all of the peculiarities of the system. It is in this section that all known or suspected hazards need to be summarized along with safe guards needed to protect users against serious injury or loss of the system.

b. List exceptions for all real and potential hazards that may be encountered. Make specific safety recommendations to ensure the safety of personnel and preservation of materiel and property.

(1) Related hazards should be classed as expected to occur under normal or abnormal operating conditions.

(2) Explosive, electrical, mechanical, health, radiological, and composite hazards should be covered.

c. Highlight any known safety or health problems that will require further investigation during testing.

6. REFERENCES:

List references such as test reports, preliminary operating manuals, maintenance manuals, and health hazard studies.

7. SIGNATURE BLOCKS:

The SAR should be signed as stated below:

Prepared by:________________________________Date______________________

Concurred by:_______________________________Date______________________

Approved by:________________________________Date______________________

IV APPENDIX

## APPENDIX A - REFERENCES

1. DA Pamphlet 385-16 (draft), System Safety Management Guide, 1 January 1986.

2. AR 385-16, System Safety Engineering and Management, 3 September 1985.

3. MIL-STD-882B, System Safety Program Requirements, 30 March 1984.

## APPENDIX B - SAFETY ASSESSMENT REPORT (D1-SAFT-80102)

1. Introduction.

a. State purpose of the safety assessment report.

b. Give short summary.

c. Provide an operational scenario description and analysis of hazards peculiar to the operational environment.

2. System description.

a. State purpose and intended use of item.

b. Give background information on development of item.

c. Describe the item fully. include name, type, model number, presence of any radioactive source, general physical features, and specifice operational features.

d. Describe fully any system that will be tested along with the item.

3. System operations.

a. Present a complete sequence of system operations. Emphasize the safety features.

b. Lest and describe fully and special procedures needed to assure safe operations.

4. Safety engineering.

a. Include all system safety data and include contractor safety data developed during design and development phases.

b. Show analyses and tests performed to point out hazardous conditions in the item.

(1) Show hazard severity and probability of occurrence (MIL STD 882), if applicable, and the effect of hazards on system operation and mission.

(2) Explain system interface and associated safety implications.

(3) Show results of hazard analysis validation tests.

c. Include surface danger zone data and other range safety data for weapons or explosive items and sources of nonionizing/ionizing radiation.

d. When the developer states that the test presents no hazard, include the basis for this decision and the supporting evidence.

e. Address any known or potential health hazards to test participants as a result of the design or use of the system. Attach OTSG Health Hazard Assessment (AR 40-10).

5. Conclusions and recommendations.

a. State whether the system is completely safe for testing or whether it is safe for testing with exceptions.

b. List exceptions for all real and potential hazards that may be encountered. Make specific safety recommendations to insure the safety of personnel and preservation of materiel and property.

(1) Related hazards should be classed as expected to occur under normal or abnormal operating conditions.

(2) Explosive, electrical, mechanical, health, radiological, and composite-type hazards should also be covered.

c. Highlight any known safety or health problems that will require further investigation during testing.

6. References. List references such as test reports, preliminary operating manuals, maintenance manuals, and health hazard studies.

Prepared by:____________________ Date____________________

Concurred in by:____________________ Date____________________

Approved by:____________________ Date____________________

## APPENDIX C - SYSTEM SAFETY ANALYSIS

Starting in basic research (6.1) the developer and contractor should perform various factory, laboratory, and proving ground tests of parts, components, and subsystems, using "breadboard" or "brassboard" configuration.

From the begining, the system shall be designed, in a timely and cost effective manner, to eliminate all potential and actual safety and health hazards. These hazards shall be identified and evaluated in accordance with hazards evaluation techniques as spelled out in MIL-STD-882B. These techniques shall include, but not be limited to the following:

## Preliminary Hazard Analysis (PHA)

A Preliminary Hazard Analysis is an inductive process which should be conducted early in the design phase of the system life cycle to identify in broad or gross terms the potential hazards associated with the postulated operational concept. The analysis is a comprehensive, qualitative, evaluation of the system which considers the system from the viewpoint of its operational environment. As potentially hazardous operations, materials, and design are identified, this information should be used in the development of safety criteria to be imposed in the performance/design specifications. The Preliminary Hazard Analysis, therefore, becomes a necessary system safety program element to provide assurance that the system safety requirements become an integral part of the overall technical design requirements.

The Preliminary Hazard Analysis should include, but not be limited to, the following activities:

- A review of pertinent historical safety experience data.
- A categorized listing of basic hazard sources including an identification of possible causes in each category.
- An investigation of the various sources to determine the provisions which have been developed for their control.
- Identification of hazards sources for which inadequate control has been provided in the proposed design/procedures.
- The provision of specific safety requirements/criteria which should be incorporated into the program documentation to assure control of the sources which present unacceptable hazard levels.

The following activities, areas, conditions should be considered when performing the PHA:

1) Hazardous components
    - Hazardous materials
    - Energy sources
    - Fluids and oils
    - Off-property sources
    - Pressure systems

2) Safety related interface considerations among various elements
    - EMI
    - Inadvertent activation
    - Fire/explosive initiation and propagation

3) Environmental constraints

- Temperature extremes
- Shock
- Noise and health hazards
- X-Rays

4) Construction constraints

In addition to many of the environmental constraints are

- Transportation
- Installation
- Utilities
- OSHA
- Laser radiation

5) Operating, test and maintenance procedures

- Layout and lighting
- Crash safety
- Egress and rescue

6) Facilities, support equipment and training

- Codes and standards
- Certification
- Storage, assembly and checkout

7) Safety related equipment, safeguards

- Interlocks
- Redundancy
- Fail safe design
- Fire suppression systems
- Personnel protective equipment

## PRELIMINARY HAZARD ANALYSIS (PHA) - ________

### Instructions for Completing

In Contract No. ________, enter the contract number for which PHA is being performed.

In Contractor ________________, enter the name of the Contractor responsible for the PHA.

In PHA No. ________, enter the PHA Number which shall be coded and sequentially numbered by each Contractor for each system. This coding sequence will be utilized for all related analysis.

In Revision No. ________, enter the revision number to indicate the latest status.

In Subsystem ________________, enter the nomenclature of the subsystem as broken out from the system.

In System ________________, enter the nomenclature of the applicable system.

In Drawing No. ________, enter the drawing number of the drawing on which the subsystem is indicated.

In Prepared by ______________ Date ________, the preparer will sign and enter the date of issue or completion on each sheet of the analysis.

In Reviewed by ______________ Date ________, the reviewer will sign and enter the date of review on each sheet of the analysis.

In Approved by ______________ Date ________, the Contractor's Project Manager will sign to approve and enter the date of approval on each sheet of analysis.

In (1) Function Description & No., enter the reference number and a brief functional description of the subsystem under analysis.

In (2) System Mode, enter the state of the system, at the time of the failure mode or condition.

In (3) Hazard Description, enter the nature of hazard condition introduced by the failure of the subsystem.

In (4) Potential Cause, enter the most likely primary and secondary causes of the hazard condition.

In (5) Effect on Subsystem/Interfacing Subsystems, enter a brief description of the hazard condition effect(s) on the subsystem and other interfacing subsystems.

## PRELIMINARY HAZARD ANALYSIS (PHA) (cont'd)

Instructions for Completing

In (6) Hazard Category, enter the highest applicable hazard class in accordance with MIL-STD-882B.

In (7) Redesign/Control Remarks, enter a brief description of the redesign/control/corrective action(s) necessary for the hazard condition being analyzed. Enter name(s) of related analysis and reference number(s) and which approach is being proposed - Design Change, Procedures, Special Training, etc.

# PRELIMINARY HAZARD ANALYSIS (PHA)

NO. ______ REV. NO. ______

SHEET NO. ______ OF ______

CONTRACT NO. ____________ CONTRACTOR ____________

SUBSYSTEM ____________

SYSTEM ____________

DRAWING NO. ____________

PREPARED BY ____________ DATE ____________

REVIEWED BY ____________ DATE ____________

APPROVED BY ____________ DATE ____________

| GENERAL DESCRIPTON | | | HAZARD CAUSE EFFECT | | | CORRECTIVE ACTION |
|---|---|---|---|---|---|---|
| (1) FUNCTION DESCRIPTION & NO. | (2) SYSTEM MODE | (3) HAZARD DESCRIPTION | (4) POTENTIAL CAUSE | (5) EFFECT ON SUBSYSTEM / INTERFACING SUBSYSTEM | (6) HAZ. CAT. | (7) REDESIGN/CONTROL REMARKS |
| | | | | | | |

## SYSTEM HAZARD ANALYSIS (SHA)

Instructions for completing

In Contract No. ________, enter the contract number for which SHA is being performed.

In Contractor ____________, enter the name of the Contractor responsible for the SHA.

In SHA No. __________, enter the SHA number which shall be coded and sequentially numbered by each Contractor for each system. This coding sequence will be utilized for all related predictions and analysis.

In Revision No. ________, enter the revision number to indicate the latest status.

In System ____________, enter the nomenclature of the applicable system.

In Drawing No. _________, enter the drawing number of the drawing on which the subfunction is indicated.

In Interfacing System ____________, enter the nomenclature of the applicable interfacing system.

In Prepared by ______________ Date ______, the preparer will sign and enter the date of issue or completion on each sheet of the analysis.

In Reviewed by ________ Date ________, the reviewer will sign and enter the date of issue or completion on each sheet of the analysis.

In Approved by _____________ Date ______, the Contractor's Project Manager will sign to approve and enter the date of approval on each sheet of analysis.

In (1) Hazard Description, enter the nature of hazard condition introduced by the failure of the system.

In (2) System Mode, enter the state of the system, instance before the failure mode or condition.

In (3) Potential Cause, enter the most likely primary and secondary causes of the hazard condition.

In (4) Effect(s) on System, enter a brief description of the hazard condition effect(s) on the system.

In (5) Effect(s) on Interfacing System(s), enter a brief description of the hazard condition effect(s) on the interfacing system(s).

## SYSTEM HAZARD ANALYSIS (SHA) (cont'd)

Instructions for completing

In (6) Interfacing Parameters, enter the parameters responsible for the interfaction of the system with other systems.

In (7) Hazard Category, enter the highest applicable hazard class in accordance with MIL-STD-882B.

In (8) Redesign/Control Actions, enter a brief description of the redesign/control/corrective action(s) necessary for the hazard condition being analyzed. Enter name(s) of related analysis and reference number(s).

SHA NO. ______ REV. NO ______

SHEET NO. ______ OF ______

# SYSTEM HAZARD ANALYSIS (SHA)

CONTRACT NO. ______ CONTRACTOR ______

SYSTEM ______ INTERFACING SYS. ______ INTERFACING SYS. ______ PREPARED BY: ______ DATE ______

DRAWING NO. ______ DRAWING NO. ______ DRAWING NO. ______ REVIEWED BY ______ DATE ______

APPROVED BY ______ DATE ______

| GENERAL DESCRIPTION | | HAZARD CAUSE / EFFECT | | | | | CORRECTIVE ACTION |
|---|---|---|---|---|---|---|---|
| (1) HAZARD DESCRIPTION | (2) SYSTEM MODE | (3) POTENTIAL CAUSE | (4) EFFECT(S) ON SYSTEM | (5) EFFECT(S) ON INTERFACING SYSTEM(S) | (6) INTERFACING PARAMETERS | (7) HAZ. CAT. | (8) REDESIGN/CONTROL ACTIONS |
| | | | | | | | |

Operating & Support Hazard Analysis [(O & S) HA]

The purpose of the (O & S) HA is to identify and analyze hazards associated with personnel and procedures during production, testing, installation, training, escape and operations.

The (O & S) HA is normally conducted on all identified hazards involved with tasks with man/machine interfaces. When the (O & S) HA indicates a potential problem, it should be make known to the responsible engineer in order to initiate a design review or a system safety working group action item. The (O & S) HA should be reviewed on a continuous basis to ensure that design modifications, procedures, testing, etc., do not create hazardous conditions.

The (O & S) HA helps ensure that corrective or preventive measures will be taken to minimize the possibility that any human error procedure will result in injury or system damage. The (O & S) HA provides inputs for recommendations for changes or improvements in design or procedures to improve efficiency and safety, development of warning and caution notes to be included in manuals and procedures, and the requirement of special training of personnel who carry out the operation and maintenance of the system.

A well-documented analysis shows compliance with the specified system safety and operational requirements.

Subsystem Hazard Analysis (SSHA)

The SSHA is an inductive process which, in effect, is an expansion of, with increased complexity over, the Preliminary Hazard Analysis. The completion of this analysis will normally occur during the design phase and prior to the design freeze (in a system development, prior to CDR). This occurs when the actual system design has been refined to the point where the detailed information is available. However, it can be used effectively during operations as part of an investigation to establish cause and effect relationships and probabilities.

There are several types of SSHA's:

- Fault Hazard Analysis (FHA)
- Sneak Circuit Analysis
- Fault Tree Analysis (FTA)

However, only the FHA and FTA are discussed herein.

An SSHA/FHA is conducted on identified failure modes, and will be qualitative to a quantitative analysis as the design develops. When the analysis indicates a potential problem, it should be made known to the responsible Engineer in order to initiate proper action. An FHA should be reviewed on a continuous basis to ensure that design modifications do not add hazards to the system. The FHA should be developed in conjunction with the FMECA

It provides information to evaluate identified hazards, identify safety critical areas and provide inputs to safety design criteria and procedures with provisions and alternatives to eliminate or control all category I and II hazards, to minimize or control category III and IV hazards, and to identify critical items.

## FAULT HAZARD ANALYSIS (FHA)

### Instructions for Completing

In Contract No. __________, enter the contract number for which FHA is being performed.

In Contractor ______________, enter the name of the Contractor responsible for the FHA.

In FHA No. __________, enter the FHA number which shall be coded and sequentially numbered by each Contractor for each system. This coding sequence will be utilized for all related predictions and analysis.

In Revision No. __________, enter the revision number to indicate the latest status.

In Subsystem ______________, enter the nomenclature of the subsystem as broken out from the system and which includes the item undergoing FHA.

In System ______________, enter the nomenclature of the applicable system.

In Drawing No. __________, enter the drawing number of the drawing on which the LRU is indicated.

In Prepared by ______________, Date __________, the preparer will sign and enter the date of issue or completion on each sheet of the analysis.

In Reviewed by ______________, Date __________, the reviewer will sign and enter the date of review on each sheet of the analysis.

In Approved by ______________, Date __________, the Contractor's Project Manager will sign to approve and enter the date of approval in each sheet of analysis.

In (1) LRU No & Description, enter the reference number nomenclature and brief functional description of the component/assembly.

In (2) Failure Mode, enter a brief description of the failure or condition that is being analyzed.

In (3) Failure Rate, enter the probability of occurrence of failure mode or condition. Give data source, such as experience, GIDEP, MIL HBK 217.

In (4) System Mode, enter the state of the system when the failure mode or condition occurs.

In (5) Cause, enter the most likely primary and secondary causes of the failure mode or condition.

## OPERATING & SUPPORT HAZARD ANALYSIS [(O & S) HA]

Instructions for Completing Form 004:

In Contract No. _______, enter the contract number for which (O & S) HA is being performed.

In Contractor ____________, enter the name of the Contractor responsible for the (O & S) HA.

In (O & S) HA No. ________, enter the (O & S) HA number which shall be coded and sequentially numbered by each Contractor for each system. This coding sequence will be utilized for all related analyses.

In Revision No. ______, enter the revision number to indicate the latest status.

In Subsystem Function ___________, enter the nomenclature and function of the subsystem as broken out from the system.

In System __________, enter the nomenclature of the applicable system.

In Facility __________, enter the description of the facility which includes the system.

In Drawing No. _______, enter the drawing number of the drawing on which the subfunction is indicated.

In Prepared by ___________, Date ________, the preparer will sign and enter the date of review on each sheet of the analysis.

In Reviewed by ___________, Date ________, the reviewer will sign and enter the date of review on each sheet of the analysis.

In Approved by ___________, Date _______, the Contractor's Project Manager will sign to approve and enter the date of approval on each sheet of analysis.

In (1) Task or Operation, enter a brief description of the task or operation for which the hazard condition is being analyzed.

In (2) Potential Cause, enter the most likely primary and secondary causes of the hazard condition.

In (3) Effect(s) on Personnel System, enter a brief description of the hazard condition effect(s) related to personnel and/or system(s).

## Instructions for Completing

In (5) Hazard Category, enter the highest applicable hazard class in accordance with MIL STD 882B.

In (6) Redesign/Control Actions, enter a brief description of the redesign/control/corrective action(s) necessary for the hazard condition being analyzed. Enter name(s) of related analysis and reference number(s).

## SUPPORT ACTIVITIES

### General

Throughout a system's life cycle there must be a continuing flow of information between disciplines. This is especially true for the safety and assurance disciplines. "Next to design inadequacies and deficiencies, the principal causes of equipment and system failure and accidents are errors made during manufacturing and maintenance".

Much of the analytic work is complementary, and data developed for reliability purposes can be used in safety analyses. There is a continuous interplay that must be recognized during the analytic and investigatory processes.

Some of these analyses are:

1) Failure Modes and Effects Analysis (FMEA)

2) Failure Modes, Effects and Criticality Analysis (FMECA)

3) Maintenance Engineering Analysis (MEA)

4) Predicted Mean Time to Repair

The FMECA and the PMTTR are discussed herein.

In addition it is essential that the system safety engineer be able to track category I & II hazards and the verification of the eventual "fix", whether it be a

- Design/hardware change,
- Procedural change, or
- Training requirement.

The critical Items List (CIL) enables the engineer to do this.

## Critical Items List (CIL)

The purpose of the CIL is to compile all the identified safety-critical items to provide visibility for immediate corrective action to prevent personal injury or system damage when a category I or II hazard is identified. The CIL also provides a control technique for reliability when a category 1 and 2 criticality item is identified. The CIL should be reviewed on a continuous basis until all items are resolved.

The CIL helps ensure that corrective action or preventive measures are taken to optimize system safety, reliability and maintainability by minimizing the magnitude and seriousness of those items which could result in personal injury, system damage and loss of operation, but which cannot be completely eliminated. The CIL provides inputs for recommendations for: changes or improvements in design; procedures to improve efficiency and safety; development of warning and caution notes to be included in manuals and procedures; requirements for special training, and; management information for the operation and maintenance of the system. Those corrected CIL items should be incorporated into test program to verify effectiveness of corrective measure(s).

Complete documentation shows compliance with the specified system safety and operational requirements.

## CRITICAL ITEMS LIST - ________

### Instructions for Completing

In Contract No. ________, enter the contract number for which CIL is being prepared.

In Contractor ______________, enter the name of the Contractor responsible for the CIL.

In CIL No. _________, enter the CIL number which shall be coded and sequentially numbered by each Contractor. This coding sequence will be utilized for all related predictions and analysis.

In Revision No. _______, enter the revision number to indicate the latest status.

In Prepared by ______________ Date _______, the preparer will sign and enter the date of issue of completion on each sheet.

In Reviewed by ______________ Date ________, the reviewer will sign and enter the date of review on each sheet.

In Approved by _____________ Date ________, the Contractor's Project Manager will sign to approve and enter the date of approval on each sheet.

In (1) LRU Description, enter nomenclature and brief functional description of the lowest replaceable unit.

In (2) Failure Reference Analysis, enter the applicable analysis name and number performed.

In (3) Failure Criteria Category, enter the highest applicable criticality category in accordance with the description in the Glossary of Terms.

In (4) Hazard Reference Analysis, enter the applicable hazard analysis name and number performed.

In (5) Hazard Category, enter the highest applicable hazard class in accordance with MIL-STD-882B and the description of the corrective action(s) or procedures which can be adopted to eliminate or minimize the effects or failure condition being analyzed.

In (6) Requirement, enter the specified safety and/or reliability guidelines.

In (7) Corrective Action, enter a brief description of the corrective actions necessary for the hazard condition analyzed.

## CRITICAL ITEMS LIST - ______ (cont'd)

Instructions for Completing

In (8) Resolution, enter a brief description of final action taken to eliminate or control the hazard(s).

In (9) Retention Rationale, state the reasons for retaining the category I and II hazards as critical items 1 & 2.

## CRITICAL ITEM LIST (CIL)
### HAZARD CATEGORY I AND II ITEMS
### CRITICALITY CATEGORY 1 AND 2 ITEMS

CIL NO. ______ REV. NO. ______

SHEET NO. ______ OF ______

CONTRACT NO. ______________ CONTRACTOR ______________

PREPARED BY ______________ DATE ______________

REVIEWED BY ______________ DATE ______________

APPROVED BY ______________ DATE ______________

| LRU | FAILURE | | HAZARD | | SAFETY | RELIABILITY | STATUS | |
|---|---|---|---|---|---|---|---|---|
| (1) DESCRIPTION | (2) REF. ANALYSIS | (3) CRIT CAT. | (4) REF ANALYSIS | (5) HAZ. CAT. | (6) REQUIREMENT | (7) CORRECTIVE ACTION | (8) RESOLUTION | (9) RETENTION RATIONALE |
| | | | | | | | | |

## Failure Modes, Effects and Criticality Analysis (FMECA)

The purpose of the FMECA is to identify and analyze possible failure as early as possible during the design phases so that appropriate actions are taken to eliminate minimize or control the identified LRUs classified in criticality categories 1, 2 & 3.

The FMECA is normally conducted down to the lowest replaceable unit (LRU) of each of its systems and subsystems to determine the cause and effect of a single primary mode of failure. When the FMECA indicates a hazard the engineer should conduct a Fault Hazard Analysis (FHA). When the FMECA indicates a potential problem, it should be made known to the responsible engineer in order to initiate a design review. The FMECA should be reviewed on a continuous basis to ensure that design modifications do not add critical failure modes to the System.

FMECA helps ensure that all failure related information is traceable to an identified piece of hardware. The effects of failure are determined in a single analysis, which avoids duplication of effort for other system assurance activities. It provides inputs to the following:

1) Design Reviews

2) Maintainability Baseline

3) Reliability Baseline

4) System Safety Baseline

5) System Operation

6) Demonstration Test Plan and Procedures

7) Identify Hardware Requiring Close Control

8) Critical Hardware and Quantities to be Tested

A well-documented analysis shows compliance with specified safety, reliability and maintainability requirements.

Hazard Severity. Hazard severity categories are qualitative measure of the worst credible mishap result g ... error; environmental conditions; design inadequacies; procedural deficiencies; or system, subsystem or component failure or malfunction as follows:

| Description | Category | Mishap Definition |
|---|---|---|
| CATASTROPHIC | I | Death or system loss. |
| CRITICAL | II | Severe injury, severe occupational illness, or major system damage. |
| MARGINAL | III | Minor injury, minor occupational illness, or minor system damage. |
| NEGLIGIBLE | IV | Less than minor injury, occupational illness, or system damage. |

These hazard severity categories provide guidance to a wide variety of programs. However, adaptation to a particular program is generally required to provide a mutual understanding between the MA and the contractors as to the meaning of the terms used in the category definitions. The adaptation must define what constitutes system loss, major or minor system damage, and severe and minor injury and occupational illness.

Hazard Probability. The probability that a hazard will be created during the planned life expectancy of the system can be described in potential occurrences per unit of time, events, population, items, or activity. Assigning a quantitative hazard probability to a potential design or procedural hazard is generally not possible early in the design process. A qualitative hazard probability may be derived from research, analysis, and evaluation of historical safety data from similar systems. Supporting rationale for assigning a hazard probability shall be documented in hazard analysis reports. An example of a qualitative hazard probability ranking is:

| Description* | Level | Specific Individual Item | Fleet or Inventory** |
|---|---|---|---|
| FREQUENT | A | Likely to occur frequently | Continuously experienced |
| PROBABLE | B | Will occur several times in life of an item | Will occur frequently |
| OCCASIONAL | C | Likely to occur sometime in life of an item | Will occur several times |
| REMOTE | D | Unlikely but possible to occur in life of an item | Unlikely but can reasonably be expected to occur |
| IMPROBABLE | E | So unlikely, it can be assumed occurence may not be experienced | Unlikely to occur, but possible |

*Definitions of descriptive words may have to be modified based on quantity involved.

**The size of the fleet or inventory should be defined.

SAR EXAMPLE

APPENDIX D

SAFETY ASSESSMENT REPORT

FOR THE

XM52 SMOKE GENERATOR

MAY 1984

CONCURRED BY:

CONCURRED BY:

SUBJECT: Safety Assessment Report for XM52 Smoke Generator

## 1.0 INTRODUCTION.

1.1 Purpose. The purpose of this Safety Assessment Report is to provide the test agency with the minimum protective measures, safety features of the system and the specific safety procedural controls and precautions to be followed during development testing IAW the requirements of AR 385-16 and AMC Reg 385-12.

1.2 Summary. The XM52 Smoke Generator has been designed to include provisions for safeguarding personnel. Safety precautions have been located on the equipment where necessary and are included within the operating maintenance manual applicable to the system.

1.3 Content. The safety features included in the XM52 design are identified. These features include potential hazard controls in the form of hardware; system parameter monitors which provide input to the turbine engine's Electronic Sequencing Unit which contains the logic to shut down the XM52 in the event of out-of-tolerance conditions which may result in a hazardous condition if left unchecked; provision of DANGER and CAUTION labels on the unit to apprise operating personnel of potential hazards; establishment of proper operating procedures to minimize hazard potentials resulting from operator error; and, specification of support equipment and/or procedures to suppress or control a hazard should it develop.

## 2.0 SYSTEM DESCRIPTION.

2.1 Purpose and Intended Use.

2.1.1 Purpose. The XM52 Smoke Generator is to provide a large area smoke screen which will provide protection from both visual and IR detection devices.

2.1.2 Intended Use. The XM52 Smoke Generator has been configured for deployment on the bed of the HMMWV, a trailer towed by the HMMVW or two units mounted on the roof of a M113 APC (XM1059E1 Smoke Carrier) with the IR material and fog oil supplies mounted inside the M113.

2.2 Historical Summary of System Development.

2.2.1 A predecessor to the XM52 program was the XM49 Smoke Generator. The XM49 was to replace the current M3A3 Smoke Generator. While in Advanced Development, the XM49 project was terminated primarily because it had no potential for providing IR screening and had operational problems which showed up during development testing.

2.2.2 The current XM52 Smoke Generator program has been to develop a smoke generator which provides improvements over the M3A3, including the capability of dispensing IR defeating smoke material and the capability of being mounted on and operated from fast moving wheeled and tracked vehicles.

2.2.3 The XM52 was to be developed around a lightweight turbine engine and meet the following performance requirements:

- after starting, the XM52 shall not require tending except to replenish both smoke material and fuel.

- operate continuously for one hour without replenishment.

- produce good quality (dry) smoke from fog oil at the rate of 60 gallons per hour.

- provide IR screening protection by dispensing IR material EA5763 in a cloud at the rate of 600 lbs per hour.

- be operated from the intended mounting vehicles while on the move.

- there shall be consideration given to fire/flame suppression for tracked and wheeled vehicle application.

- fuel/smoke material spillage and unvaporized visual smoke material are unacceptable.

- torching at any time is unacceptable.

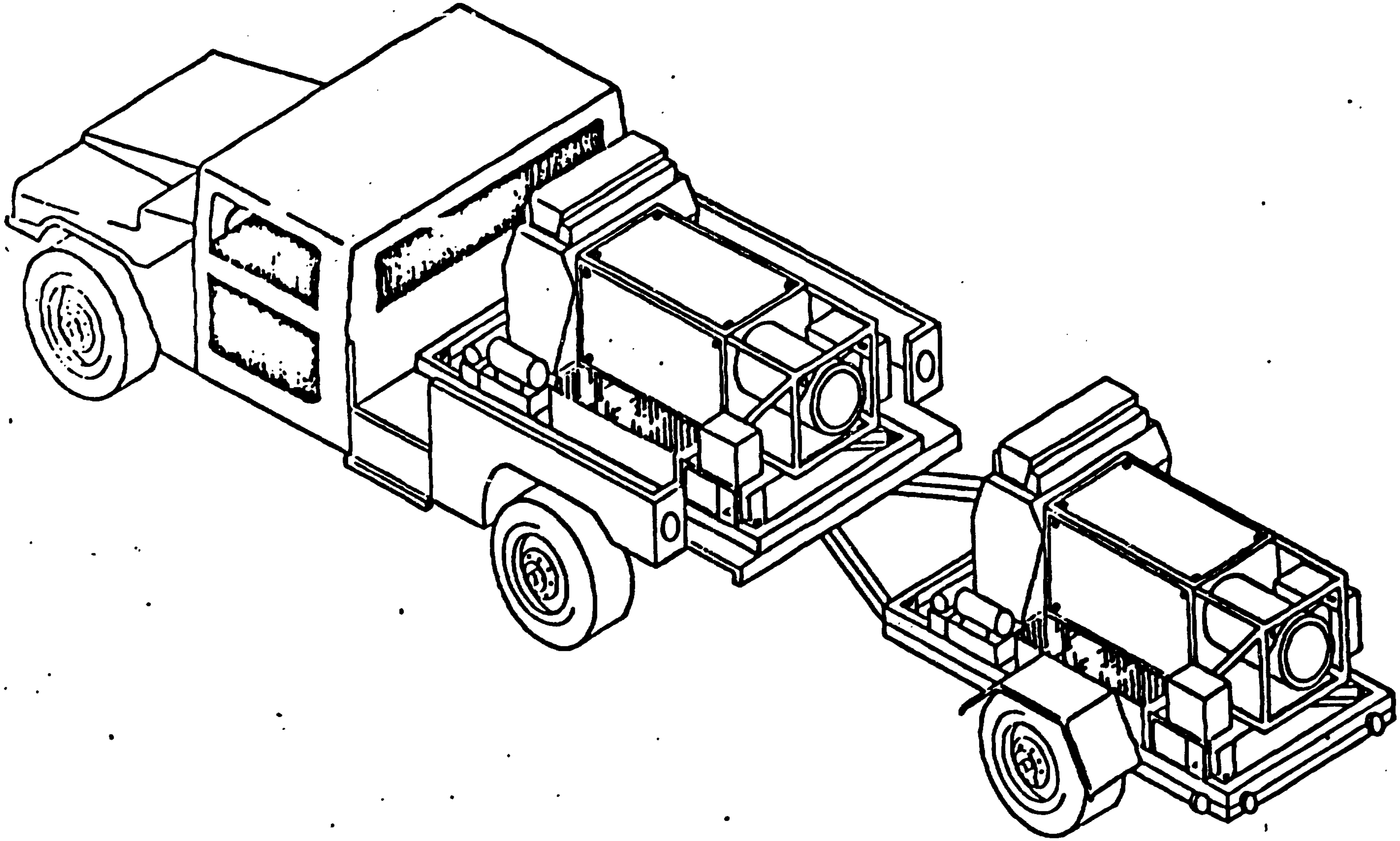
2.3 System Description.

2.3.1 Graphics. Figures 1 and 2 present the various deployment configurations and Figures 3 thru 5 are detailed illustrations of the HMMWV/trailer mountable XM52 system.

2.3.2 Subsystems. The following list presents the major subsystems and components of the XM52 Smoke Generator. While there are some differences between the XM52 for the HMMWV/trailer application and the M113 application, these differences do not affect subsystem functions, only the provisions for mounting, length of cables and fluid lines and configuration and placement of fluid tanks The list pertains to any XM52 system regardless of its application.

a. Frame structure

b. Turbine (Turbomach Titan Model T-62T-2D)



HIGH MOBILTY MULTIPURPOSE WHEEL VEHICLE, (HMMWV) AND
3/4 TON TRAILER WITH 1 XM52 SMOKE GENERATOR SYSTEM EACH

Figure - 1

## M113, APC WITH XM52 SMOKE GENERATOR SYSTEM

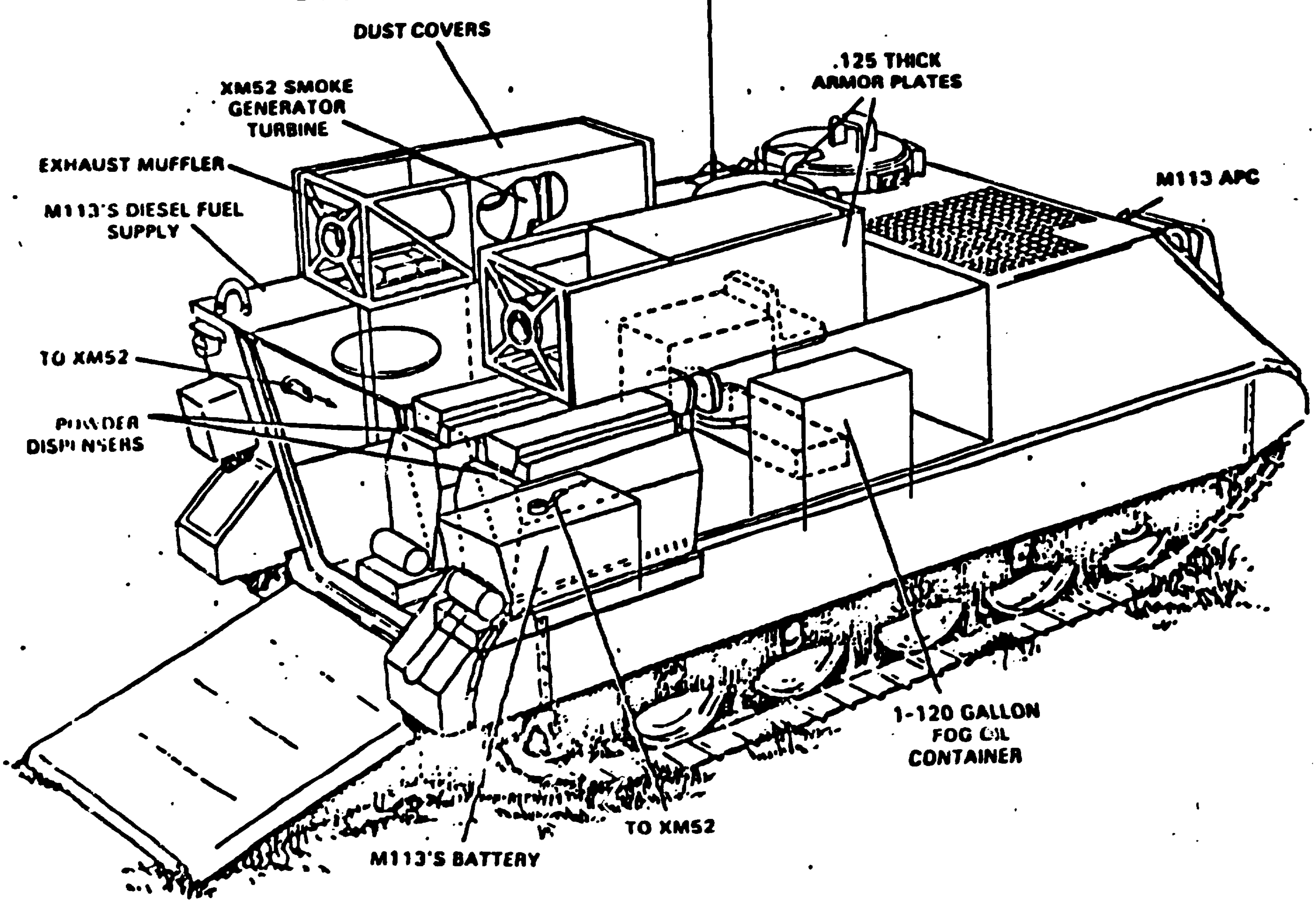
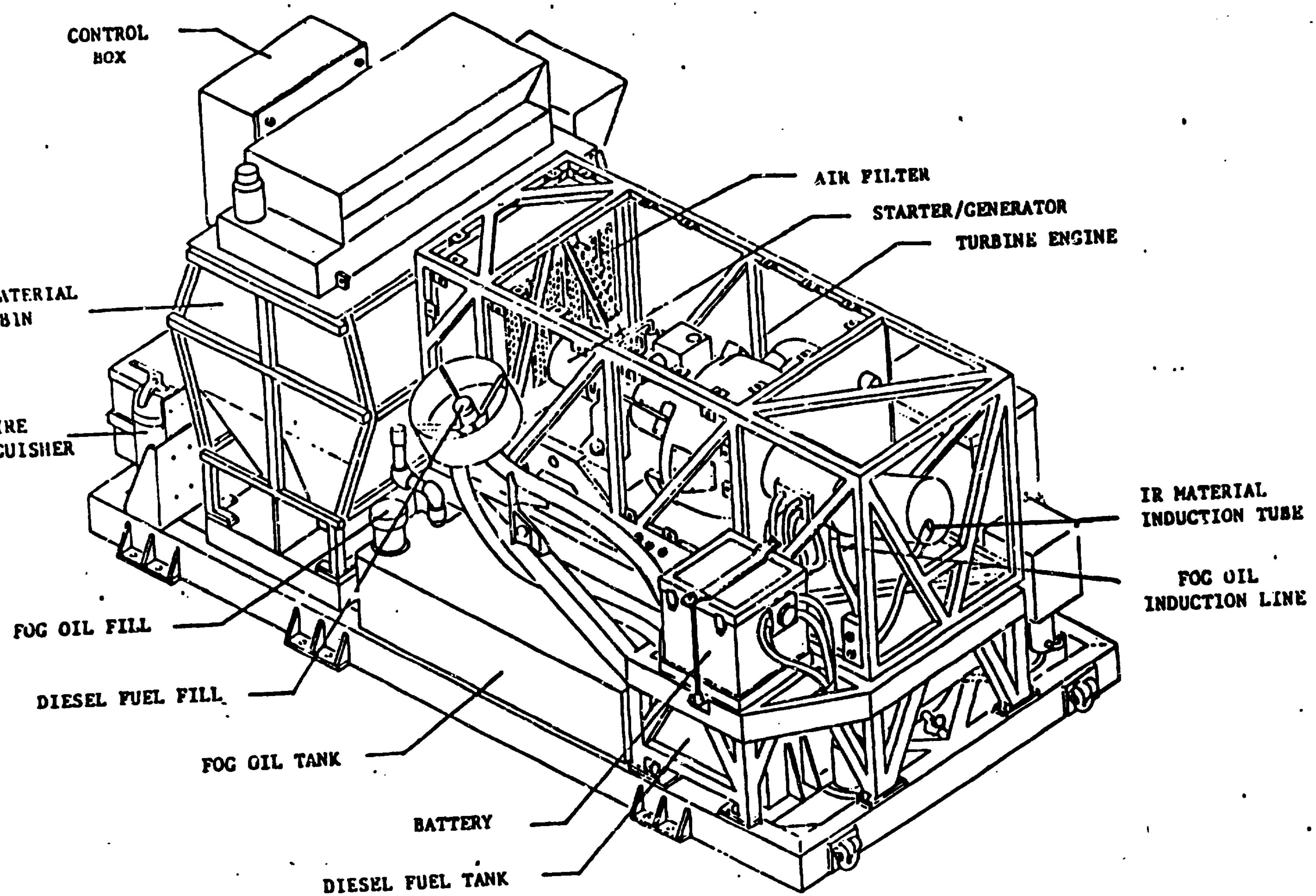
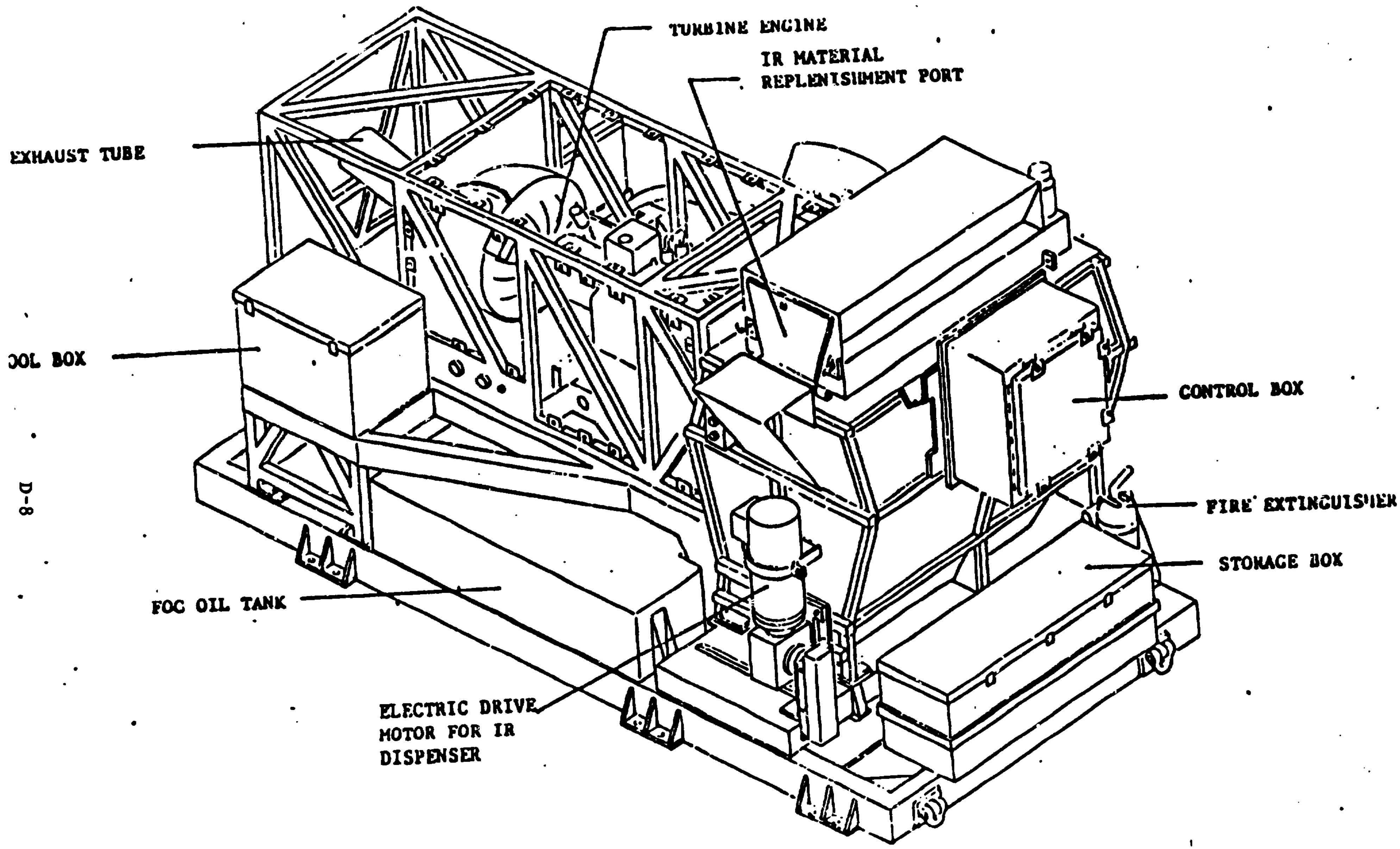


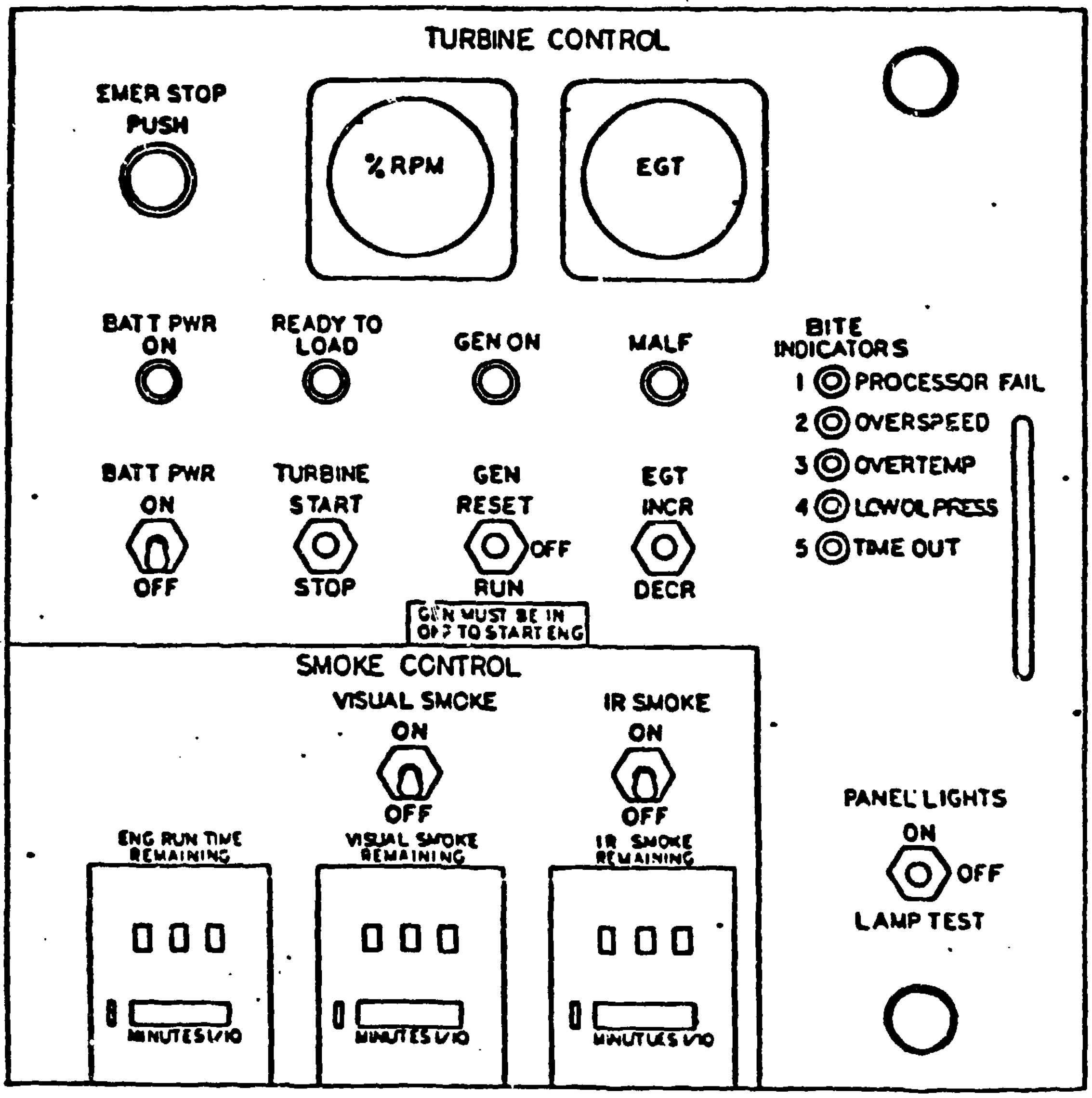

Figure 2




XM-52 DETAILED ARTIST'S CONCEPT (LEFT SIDE)
Figure 3




XM-52 DETAILED ARTIST'S CONCEPT (RIGHT SIDE)
Figure 4




XM52 SMOKE GENERATOR CONTROL PANEL
Figure 5

c. Starter/Generator

d. Air Filter System

e. Storage batteries (not on M113)

f. IR dispenser w/electric motor

g. Diesel fuel tank with electric fuel pump

h. Fog oil tank with electric fog oil pump

i. Operator's control panel

j. Electrical and fuel lines

3.0 SYSTEM OPERATIONS.

The XM52 Smoke Generator System can be operated locally in the static mode or remotely (i.e. control box inside a vehicle and connected to the unit by cable) while the vehicle is on the move.

Once the system is supplied with diesel fuel, fog oil and IR material, all operation is conducted from the control box which is located at the opposite end of the unit away from the hot exhaust tube. (See Figures 1 thru 5 to review various vehicle applications, component locations and control panel layout.)

3.1 <u>Operating Procedures</u>.

3.1.1 Turbine Starting and Smoke Generation.

3.1.2 To start the turbine engine and generate smoke, the operator must perform the following sequence of actions:

a. Verify the GEN switch is in the OFF position.

b. Set BATT PWR switch to ON position.

c. Move TURBINE switch to START position and release. This action causes the START circuit to be energized, i.e. spinning up the rotor, initiating fuel flow and initiating the ignition spark when the rotor has achieved the required RPM.

d. When the turbine reaches 100 percent RPM, the READY TO LOAD indicator illuminates. Move the GEN switch to the RESET position and release the switch.

NOTE: The RESET position has been incorporated to prevent possible damage to the turbine from premature loading. Therefore, even the GEN RESET position is not enabled until the READY TO LOAD criterion has been met and the indicator illuminates.

e. Set GEN switch to RUN position. Observe: GEN ON indicator illuminates.

f. For fog oil smoke, set VISUAL SMOKE switch to ON position.

g. For IR screening, set IR SMOKE switch to ON position.

3.1.3 Since visual smoke quality is dependent on atmospheric conditions, the operator can improve smoke quality by adjusting the exhaust temperature with EGT INCR/DECR control.

3.2 Special Operating Procedures. A number of system parameters are monitored electronically and result in a system shutdown, warning or a no start condition. They are:

Processor Failure - Shutdown*

Overspeed - Shutdown

Underspeed - Shutdown

Overtemperature Probe 1 - Shutdown

Open Probe 2 - Warning

No temp data Card 1 - Warning

Both probes open - No start

Low Oil pressure - Shutdown

Power Latch transistor failed - Shutdown

Temperature Circuit Calibration required - Warning

No temp data card 2 - Warning

Shorted Probe 1 - Shutdown

Over Temp Probe 2 - Shutdown

Open Probe 1 - Warning

Faiure to accelerate (approx 90 sec) - Shutdown

Data circuit test failure - Shutdown*

RAM test failure - Shutdown

Failure to accelerate (approx 15 sec) - Shutdown

Bleed valve not closed - No start

Shorted Probe 2 - Shutdown

Overtemperature (av) - Shutdown

Shorted or failed oil press SW - Shutdown

Flame out Deccel N 98% - Shutdown

High oil temp - Shutdown

No speed data - Shutdown

Seq. Fail - Shutdown

Both Probes shorted - Shutdown

*Internal failure, no external test possible.

These malfunctions are indicated to the operator through the BITE indicators. In the event the operator should notice a system problem which does not result in a system shutdown, the EMERGENCY STOP switch can be activated which removes all electrical power and shuts down the system. Following an EMERGENCY STOP and alleviation of the problem, all switches must be returned to their NEUTRAL or OFF position before the unit can be restarted.

3.3 Operating Environment. The XM52 Smoke Generator has been designed for operation in ambient temperature ranging from -25°F to 120°F. No procedural differences have been identified for safe operation throughout this temperature range.

3.4 Support Equipment.

3.4.1 When the XM52 Smoke Generator is operating the turbine emits high intensity noise, even though sound absorbing panels surround the turbine. Preliminary noise measurement readings taken at various locations within two feet of the unit produced the following:

a. At the control panel - 102 dBA.

b. At the diesel fuel and fog oil fill ports - 120 dBA.

c. At rear of unit near bleed air overboard duct - 132 dBA.

It is obvious from these initial readings that personnel must be required to wear hearing protection. Due to the very high noise levels at some locations (132 dBA), double hearing protection should be used when working around the generator. A CAUTION placard concerning the requirement for hearing protection has been affixed to the unit.

3.4.2 When replenishing the IR material, personnel will be required to wear a particulate filter mask and eye protection. The IR material EA5763 is a skin irritant and should be washed from the skin with soap and water should personnel become exposed.

3.4.3 While the unit has been designed to shutdown should the turbine experience overtemperature or overspeed conditions, a fire extinguisher has been mounted on the unit to be used in the extremely unlikely event of a fire. When the unit is shutdown, either manually or automatically, the volatile diesel fuel and fog oil cannot fuel a fire since the electric pumps which supply these substances are deenergized.

3.5 Safety Design Features. For the safety features contained in the system, refer to AAI Report No. ER-12871A, "Operating and Support Hazard Analysis Report" (enclosure 1) and AAI Report No. ER-12555A, "System Hazard Analysis Report (enclosure 2).

3.6 Special Procedures Needed To Assure Safe Operations.

a. Assure that ear protection is worn by all personnel conducting and witnessing tests.

b. Assure that ear plugs and ear muffs are worn by personnel within 23 feet of the system while in operation.

c. Assure that noise hazard signs are located in accordance with para 4.3 of MIL-STD-1474B(MI).

d. Monitor exposure times for all personnel for dBA(s) as required by TB MED 501. For example 122 dBA - less than 4 hrs, 126 dBA - less than 2 hrs, 130 dBA - less than 1 hr, etc.

e. Assure that fire extinguishers are available on-site and are operable/charged prior to testing.

f. Assure that all personnel conducting/witnessing tests have M9/M17 masks in slung position.

g. Personnel should wear masks when handling the IR material or when exposure to the IR smoke cloud appears likely.

h. Personnel must stay clear of the hot exhaust area at the rear of the XM52 during operation.

4.0 SYSTEM SAFETY ENGINEERING.

4.1 The methodology of MIL-STD-882A and AR 385-10 was used to identify and rank potential hazards associated with the XM52 Smoke Generator.

4.2 During the development of the XM52 Smoke Generator, a System Hazard Analysis and an Operating & Support Hazard Analysis were conducted. These analyses were based upon review of design drawings, existing documentation on the unmodified Titan Model T-62T-2A1 turbine engine (the ending model employed is a T-62T-2D which is a modification of the aforementioned engine) and observation of the initial test runs of the XM52. Hazardous conditions and their respective hazard severity levels, probability levels and control measures are identified in the following:

a. AAI Report No. ER-12871A, Operating and Support Hazard Analysis Report (enclosure 1).

b. AAI Report No. ER-12555A, System Hazard Analysis Report (enclosure 2).

5.0 HEALTH HAZARD ASSESSMENT. No Health Hazard Assessment (HHA) Report has been performed to date. Upon completion of the HHA Report, this paragraph will be updated/amended to include the report.

6.0 CONCLUSIONS AND RECOMMENDATIONS.

6.1 All known safety hazards have been evaluated throughout the design of the XM52. The system is considered to be safe to operate and test as long as the procedures stated in paragraph 3.6 are followed. For information on environmental conditions, demilitarization, disposal, etc., refer to ARCSL-EA-83005 "Programmatic Life Cycle Environmental Assessment of Smoke Obscurants, Vol. 3 of 5, dated Jul 83, and "Life Cycle Environmental Assessment, XM52 Gas Turbine Smoke Generator, dated Jan 83.

6.2 The intended obscuration function of a smoke generating device necessitates localized air pollution, therefore the appropriate environmental permits must be obtained prior to testing. The XM52 utilizes materials currently in the Army inventory, i.e. diesel fuel and fog oil. The established handling procedures for these substances apply to the XM52 Smoke Generator.

The handling procedures for handling the IR screening material EA5763 established during the XM49 Smoke Generator program also apply to the current XM52 Smoke Generator program.

7.0 REFERENCES.

7.1 MIL-STD-147B (MI).

7.2 [illegible] 1.

7.3 ARCSL-EA-83005, Vol 3, dated Jul 83.

7.4 ARCSL-TR-82065, dated Jun 83, "Life Cycle Environmental Assessment XM52 Gas Turbine Smoke Generator", dated Jan 83.

SYSTEM HAZARD ANALYSIS REPORT

FOR

XM52 LARGE AREA

SMOKE GENERATOR

REPORT NO. ER-12555A

DATE October, 1983

SUBMITTED BY

FOR

PREPARED BY

CONTRACT NO

APPROVED BY

SEQUENCE NO. A00T

W/P LOG NO.



DATA ITEM DI-H-7048

TABLE OF CONTENTS

## LIST OF FIGURES

## 1.0 INTRODUCTION

This System Hazard Analysis (SHA) Report, is submitted in accordance with the requirements of Line Item A00T of the DD1423, Contract Data Requirements List, for Contract No. DAAK 11-82-C-0126, Advanced Development of the Large Area Smoke Generator, XM52. This report meets the requirements of Data Item Description (DID) DI-H-7048, System Safety Hazard Analysis Report.

## 2.0 GENERAL

The scope of this SHA is the systematic assessment of real and potential hazards associated with the subsystems of the XM52 Smoke Generator. This SHA was conducted on the available system concept data in an attempt to identify hazards and then direct design efforts toward the elimination or control of the identified hazards.

When the XM52 is viewed as a system, with the turbine engine being a subsystem thereof, the number of subsystems are relatively few as indicated in the accompanying figures and system description.

## 3.0 SYSTEM DESCRIPTION

The XM52 Smoke Generator is used to provide a large area smoke screen which will provide protection from both visual and IR detection devices.

The XM52 Smoke Generator is being designed to provide large area obscuration capability to minimize detection by the enemy through either visual or infrared means. To accomplish this goal, the XM52 uses a slightly modified Turbomach turbine engine (Titan Model T-62T-2A1 which is to be designated as Model T-62T-2D) as a heat and power source. By introducing fog oil into the hot turbine exhaust, the unit will be able to produce good quality smoke for protection from visual detection. Also, by using turbine bleed air and an electrically drive IR dispenser system, the XM52 will be able to introduce air-entrained IR material into the exhaust stream to provide protection from detection by IR devices.

### 3.1 Major Subsystems and Components

The following list presents the major subsystems and components of the XM52 Smoke Generator. While there are some differences between the XM52 for the HMMWV/Trailer application and the M113 application, these differences do not affect subsystem functions, only the provisions for mounting, length of cables and fluid lines and configuration and placement of fluid tanks. The list pertains to any XM52 system regardless of its application.

1. Frame structure
2. Turbine, (Turbomach Titan Model T-62T-2A1 slightly modified which is to be designated as Model T-62T-2D)
3. Starter/Generator
4. Air Filter System
5. Storage batteries (not on M113)
6. IR dispenser w/electric motor
7. Diesel fuel tank with electric fuel pump
8. Fog oil tank with electric fog oil pump
9. Operator's control panel
10. Fluid lines
11. IR lines

Figures 1, 2 and 3 depict conceptually the interfaces between the major assemblies of the XM52 in both the HMMWV/Trailer and M113 applications.

## 4.0 ANALYSIS SUMMARY

The analysis results presented on the following pages address the hazard potential to the system should there be a failure in any of the subsystems. Since the Turbomach engine (Titan Model T-62T-2A1) is currently in the Army inventory, only the interfaces between the turbine and the other subsystems of the XM52 have been examined. The safety features of the turbine and its subsystem are already well documented in TM 55-2835-203-[illegible], "Organizational, DS and GS Maintenance Manual." Even so, the major safety concerns with any turbine are adequate protection from overheating and overspeeding conditions and the above turbine incorporates safety switches which shut down the turbine should either condition occur. Another concern with turbines is the potential for the turbine wheel to disintegrate from overspeed or material defect. This concern is alleviated by the turbine wheel employed which is designed to shed the vanes gradually rather than bursting catastrophically. In addition, the turbine wheel housing is designed to contain the vane fragments if the wheel fails. Also, in the XM52 application there is the added protection of the removable access panels which enclose the entire turbine.

The remaining concern with turbines is the possibility of a "hot start" or "wet start" resulting from fuel left in the combustion chamber from a previous start attempt in which ignition did not occur. The modified turbine incorporates provisions to expel the fuel from a false start out through the turbines exhaust pipe. The small amount of fuel (5-[illegible]cc) remaining from a false start presents no hazard when it is expelled to the atmosphere and ground.

Regarding electrical hazards, the XM52 uses a 28 volt power supply which is considered intrinsically safe, although injury could result from an involuntary surprise reaction if an individual comes in contact with the circuit.

## 4.1 Assignment of Risk Assessment Codes

The accompanying analysis sheets contain hazard severity levels, hazard probability levels and Risk Assessment Codes (RAC). The hazard probability levels and RAC are from AR 385-10 Interim Change No. 101. The hazard severity levels are from MIL-STD-882A so that system damage, as well as, personnel injury can be included in the definition and reflected in the hazard assessment.

HAZARD SEVERITY

a. Category I - Catastrophic. May cause death or system loss.

b. Cateogry II - Critical. May cause severe injury, severe occupational illness, or major system damage.

c. Category III - Marginal. May cause minor injury, minor occupational illness, or minor system damage.

d. Category IV - Negligible. Will not result in injury, occupational illness, or system damage.

HAZARD PROBABILITY

A - Likely to occur immediately

B - Probably will occur in time

C - Possible to occur in time

D - Unlikely to occur

RISK ASSESSMENT CODES

1 - Critical

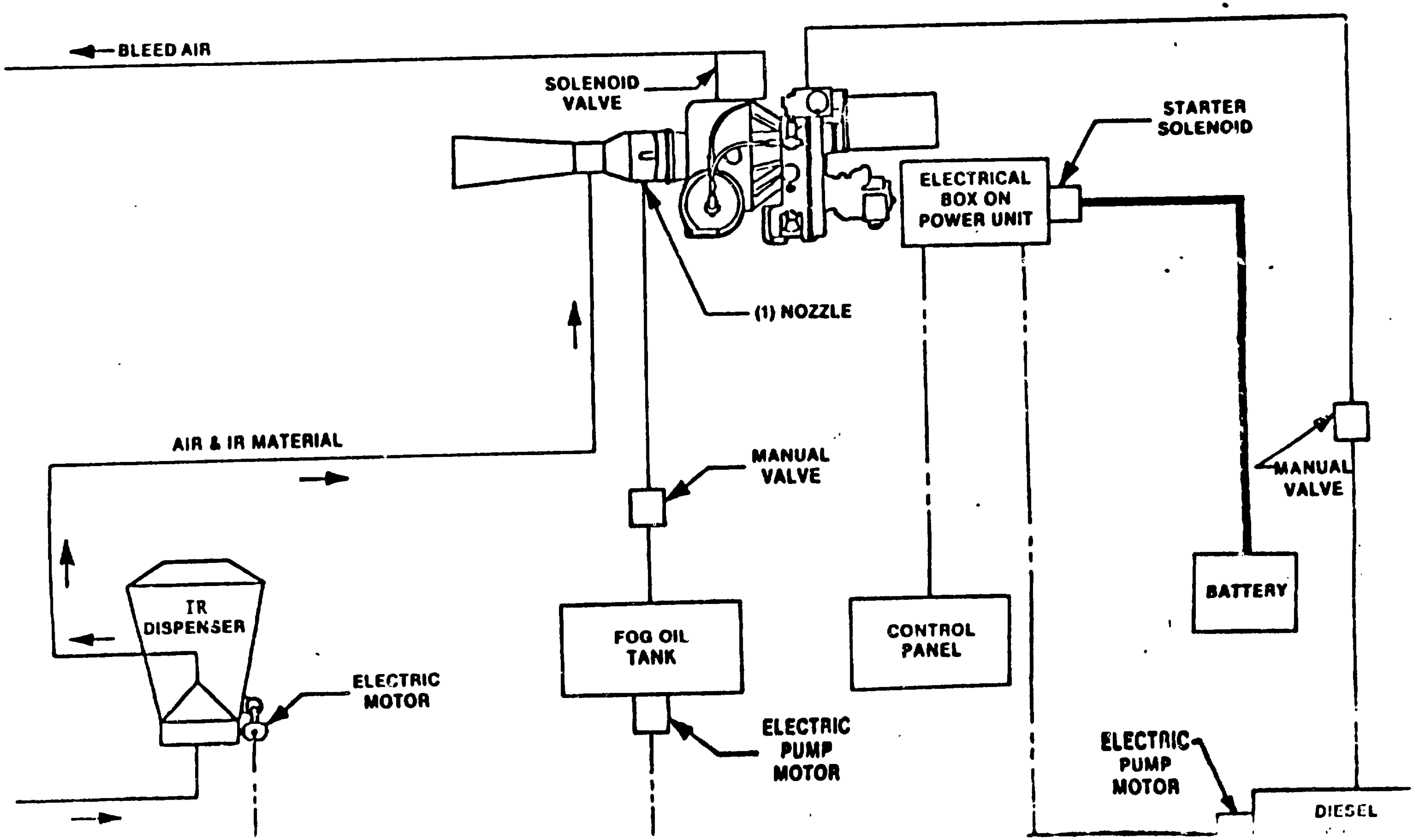
2 - Serious

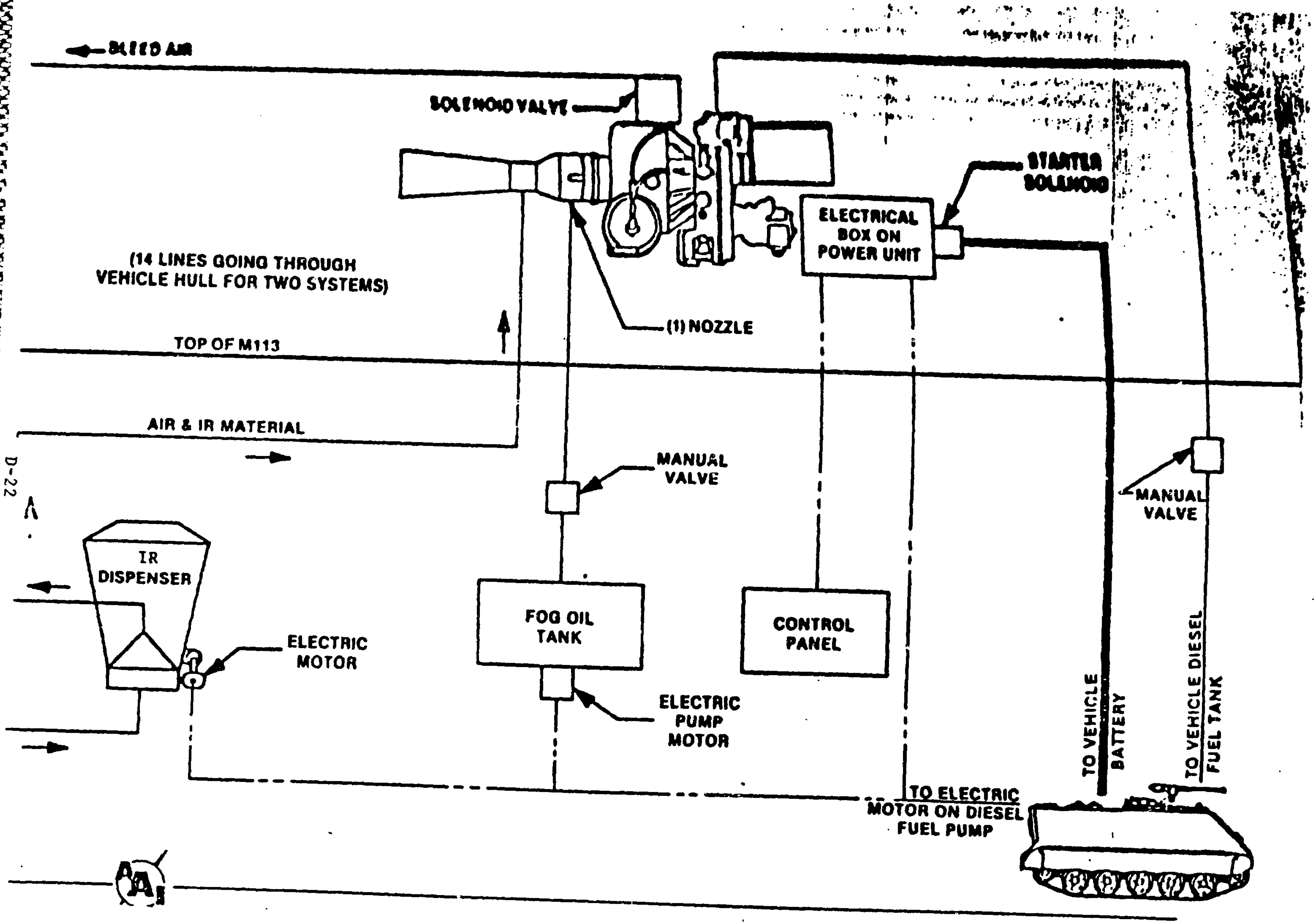
3 - Moderate

4 - Minor

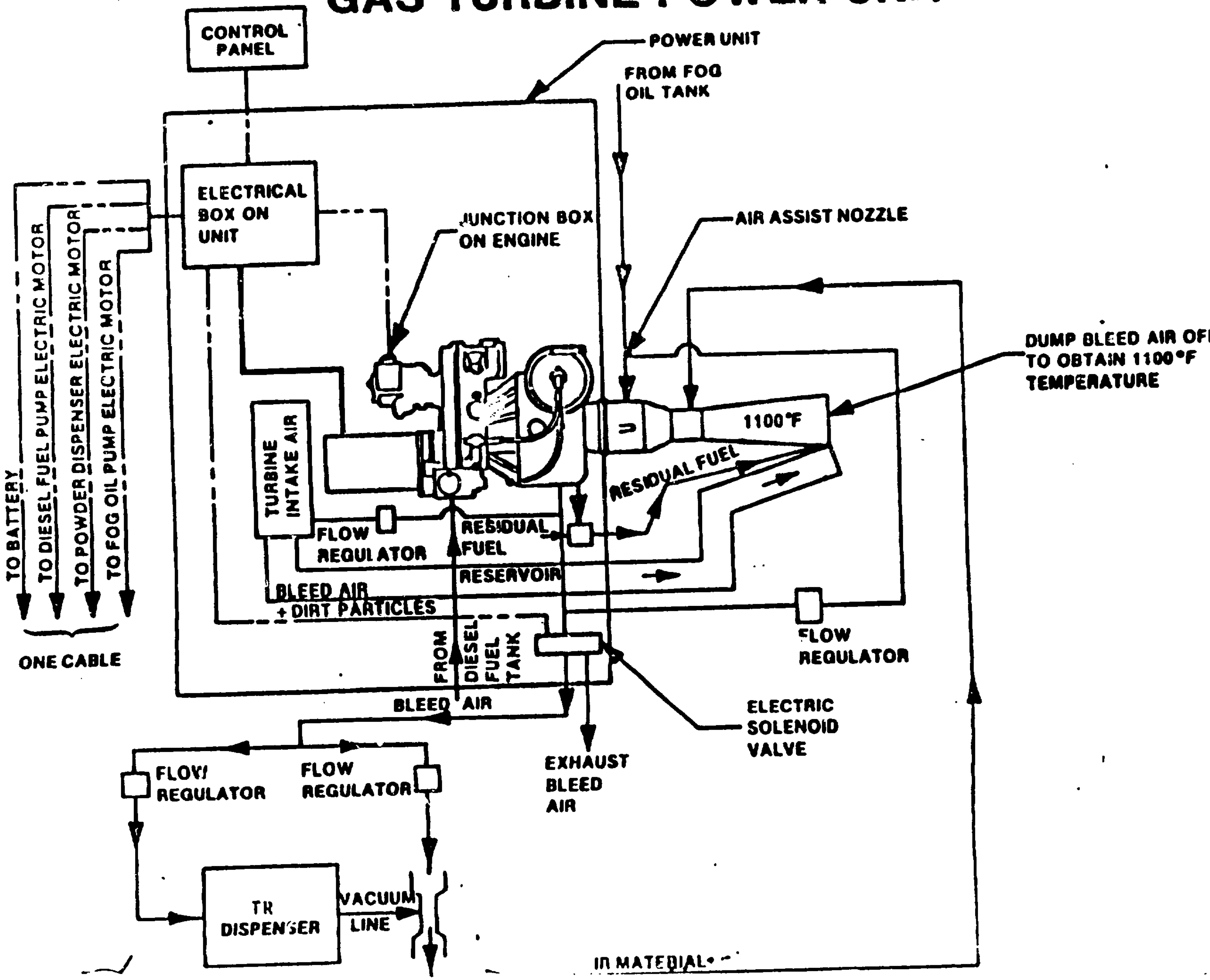
5 - Negligible

## XM52 SMOKE GENERATOR SYSTEM
## SCHEMATIC FOR PLATFORM-MOUNTED SYSTEM
## (HMMWV AND TRAILER)




BLEED AIR
SOLENOID VALVE
STARTER SOLENOID
ELECTRICAL BOX ON POWER UNIT
(14 LINES GOING THROUGH VEHICLE HULL FOR TWO SYSTEMS)
(1) NOZZLE
TOP OF M113
AIR & IR MATERIAL
MANUAL VALVE
MANUAL VALVE
IR DISPENSER
FOG OIL TANK
CONTROL PANEL
ELECTRIC MOTOR
ELECTRIC PUMP MOTOR
TO VEHICLE BATTERY
TO VEHICLE DIESEL FUEL TANK
TO ELECTRIC MOTOR ON DIESEL FUEL PUMP

# GAS TURBINE POWER UNIT



SYSTEM XM52 Smoke Generator

SUBSYSTEM Turbine

| SUBJECT HAZARD OR UNDESIRED EVENT | PROGRAM PHASE | CAUSE | EFFECT | HAZARD SEVERITY | HAZARD PROBABILITY | RAC | COMMENTS CORRECTIVE ACTION/ MINIMIZING PROVISIONS |
|---|---|---|---|---|---|---|---|
| Overspeeding of turbine rotor | Operation | Excessive fuel delivered to turbine | Turbine speed increases beyond 110% of rated speed. If this condition exists for more than 10 seconds, turbine will sustain severe damage and must be replaced. | I | D | 3 | Turbine design includes overspeed switch which is actuated if turbine exceeds 110% of rated speed. When overspeed switch is actuated, fuel flow solenoid valve closes and circuitry to igniter plug opens resulting in a turbine shutdown. Reliability rating of overspeed switch is 20 failures per million hours. |
| Turbine exhaust runs too hot | Operation | Overload or excessive turbine speed | If turbine experiences over temperature condition for more than 10 seconds, turbine will sustain severe damage and must be replaced. | I | D | 3 | The normal range of turbine exhaust when producing fog oil smoke is 900°F to 1100°F. The overtemperature switch shuts down the system when the temperature is in the range of 1150°F to 1170°F. Reliability of over-temp switch is .862 failures per million hours. |
| Hot Start | 2nd start attempt after false start | Fuel pools in base of combustion chamber | If turbine is started with excessive fuel in the combustion chamber, a fire hazard exists when a large flame exists the turbine exhaust. | II | D | 4 | The turbine is equipped with 4 drain lines which prevent a build up of residual fuel; 1) turbine fuel pump seal drain. 2) shroud drain. 3) overboard purge drain, and 3) combustor drain. The first three drains are open at all times and are aspirated out through the turbine exhaust. The combustor drain line incorporates a ball check valve which operates (closes) when combustion chamber pressure reaches 40 psi, however, any residual fuel (5-7cc) in the combustor from a false start will be expelled through the drain line and out the exhaust before the check valve closes. |
| Disintegration of turbine wheel in over-speed condition | Operation | Turbine exceeds rated speed, wheel becomes imbalanced because of shaft or bearing failure, material defect. | Turbine wheel disintegrates releasing high velocity fragments. In the HMMWV/Trailer application, the unit is mounted above the diesel fuel tank. Should a fragment penetrate the fuel tank, the potential for explosion and fire exists. | I | D | 3 | Turbine wheel is designed to shed the turbine vanes rather than bursting catastrophically. The turbine wheel housing is designed to retain the vane fragments if the wheel fails.<br><br>The overspeed safety switch would have to fail, the turbine vanes would have to be shed and the wheel housing would have to fail for a mishap to occur. This hazard probability is extremely unlikely and the RAC is more realistically a 5. |

SYSTEM: XM52 Smoke Generator

SUBSYSTEM: Starter/Generator

| SUBJECT HAZARD OR UNDESIRED EVENT | PROGRAM PHASE | CAUSE | EFFECT | HAZARD SEVERITY | HAZARD PROBABILITY | RAC | COMMENTS CORRECTIVE ACTION/MINIMIZING PROVISIONS |
|---|---|---|---|---|---|---|---|
| Failure of starter portion | Startup | Coil breakdown, bad wiring | Unit will not start | IV | C | 5 | Simple failure, no hazard identified. |
| Failure of generator portion | Startup and operation | Short or open windings | Unit will not start or if it starts, generator will not maintain spark for sustained combustion. Batteries will not be recharged if generator does not work. | IV | C | 5 | Simple failure, no hazard identified. |

SYSTEM: XM52 Smoke Generator

SUBSYSTEM: Air Filter System

| SUBJECT HAZARD OR UNDESIRED EVENT | PROGRAM PHASE | CAUSE | EFFECT | HAZARD SEVERITY | HAZARD PROBABILITY | RAC | COMMENTS CORRECTIVE ACTION/MINIMIZING PROVISIONS |
|---|---|---|---|---|---|---|---|
| Filter becomes clogged with dirt | Operation | Filter is designed to be self cleaning using bleed air. Bleed air delivered is inadequate or "sticky" adhering dirt fouls the filter. | Turbine receives inadequate airflow to sustain combustion. Turbine may overheat. | IV | C | 5 | No hazard identified. If turbine exhaust temperature exceeds specified limit, unit will shut down. |

SYSTEM: XM52 Smoke Generator

SUBSYSTEM: Storage Batteries

| SUBJECT HAZARD OR UNDESIRED EVENT | PROGRAM PHASE | CAUSE | EFFECT | HAZARD SEVERITY | HAZARD PROBABILITY | RAC | COMMENTS CORRECTIVE ACTION/MINIMIZING PROVISIONS |
|---|---|---|---|---|---|---|---|
| Explosion | Operation | Batteries may give off gases during re-charging which may be ignited by a spark source. | If battery compartment is not properly ventilated, gases may build-up in the compartment which could be ignited in the presence of a spark. Resulting explosion would damage the batteries, battery box, and possibly other system components and personnel. | I | D | 3 | Battery compartment will be properly ventilated IAW Requirement 27 of MIL-STD-454.<br><br>The storage battery will be the nickel-cadmium type. Ni-cads do not exhibit significant gas releases during the charging cycle as lead-acid batteries do. Therefore, the hazard probability is <u>extremely</u> unlikely and the RAC is more realistically a 5. |

SYSTEM: XM52 Smoke Generator

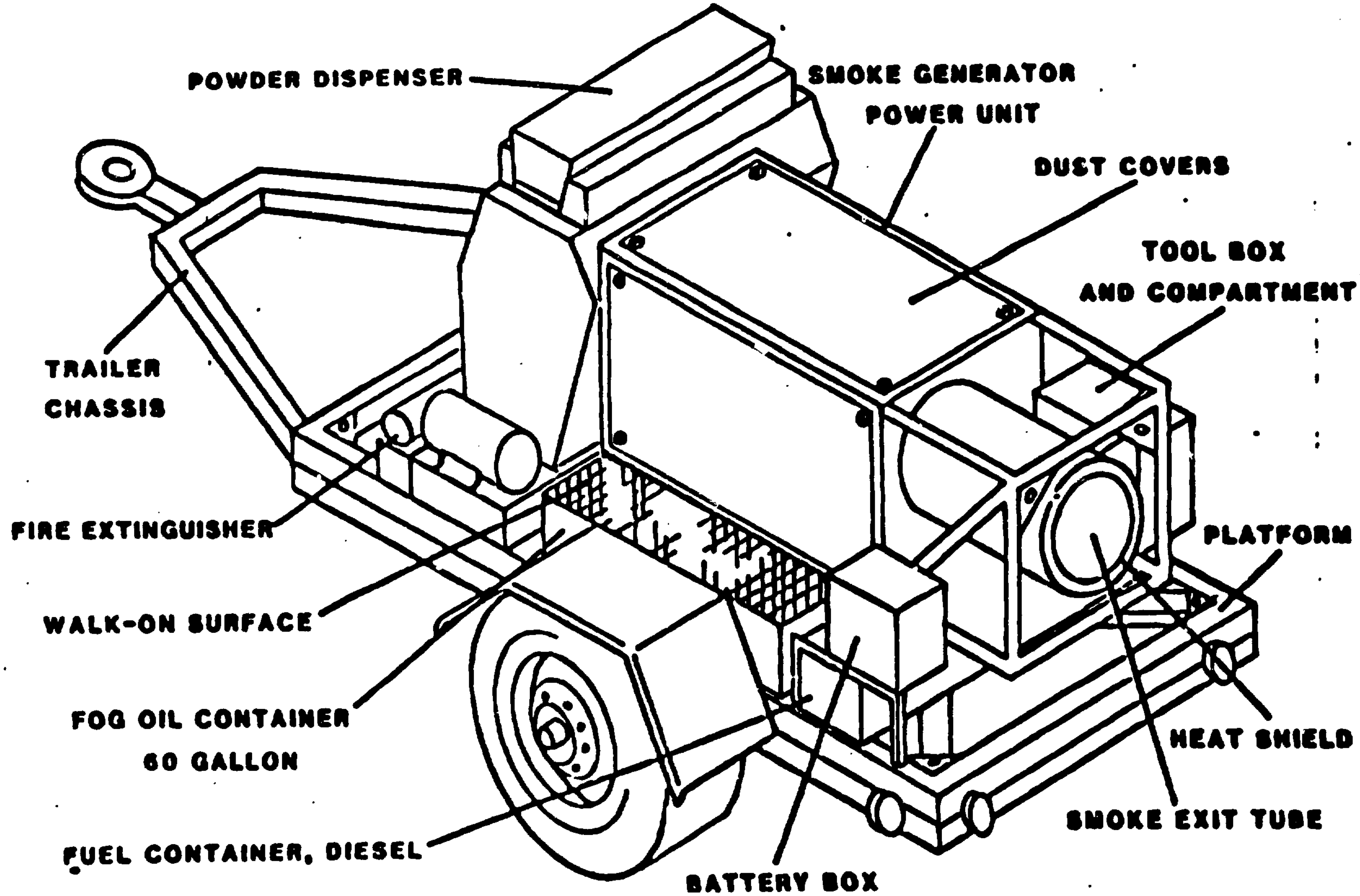
SUBSYSTEM: IR Dispenser

| SUBJECT HAZARD OR UNDESIRED EVENT | PROGRAM PHASE | CAUSE | EFFECT | HAZARD SEVERITY | HAZARD PROBABILITY | RAC | COMMENTS CORRECTIVE ACTION/MINIMIZING PROVISIONS |
|---|---|---|---|---|---|---|---|
| Drive belts break or drive motor fails. | Operation | Belts fail from wear or abuse. Motor experiences a short or winding failure. | IR dispenser will not work. | IV | D | 3 | IR dispenser will not work, but no hazard identified. Fog Oil Smoke Generation unaffected. |

SYSTEM: XM52 Smoke Generator

SUBSYSTEM: Diesel Fuel Tank & Fuel Pump

| SUBJECT HAZARD OR UNDESIRED EVENT | PROGRAM PHASE | CAUSE | EFFECT | HAZARD SEVERITY | HAZARD PROBABILITY | RAC | COMMENTS CORRECTIVE ACTION/MINIMIZING PROVISIONS |
|---|---|---|---|---|---|---|---|
| Tank ruptures or springs a leak. Fire hazard. | Operation | Material defect or puncture. | Fuel will be spilled causing a potential fire hazard. | I | D | 3 | Smoke generator system is equipped with a fire extinguisher to suppress a fire should one occur. Diesel fuel tank will be tested to ensure integrity. |
| Fuel pump fails. | Operation | Seal failure, loss of electrical power. | No fuel delivered to turbine. Unit shuts down. | IV | D | 5 | Unit will not operate, no hazard identified. |




TRAILER, 3/4 TON, 2 WHEEL, M116A1/A2 WITH XM52
SMOKE GENERATOR SYSTEM

FIGURE 2

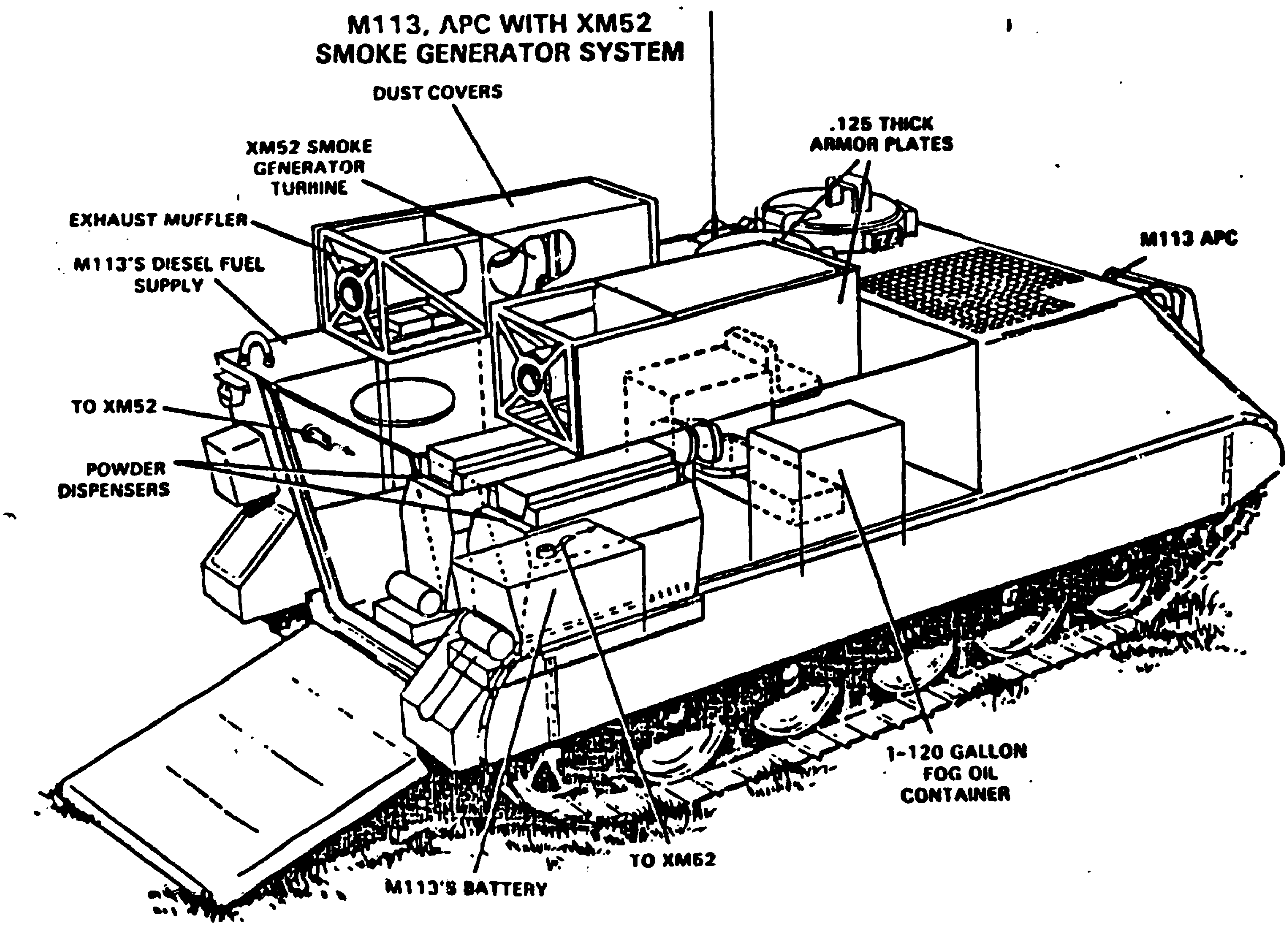

M113, APC WITH XM52
SMOKE GENERATOR SYSTEM
DUST COVERS
XM52 SMOKE GENERATOR TURBINE
EXHAUST MUFFLER
M113'S DIESEL FUEL SUPPLY
TO XM52
POWDER DISPENSERS
.125 THICK ARMOR PLATES
M113 APC
1-120 GALLON FOG OIL CONTAINER
TO XM52
M113'S BATTERY

FIGURE 3

... M52 Smoke Generator

... Fog Oil Tank & Fog Oil Pump

| ... HAZARD ... EVENT | PROGRAM PHASE | CAUSE | EFFECT | HAZARD SEVERITY | HAZARD PROBABILITY | RAC | COMMENTS CORRECTIVE ACTION/MINIMIZING PROVISIONS |
|---|---|---|---|---|---|---|---|
| ...ctures or ... a leak, ...zard. | Operation | Material defect or puncture. | Fog oil will be spilled causing a potential fire hazard. Smoke generation will cease. | I | D | 3 | System equipped with fire extinguisher to suppress a fire should one occur. Fog oil tank will be tested to ensure integrity. |
| ...pump fails. | Operation | Seal failure, loss of electrical power. | Smoke generation ceases. | IV | D | 5 | Unit will not produce smoke, no hazard identified. IR dispensing unaffected. |

OPERATING & SUPPORT HAZARD

ANALYSIS REPORT

FOR

XM52 LARGE AREA

SMOKE GENERATOR (FINAL)

REPORT NO. ER-12871A

DATE September 1983

SUBMITTED BY

FOR

PREPARED BY ______ CONTRACT NO.

APPROVED BY SEQUENCE NO. A00U

W/P LOG NO. DATA ITEM DI-H-7048

## FOREWORD

Included herein are the results of the Operating and Support Hazard Analysis (O&SHA) conducted by AAI's system safety personnel on the entire XM52 Smoke Generator system. In the body of the AAI report, there are several references to the turbine engine as a "modified Turbomach Model T-62T-2A1 turbine engine." Since this engine is in the Army inventory, these references have been retained so that reviewing personnel may refer to existing documentation to gain an understanding of the basic turbine capabilities. However, the modifications made to Model T-62T-2A1 were of sufficient scope that a new model number (T-62T-2D) has been assigned to the turbine engine to be used in the XM52 Smoke Generator application.

Included as the Attachment is the O&SHA report prepared by Turbomach personnel on the turbine engine, Model T-62T-2D. In the interest of clarity, the Turbomach report has been appended in its entirety.

This updated O&SHA Report incorporates the changes and corrections suggested by the Chemical Research and Development Center Safety Office letter dated August 23, 1983.

Of particular concern to the Safety Office was the possibility of IR material being blown back through the line which supplies atmospheric air to the venturi assembly. This potential hazard was recognized some months ago and an antiblowback valve has been incorporated in this line.

A request was also made by the Safety Office to analyze the hazard potential of either the fog oil tank or IR dispenser breaking free from their mounts in the M113 during an accident. The responsibility for the

XM52 installation in the M113 has been contracted with FMC Corporation for analysis to determine component locations and providing mount requirements. The shock and vibration testing requirements of MIL-STD-810 should be the guidelines to drive the design of the mounting provisions in the M113.

TABLE OF CONTENTS

# LIST OF FIGURES

## 1.0 INTRODUCTION

This Operating and Support Hazard Analysis (O&SHA) Report, is submitted in accordance with the requirements of Line Item A00U of the DD1423, Contract Data Requirements List, for Contract No. DAAK 11-82-C-0126, Advanced Development of the Large Area Smoke Generator, XM52. This report meets the requirements of Data Item Description (DID) DI-H-7048, System Safety Hazard Analysis Report.

## 2.0 GENERAL

The scope of this O&SHA is the systematic assessment of real and potential hazards associated with the operating and support tasks for the XM52 Smoke Generator. This O&SHA was conducted on the available system concept data and engineering drawings in an attempt to identify hazards and then direct design efforts toward the elimination or control of the identified hazards.

## 3.0 SYSTEM DESCRIPTION

The XM52 Smoke Generator is to provide a large area smoke screen which will provide protection from both visual and IR detection devices.

The XM52 Smoke Generator is being designed to provide large area obscuration capability to minimize detection by the enemy through either visual or infrared means. To accomplish this goal, the XM52 uses a slightly modified Turbomach turbine engine (Titan Model T-62T-2A1) as a heat and power source. By introducing fog oil into the hot turbine exhaust, the unit will be able to produce good quality smoke for protection from visual detection. Also, by using turbine bleed air and an electrically driven IR dispenser system, the XM52 will be able to introduce air-entrained IR material into the exhaust stream to provide protection from detection by IR devices.

### 3.1 Major Subsystem and Components

The following list presents the major subsystems and components of the XM52 Smoke Generator. While there are some differences between the XM52 for the HMMWV/Trailer application and the M113 application, these differences do not affect subsystem functions, only the provisions for mounting, length of cables and fluid lines and configuration and placement of fluid tanks. The list pertains to any XM52 system regardless of its application.

1. Frame structure
2. Turbine, (Turbomach Titan Model T-62T-2A1 slightly modified)
3. Starter/Generator
4. Air Filter System
5. Storage batteries (not on M113)
6. IR dispenser w/electric motor
7. Diesel fuel tank with electric fuel pump
8. Fog oil tank with electric fog oil pump
9. Operator's control panel
10. Electrical and fuel lines

## 4.0 ANALYSIS SUMMARY

The analysis results presented on the following pages address the hazard potential inherent in operating and support personnel tasks. Major concerns from the inception of the XM52 program have been the following:

1. Control of excessive noise.
2. Provisions of safe techniques for the replenishment of diesel fuel, fog oil and IR material.
3. Protection from inadvertent contact with hot surfaces and components.
4. Assurance of sound footing for maintenance tasks.
5. Avoidance of personnel contact with IR material.
6. Provision of guards around moving components.
7. Control (i.e. minimization) of possible fire conditions. Fire potential is impossible to eliminate where fuels are used.
8. Elimination of sharp edges, protrusions and pinch points.

As evidenced in the "Corrective Action/Minimizing Provisions" column of the analysis data sheets, the design incorporates provisions to address the concerns enumerated above.

Potential hazards associated with the maintenance of the turbine engine (i.e., use of cleaning agents) are not addressed in the accompanying analysis sheets. These hazards have been addressed in the technical manual (TM 3-1040-274-12&P) for the maintenance of the turbine engine.

4.1 The accompanying analysis sheets contain hazard severity levels, hazard probability levels and Risk Assessment Codes (RAC). The hazard probability levels and RAC are from AR 385-10 Interim Change No. 101. The hazard severity levels are from MIL-STD-882A so that system damage, as well as, personnel injury can be included in the definition and reflected in the hazard assessment.

HAZARD SEVERITY

a. Category I - Catastrophic. May cause death or system loss.

b. Category II - Critical. May cause severe injury, severe occupational illness, or major system damage.

c. Category III - Marginal. May cause minor injury, minor occupational illness, or minor system damage.

d. Category IV - Negligible. Will not result in injury, occupational illness or system damage.

HAZARD PROBABILITY

A - Likely to occur immediately

B - Probably will occur in time

C - Possible to occur in time

D - Unlikely to occur

RISK ASSESSMENT CODES

1 - Critical

2 - Serious

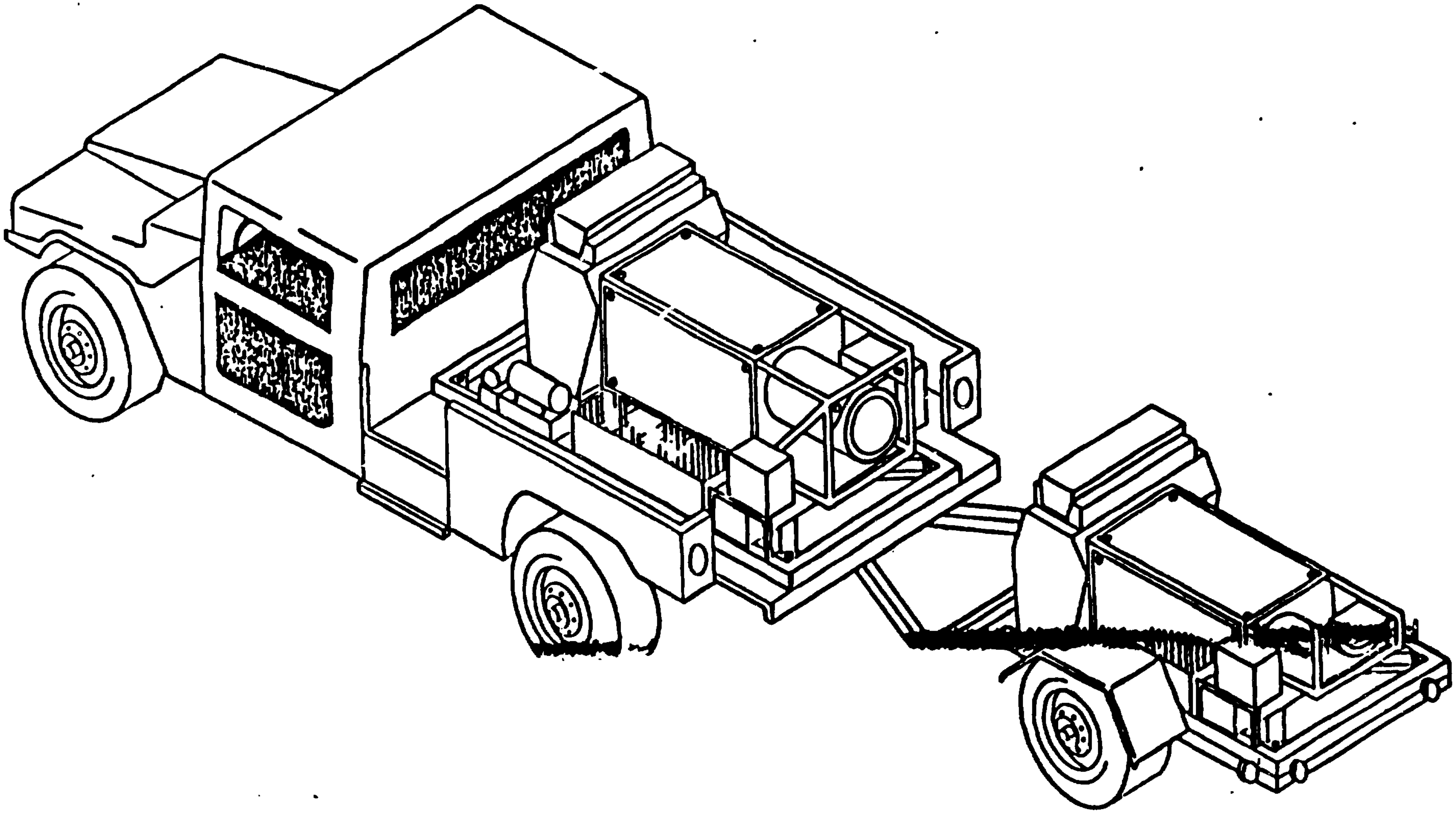
3 - Moderate

4 - Minor

5 - Negligible

## 5.0 PROPOSED DEPLOYMENT CONFIGURATION OF XM52 SMOKE GENERATOR

The XM52 Smoke Generator has been designed for deployment on the bed of the HMMWV, a towable trailer or on top of a M113 Armored Personnel Carrier (APC). The artist's conceptions of these three configurations are presented in the following figures. These figures are presented to aid the reader in understanding the details of the hazard analysis data sheets. It should be noted that the HMMWV and trailer configurations are identical with the entire system mounted on a subframe structure. The M113 configuration has only the generator units mounted on the top exterior, while the diesel fuel, fog oil and IR material supplies are located inside the vehicle.



HIGH MOBILTY MULTIPURPOSE WHEEL VEHICLE, (HMMWV) AND
3/4 TON TRAILER WITH 1 XM52 SMOKE GENERATOR SYSTEM EACH

FIGURE 1

## HAZARD ANALYSIS DATA SHEETS

SYSTEM XM52

SUBSYSTEM

| SUBJECT HAZARD OR UNDESIRED EVENT | PROGRAM PHASE | CAUSE | EFFECT | HAZARD SEVERITY | HAZARD PROBABILITY | RAC | COMMENTS CORRECTIVE ACTION/MINIMIZING PROVISIONS |
|---|---|---|---|---|---|---|---|
| Personnel exposure to excessive noise. | Operation | Turbine unit runs at very high rpm and moves a large volume of air which results in a high noise level. | Short duration exposure to high noise level results in temporary threshold shift and difficulty in verbal communication. Long term exposure can result in permanent hearing deficiency | III | B | 3 | Majority of generated noise is at the exhaust end of the unit which is also hazardous because of hot exhaust temperature, personnel must stay clear of this area. In order to minimize exposure to noise, the following have been incorporated into the design:<br>1) operating tasks are at the forward end of the unit<br>2) exhaust tube is equipped with a muffling device<br>3) unit enclosure panels internal surfaces are covered with sound deadening panels<br>All of these features will reduce personnel exposure to high noise levels, yet specific effectiveness of the above features cannot be evaluated until initial units have been manufactured for testing and performance evaluation.<br>Final Assessment - III, B, 4<br>NOTE: "Operator manuals will incorporate warnings requiring personnel to wear hearing protection devices when exposed to noise levels above 85 dB (A). |

SYSTEM XM52

SUBSYSTEM

## HAZARD ANALYSIS DATA SHEETS

| SUBJECT HAZARD OR UNDESIRED EVENT | PROGRAM PHASE | CAUSE | EFFECT | HAZARD SEVERITY | HAZARD PROBABILITY | RAC | COMMENTS CORRECTIVE ACTION/MINIMIZING PROVISIONS |
|---|---|---|---|---|---|---|---|
| Personnel exposure to hot surfaces. | Operation and Maintenance | Turbine combustion chamber and exhaust tube attain very high temperature. | Personnel contact with these items can result in severe burns. | III | B | 3 | Turbine combustion chamber is covered with a shroud to dissipate heat and contain turbine wheel fragments should the wheel shatter during operation (highly unlikely). In addition, the turbine is mounted in an enclosure to protect the unit from exposure to the elements and foreign objects. This enclosure also protects personnel from contacting the hot combustion chamber. Current estimate of enclosure internal temperature is 200-250°F during operation. Testing will determine the appropriate cool down period before maintenance can be attempted safely after the unit is shut down.<br><br>Similarly, the exhaust tube must not be touched until it has cooled to an acceptable temperature. The exhaust tube is centrally located within the skeletal frame at the rear of the unit to prevent inadvertent personnel contact.<br><br>Final Assessment - III, C, 4<br><br>NOTE: "Operator manuals will incorporate warnings to prevent personnel contact with hot surfaces". |

SYSTEM XM52

SUBSYSTEM Replenishment of IR Material

## HAZARD ANALYSIS DATA SHEETS

| SUBJECT HAZARD OR UNDESIRED EVENT | PROGRAM PHASE | CAUSE | EFFECT | HAZARD SEVERITY | HAZARD PROBABILITY | RAC | COMMENTS CORRECTIVE ACTION/MINIMIZING PROVISIONS |
|---|---|---|---|---|---|---|---|
| Personnel inhalation of IR particles | Replenishment of IR material | During IR material replenishment, personnel may encounter small amounts of IR material which becomes airborne during the replenishment process. These airborne particles may be inhaled | Research on the effects of ingesting the IR material have been inconclusive, however, the situation must be treated as potentially harmful to personnel health until more definitive data is collected. | II | C | 3 | Care has been taken in the design of the procedure for IR material replenishment to minimize personnel exposure to the material. Despite the minimal likihood of exposure, it is recommended that the personnel wear some form of particulate filter mask over the mouth and nose during the replenishment of IR material.<br><br>Introduction of IR material into the turbine exhaust stream is accomplished by using turbine bleed air to create a vacuum beneath the IR hopper. The IR hopper is equipped with a belt driven conveyor which supplies the vacuum air stream. Since this is a vacuum system, there is no potential for particulate blowback up through the hopper during replenishment. This arrangement again minimizes personnel exposure during the replenishment task.<br><br>Final Assessment - III, D, 5<br><br>NOTE: An anti-blowback valve has been incorporated in the line which supplies atmospheric air to the venturi assembly. |

SYSTEM XM52 (HMMWV & Trailer)

<u>HAZARD ANALYSIS DATA SHEETS</u>

SUBSYSTEM Replenishment of Fog & Diesel Oil Supplies

| SUBJECT HAZARD OR UNDESIRED EVENT | PROGRAM PHASE | CAUSE | EFFECT | HAZARD SEVERITY | HAZARD PROBABILITY | RAC | COMMENTS CORRECTIVE ACTION/MINIMIZING PROVISIONS |
|---|---|---|---|---|---|---|---|
| Fire during replenishment of fog oil while unit is running. | Operation | Accumulation of fog oil vapors or fog oil spillage which may be ignited if the tank refill port is located in close proximity to the hot exhaust of the turbine engine. | Fire potential external of the turbine combustion chamber, resulting in possible equipment damage or personnel injury. | I | C | 2 | Fog oil tank refill port is located near the forward end of the unit away from the hot exhaust. With this arrangement, the possibility of a resulting fire is negligible. As an added precaution, a fire extinguisher has been placed near the replenishment port.<br><br>Final Assessment - III, D, 5 |
| Fire during replenishment of diesel oil while unit is running. | Operation | Accumulation of fuel vapors or fuel spillage which may be ignited if the tank refill port is located in close proximity of the turbine engine. | Fire potential external of the turbine combustion chamber, resulting in possible equipment damage or personnel injury. | I | C | 2 | Diesel fuel tank refill port is located near the forward end of the unit away from the hot exhaust. With this arrangement, the possibility of a resulting fire is negligible. As an added precaution, a fire extinguisher has been placed near the replenishment port. Since diesel tank replenishment may be performed using 5-gallon cans, a splash guard/spill catch has been affixed to the diesel tank refill port. This spill catcher prevents fuel accumulation on walking surfaces used by maintenance personnel.<br><br>Final Assessment - III, D, 5 |

SYSTEM: XM52 (HMMWV & Trailer)

HAZARD ANALYSIS DATA SHEETS

SUBSYSTEM: Walking Surface

| SUBJECT HAZARD OR UNDESIRED EVENT | PROGRAM PHASE | CAUSE | EFFECT | HAZARD SEVERITY | HAZARD PROBABILITY | RAC | COMMENTS CORRECTIVE ACTION/MINIMIZING PROVISIONS |
|---|---|---|---|---|---|---|---|
| Personnel injury as a result of slip and fall | Maintenance | In order to gain access to the turbine for maintenance, personnel must stand on top of the fog oil tank. Since both fog oil and diesel fuel ports are located above this walking surface, minor fuel spills onto the walking surface are likely to occur. | Personnel may sustain injury as a result of slipping on the spilled fuel and falling to the ground. | II | C | 3 | Walking surface will be covered with non-skid surface to minimize the likelihood of slipping. Diesel fuel port is equipped with an overflow cup to minimize fuel spillage during refueling using 5-gallon containers. Refilling of fog oil tank is expected to be performed using a nozzle which is inserted into the tank's refill port, thus minimizing the possibility of spillage.<br><br>Final Assessment - III, D, 5 |

SYSTEM XM52 (M998/V & Trailer)

## HAZARD ANALYSIS DATA SHEETS

SUBSYSTEM IR Dispenser

| SUBJECT HAZARD OR UNDESIRED EVENT | PROGRAM PHASE | CAUSE | EFFECT | HAZARD SEVERITY | HAZARD PROBABILITY | RAC | COMMENTS CORRECTIVE ACTION/MINIMIZING PROVISIONS |
|---|---|---|---|---|---|---|---|
| Personnel overtaxing upper body muscles | Replenishment of IR Material | When replenishing the IR dispenser, personnel are required to lift 60 pound boxes of IR material to a height of approximately six feet. A lift of this weight to a height of six feet exceeds the capabilities of many personnel. | Possible upper body muscle strains and potential back injury. Probable spillage of IR material if replenishment package should rupture when dropped because the weight has become unmanageable. | III | C | 4 | It is recommended that two people perform the task of IR dispenser replenishment to minimize the probability of personnel injury.<br><br>Final Assessment - III, D, 5<br><br>NOTE: In compliance with paragraph 5.9.11.3.1 of MIL-STD-1472C, the boxes of IR material will be prominently labeled with weight indication and lift limitation, i.e. two person lift. |

SYSTEM XM52

SUBSYSTEM IR Dispenser

**HAZARD ANALYSIS DATA SHEETS**

| ..JECT HAZARD OR UNDESIRED EVENT | PROGRAM PHASE | CAUSE | EFFECT | HAZARD SEVERITY | HAZARD PROBABILITY | RAC | COMMENTS CORRECTIVE ACTION/MINIMIZING PROVISIONS |
|---|---|---|---|---|---|---|---|
| Entangling clothing, tools, or fingers in drive mechanism of conveyor belt beneat IR dispenser. | Maintenance and material replenishment | Conveyor belt requires use of pulleys and drive belts. | If drive pulleys and belts are exposed, personnel may be injured and equipment damaged if object becomes entangled in this mechanism. | II | C | 3 | Pulley and belts are covered by metal guards to preclude the likelihood of entanglement. Caution must be exercised if the guards are removed during the performanc of maintenance and functional checkout.<br><br>Final Assessment - III, D, 5<br><br>NOTE: Operator manuals will incorporate warnings to prevent entangling of clothing, tools, or fingers when the guards are removed. |

## HAZARD ANALYSIS DATA SHEETS

SYSTEM XM52

SUBSYSTEM Fog Oil Tank (M113)

| SUBJECT HAZARD OR UNDESIRED EVENT | PROGRAM PHASE | CAUSE | EFFECT | HAZARD SEVERITY | HAZARD PROBABILITY | RAC | COMMENTS CORRECTIVE ACTION/MINIMIZING PROVISIONS |
|---|---|---|---|---|---|---|---|
| Spilling fog oil inside of M113. | All | M113 is overturned in an accident causing fog oil to spill out the fill port. | Fog oil is spilled inside of M113 presenting a potential fire hazard as well as a fall hazard for personnel attempting to evacuate the vehicle. | I | C | 2 | While not yet designed, the intent is to provide M113 fog oil tank with an external fill port. Therefore, in the event of an overturn accident, there will be no fog oil spillage within the vehicle unless the tank itself is ruptured in the accident.<br><br>Final Assessment - I, D, 3<br><br>NOTE: The final assigned RAC of 3 is more appropriately a 5.<br><br>Hazard severity is unchanged, yet the hazard probability is extremely remote. However, this category is not included in the assignment scheme presented in AR 385-10. |

ATTACHMENT

SYSTEM XM52

SUBSYSTEM IR Dispenser (M113)

## HAZARD ANALYSIS DATA SHEETS

| SUBJECT HAZARD OR UNDESIRED EVENT | PROGRAM PHASE | CAUSE | EFFECT | HAZARD SEVERITY | HAZARD PROBABILITY | RAC | COMMENTS CORRECTIVE ACTION/MINIMIZING PROVISIONS |
|---|---|---|---|---|---|---|---|
| Spilling IR material inside of vehicle. | All | M113 is overturned in an accident causing IR material to flow to the top of the hopper where normal replenishment is accomplished. | If replenishment section of IR dispenser is not sealed, IR material would be spilled in the event of an accident. The resultant IR spillage would present a potential fall hazard (IR material makes surfaces slippery) and a potential health hazard (inhalation of airborne IR material). | III | D | 5 | Replenishment section of IR dispenser is equipped with a locking cover. In the event of an accident in which the M113 is overturned, IR material could not be spilled from the dispenser unless the dispenser hopper ruptured.<br><br>Final Assessment - IV, D, 5 |

OPERATING AND SUPPORT HAZARD ANALYSIS FOR
THE MODEL T-62T-2D ENGINE FOR THE XM52 SMOKE GENERATOR PROGRAM
SDRL ITEM AU08

## INTRODUCTION

This report contains the O & S (Operating and Support) Analysis for the Model T-62T-2D engine to be used in the XM52 Smoke Generator Program. This report is intended to satisfy the requirements of AAI SDRL item AU08 as described in SD1-0126-8. The scope of analysis was further defined and clarified by AAI personnel during the 5 May 1983 coordination meeting held at Turbomach. The report contains a description of the major engine components and their function, statements regarding design considerations affecting safety, failure modes, control measures in effect to minimize failure effects, and assessments of hazard severity and probability in accordance with MIL-STD-882A.

## DESCRIPTION

### General

The major components of the T-62T-2D are a turbine engine and electrical control devices. The turbine engine consists of a powerplant, accessories, and associated plumbing and wiring. The powerplant is divided into four main assemblies; turbine, combustor, reduction drive, and accessory drive.

The turbine engine incorporates an integral lubrication system. The lubricating oil supply is contained in an oil sump on the bottom of the reduction drive housing. A fuel supply must be connected to the unit, but all fuel system components necessary for operating the turbine engine are installed on the unit.

An Electronic Sequence Unit (ESU) is provided to sequence the functions during start. In addition, safety circuits are provided to shut down the unit in cases of failure to sequence, overspeed, overtemperature, or low oil pressure conditions, and processor failure. Speed is sensed from a signal generated by a magnetic pickup installed on the accessory drive. Exhaust gas temperature (EGT) is sensed by a thermocouple mounted on the exhaust end of the combustor with its probe extending into the exhaust gas stream.

Engine speed is controlled by a droop-type flyweight governor that delivers the correct amount of fuel regardless of the ambient conditions or load requirements within the specified limits.

Starting is initiated by energizing a starter-generator. During cranking, air is drawn into the compressor portion of the turbine where the air is compressed and then directed into the combustor. Fuel entering the combustor from a single start fuel nozzle and a fuel manifold containing three main fuel injectors is mixed with compressed air and ignited by the igniter plug. The resultant hot gases flow through the turbine nozzle and impinge on the blades of the turbine wheel. Rotation of the turbine rotor shaft provides the power to drive the compressor and output shaft of the turbine engine. The compressor wheel, mounted on the same shaft as the turbine wheel, continues to draw air into the compressor. Ignition and start fuel are cut off at a predetermined point. All fuel is then supplied through the three main fuel injectors. Combustion is a self-sustaining continuous cycle of intake, compression, combustion, and exhaust and is maintained within the engine.

Powerplant Assembly

The powerplant assembly consists of a turbine assembly, combustor, reduction drive assembly, and an accessory drive assembly. The forward end of the air inlet portion of the turbine assembly is bolted to the reduction drive assembly. The combustor assembly is clamped to a flange on the aft end of the air inlet housing. The accessory drive assembly is bolted to the top of the reduction drive assembly.

Turbine Assembly

Th. main components of the turbine assembly are an air inlet housing, rotor assembly, diffuser, turbine nozzle assembly, and an input pinion.

The air inlet housing is a contoured, cylindrical casting with forward and aft openings. The flanged forward end of the air inlet housing is bolted to the aft end of the reduction drive housing. The aft end of the air inlet housing is externally flanged to permit attachment of the combustor assembly. The housing thus serves as a rigid member between the reduction drive assembly and the combustor assembly.

The rotor assembly consists of a rotor shaft, single-stage centrifugal compressor wheel, radial-inflow turbine wheel, bearing retainer and oil slinger nut, spacer, forward ball bearing and aft roller bearing. The rotor shaft is mounted in bearings within a sleeve in the bore of the air inlet housing; the forward ball bearing carries thrust and radial loads; the aft roller bearing carries radial loads only. Three balls retain the input pinion in the forward end of the rotor shaft. The forward ball bearing is held in position by a bearing retainer plate and an oil slinger nut.

The compressor wheel shoulders against a flange on the aft end of the rotor shaft. Threaded compressor bolts are inserted through the flange into the compressor wheel. These bolts maintain the alignment of the compressor wheel and secure it to the rotor shaft. The turbine wheel is pressed onto the aft end of the rotor shaft and aligned by dowels. A threaded bolt fastens the turbine wheel to an internally threaded plug in the aft end of the rotor shaft.

A circular, compressor-to-turbine air seal separates the compressor section from the turbine section. The seal is radially positioned by a piloting diameter on the nozzle assembly. Axial position of the seal on the rotor shaft is maintained by compressor pressure which forces the seal against a shoulder on the turbine nozzle.

The cantilevered arrangement of the rotor assembly in the air inlet housing places both the forward and aft bearings in areas of minimum temperature. Cooling and lubrication of the rotor shaft bearings is accomplished by a flow of air-oil mist from the reduction drive housing, through the input pinion (within the rotor shaft), through the aft and forward bearings, and back into the reduction drive housing.

The diffuser is a circular casting consisting of vanes on the outer periphery and on the forward face. The turbine nozzle is a brazed, matched assembly consisting of a forward circular plate and an aft circular plate. The diffuser is secured in the aft portion of the air inlet housing by threaded nozzle retaining pins. These pins pass through the diffuser and also secure the turbine nozzle assembly concentric with the rotor assembly. The turbine nozzle assembly seats against a mating surface of the diffuser (fore and aft only, not radially).

Combustor Assembly

The combustor assembly is an annular air atomizing type and consists of a combustor housing, combustor liner, and nozzle shield. The combustor liner is secured in the combustor housing by three locating pins. The nozzle shield is secured to the combustor liner with six, self-tapping, screws. An external flange at the forward end of the combustor housing mates with an external flange on the aft end of the turbine assembly. The combustor is secured to the turbine assembly by a quick-release, V-type clamp that fits over the flanges. A ring on the outer wall of the combustor liner fits snugly under the inner aft edge of the turbine nozzle assembly. The mating of the combustor housing inner wall with the aft end of the turbine nozzle assembly forms a circular exhaust duct for the flow of exhaust gas as it passes through the rotor assembly and flows out of the engine.

Intake air passes through the vanes of the diffuser, flows between the walls of the combustor housing and liner, and reverses direction to enter the burner section of the combustor. This flow of air cools the combustor housing and liner. Air is also directed between the inner walls of the combustor housing and liner, passes through cooling holes immediately aft of the screws that secure the nozzle shield to the combustor liner and flows up between the nozzle shield and the aft surface of the turbine nozzle assembly. Additional cooling of the turbine nozzle is accomplished by a flow of cooling air that is forced around the aft, internal edge of the diffuser, through equally spaced holes in the ring on the combustor liner assembly, and over the aft side of the forward plate of the nozzle assembly.

An igniter plug, which is mounted in a boss at the aft, left side of the combustor housing, ignites the fuel-air mixture supplied by the start fuel nozzle during starting.

Fuel to the combustor is supplied through an external fuel manifold into three main fuel injectors that are equally spaced on the combustor housing. The main fuel injectors provide a stream of fuel into three venturi tubes which atomize and direct the fuel into the internal chamber of the combustor liner for burning. A port in the lowest position of the combustor housing, provides for a drain for fuel that may accumulate in the combustor.

A combustor shroud assembly completely encloses the combustor housing and provides a safety barrier for isolation and containment in the event of turbine wheel failure.

### Reduction Drive Assembly

The reduction drive assembly reduces the output rotational speed of the turbine assembly rotor to the speeds necessary to power the engine driven equipment. The reduction drive housing, machined from a magnesium casting and coated with fire retardant paint, contains the engine lubricating-system consisting of an oil pump, oil filter, pressure relief valve, filter bypass relief valve, oil jets, oil sump, and connecting passages.

An input pinion drives three planetary gears that in turn drive an internally splined ring gear within the reduction drive. The ring gear is centrally splined to a short output shaft. An external gear which is integral to the output shaft drives the oil pump drive gear. Also integral in the output shaft is an internal spline to which the driven equipment is coupled. The output shaft is supported at both ends by ball bearings. Axial positioning of the shaft is provided by the front bearing in addition to carrying most of the applied loads.

To prevent foaming, a deflector shield is installed between the sump and gear portions of the reduction drive assembly to minimize directed contact of the lubricating oil in the sump and the rotating gears. Lubrication of the gears and bearings is by oil jet stream and splash oil.

The oil filler cap is located on the reduction drive housing. The oil filler cap incorporates a chain to prevent its loss during servicing.

### Accessory Drive Assembly

The accessory drive assembly contains a cover plate, an accessory drive gear, two oil separator plates, two ball bearings, and two seals. The accessory drive housing is bolted to the top of the reduction drive assembly. The intermediate accessory drive gear which converts the reduction drive output speed (6000 rpm) to the speed required to drive the fuel control assembly (4200 rpm).

The accessory drive gear has an internally serrated shaft supported by ball bearings within the housing. The oil separator plates are mounted on the gear shaft at each side of the accessory drive gear.

The accessory drive gear and bearings are lubricated by splash oil from the reduction drive assembly. Seals, mounted in the housing and cover, prevent oil leakage.

### Bleed Air Valve

An electro-pneumatic servo actuated bleed air valve consists of a piston-operated valve disk and an electro-pneumatic torque motor. Operating air pressure for the butterfly valve piston is obtained from compressor discharge air pressure through a port in the valve body.

The air pressure is controlled by the electro-pneumatic torque motor, which regulates the pneumatic pressure to the piston in the bleed air valve, thereby positioning the valve disk. The valve is closed during engine start and is activated prior to smoke generation by a switch mounted on the control panel assembly.

## Fuel System

The fuel system consists of components that function automatically to provide proper engine acceleration and maintain a near constant operating speed under all operating conditions. These components are the fuel control assembly, fuel pump, start, main, and maximum fuel solenoid valves, start fuel nozzle, main fuel injectors, and fuel manifold. Fuel is supplied to the engine from the XM52 fuel system.

The main, start, and maximum fuel solenoid valves are hermetically sealed valves installed on the fuel control assembly and are operated by an electrical input.

The start fuel solenoid valve is a normally closed valve, energized to the open position at 5 percent rated speed to supply fuel to the start fuel nozzle. At 90 percent rated speed, the valve is deenergized and shuts off the fuel flow to the start fuel nozzle.

The main fuel solenoid valve is a normally closed valve, energized to the open position at 90 percent rated speed. When open, the valve allows fuel to flow to the main fuel injectors. Deenergizing this valve produces a normal shutdown of the engine.

The maximum fuel solenoid valve is a normally closed valve that is energized during engine starting to minimize the time required to reach 100 percent operating speed.

The start fuel nozzle, contained in a special fitting, is located on the left side of the combustor. Fuel to the nozzle is controlled by the start fuel solenoid valve. Fuel atomized by the nozzle is ignited by the igniter plug, located on the combustor close to, and directly in line with, the start fuel nozzle.

A start fuel nozzle purge system prevents buildup of varnish due to fuel evaporation during the period that fuel is not flowing through the start fuel nozzle while the engine is in operation. The purge system consists of a small restrictor orifice and a drain line in parallel with the start fuel nozzle.

During acceleration, when the start fuel solenoid valve is energized, fuel flows through the start fuel nozzle and also through the small restrictor orifice. The very small quantity of fuel flowing through the orifice is directed into a drain in the combustor shroud. At 90 percent speed the start fuel solenoid valve is deenergized and compressor discharge air flows through the start fuel nozzle, in reverse direction of fuel flow, through the orifice, and out the drain. This airflow cools the nozzle tip and purges residual fuel from the tip and the start fuel nozzle line assembly.

Three main fuel injector assemblies are interconnected and equally spaced around the circumference of the combustor. Each injector incorporates an integral filter that provides filtration to 15 microns. Fuel is supplied to the main fuel injectors through the main fuel solenoid valve and the fuel manifold.

The fuel pump is a positive-displacement, gear-type pump. The unit is mounted on the left output pad of the accessory drive assembly inside the fuel control assembly. The fuel pump spline adapter fits into an eight-point square drive in the shaft portion of the accessory drive gear. The other end of the fuel pump drive shaft is spline coupled to the governor drivehead assembly in the governor. A drain port in the pump housing drains fuel that might leak past the pump drive seal or past the pressure drop regulating valve pin.

The acceleration control assembly consists of the governor housing, the fuel control housing, and the bellows cover assembly.

The governor housing includes a pressure relief valve, a governor control spring, a flyweight assembly mounted in a drivehead assembly, and a matched ball bearing set which supports the internally splined shaft end of the drivehead assembly.

The flyweight assembly, located between the bearing valve assembly and the governor drivehead assembly, is pivot-mounted against the governor drivehead assembly and the bearing plate of the bearing and valve assembly.

The fuel control housing, which is secured to the forward face of the governor housing, contains a minimum fuel flow orifice, an acceleration needle adjustment, a ported fuel metering valve assembly, a governor adjusting plunger, a governor tension lever, a bearing and valve assembly, and an outlet port.

The aft end of the fuel metering valve extends into the fuel control housing. The spring retainer, which fits over the end of the fuel metering valve, is held in position around the metering valve by flanges on the spring retainer and the bearing and valve assembly. The piston of the bearing and valve assembly fits into the center of the fuel metering valve assembly.

The bellows cover assembly is secured to the top of the governor housing and consists of two interconnected sections. These sections are the diaphragm and bellows housing, and a lever housing. A diaphragm is installed between the pressure sensing portion of the belows cover assembly and the lever housing which, through mechanical connection, operates on the differential pressure regulating valve in the governor housing. A diaphragm adjusting screw is installed in the pressure sensing portion of the bellows cover assembly.

The turbine engine fuel system plumbing connections are all located on the fuel control assembly and combustor assembly.

Lubrication System

The lubrication system provides lubrication to the high-speed input pinion, reduction and accessory gears, and bearings. The lubrication system consists of the oil pump, oil filter, pressure relief valve, filter bypass relief valve, oil pressure switch, oil jet ring, centrifugal oil separator plates, oil passages, and oil sump.

The oil pump consists of two gears pinned on shafts mounted inside a two-piece housing, which is secured to the reduction drive housing. One oil pump gear (driver gear) is pinned to the oil pump drive shaft. The other gear (driven gear) is pinned to the oil pump driven shaft. A third gear, the oil pump drive gear, is pinned and secured with a nut to the end of the pump drive shaft just outside the oil pump housing, and is driven by the reduction gear train.

The oil filter consists of a filter housing in the reduction drive, a nominal 10-micron disposable filter element, and a bypass relief-valve housing that serves as a cap for the filter element. The cap (relief valve housing) incorporates a spring-loaded, ball-type, bypass relief valve.

The oil pressure switch incorporates normally closed contacts that actuate at 6 + 1 psig oil pressure. After the engine is operating at or above 90 percent rated speed, oil pressure below 6 $\pm$ 1 psig closes the contacts in the switch and initiates a low oil pressure engine shutdown. Visual indication is provided to note this occurrence.

The pressure relief valve is a spring-loaded, ball-type relief valve, internally mounted in the main oil gallery. The valve regulates the system oil pressure at 15 to 40 psig by bypassing a portion of the pump output to the sump.

Two centrifugal oil separator plates are mounted on the sides of the accessory drive gear in the top of the reduction drive housing. The plates remove the oil from the air-oil mist in the reduction gearbox before the air is vented to atmosphere.

The oil jet ring is located in the bearing carrier assembly for the planetary gear system. The jet ring encircles the high-speed input pinion and provides three jets of oil that are directed at the mesh points of the input pinion and planetary gears.

Electrical System

The engine-mounted components of the electrical system are the thermocouple, ignition exciter, ignition cable, spark plug, hourmeter, start counter, magnetic pickup, oil pressure switch, and three fuel solenoid valves. Descriptions of the oil pressure switch and fuel solenoid valves are included with the lubrication and fuel systems, respectively. Other electrical system components, lights, switches, etc. are mounted on the control panel assembly.

A single element, chromel/alumel thermocouple extends into the exhaust stream and senses engine exhaust gas temperature. The output signal of the thermocouple is transmitted to the ESU. If overtemperature is sensed the ESU will shut down the engine. The thermocouple is a component of the engine harness assembly.

The ignition exciter is bolted to the turbine assembly housing. This capacitor discharge-type exciter converts direct current input to a high-energy charge which is supplied to the spark plug for fuel ignition.

The ignition cable connects the ignition exciter to the spark plug. The high-energy pulse from the exciter to the plug is supplied through the ignition cable. The cable is protected by a flexible metal shielding.

A shunted-gap type spark plug is threaded into a boss in the left-hand, aft section of the combustor. The plug provides the spark necessary for initial ignition of fuel during the starting phase of engine operation.

The hourmeter indicates total accumulated hours of engine operation. This meter is installed on the hourmeter and electrical connector mounting bracket, located on the upper left side of the reduction drive and operates on 14 to 30 volts dc.

The start counter indicates the accumulated number of starts made on the engine. The counter is mounted on the same bracket as the hourmeter.

The magnetic pickup is installed on the accessory drive assembly. The magnetic pickup generates a frequency output as the accessory drive gear passes through the magnetic field surrounding the pole piece at the sensing end of the pickup. The frequency output is then transmitted to the ESU. An underspeed or overspeed condition detected by the ESU will result in an engine shutdown.

The ESU is a microprocessor that is programmed to control and initiate a sequence of events necessary for the satisfactory operation of the engine. Control is achieved by continuous monitoring of engine speed and exhaust gas temperature by the microprocessor.

Before the microprocessor instructs the ESU to initiate a required event, it compares input data just received against programmed data representing limit conditions for the required event. From the result of this comparison and program logic, the ESU will initiate the next event or a malfunction shutdown.

Functions controlled by this logic are engine start sequence to operation, malfunction indication and shutdown during start and engine operation. The logic also sequences itself to restart condition on reapplication of power to the system after shutdown. In addition to sequencing and protecting the engine, the ESU provides engine condition monitoring for fault isolation.

The BITE indicators incorporated in the panel assembly provide a visual indication of the malfunction that occurred at the time of unscheduled shutdown.

An RPM meter is furnished to indicate engine speed, expressed in percent rpm from 0 to 120. The meter is a long-scale instrument, having minor graduation of two percent. At rated engine speed, and with load, the pointer indicates 100 percent.

The EGT (exhaust gas temperature) meter furnished with the engine is a standard thermocouple-type temperature indicator graduated from zero to 1500°F. Its input signal is received from the same thermocouple as the temperature sensor.

HAZARD CONTROL CONSIDERATIONS

The T-62T-2D engine system designated for use in the XM52 Smoke Generator program was designed to provide bleed air and to operate at speed and temperature ranges well within the capability of the unit. The combination of a conservative design approach, quality control, selection of materials, and incorporation of engine condition sensing devices which initiate engine shutdown for out of tolerance conditions render hazard severities of potential hazards to Category III - marginal or Category IV - minor designations in accordance with MIL-STD-882A. Hazard probabilities associated with this engine fall into either level C - occasional or level D - remote. This means that even potential hazard items having both hazard probability C and hazard severity III will fall into a region of acceptability not requiring any redesign consideration. Table I contains a summary of the failure mode analysis, regarding possible hazards, including inherent failure rates, control measures to minimize failure effects, and assessments of hazard severities and probabilities.

The conclusion reached at Turbomach based upon analysis of the T-62T-2D engine design and upon field service data, test and operating experience on similar Titan engines is that the T-62T-2D engine can be operated safely for the XM52 Smoke Generator application.

All known hazards associated with the T-62T-2D engine operation have been considered and the probability of their occurrence and of their severity have been essentially eliminated through the appplication of a counservative design approach and the use of safety devices to protect the engine from unsafe operation.

The conservative design approach is to keep operating stresses to a minimum for all engine components containing fuel, lube oil, or combustion gases under pressure.

Hazards associated with high speed rotating machinery are minimized by applying a very conservative rotor design. The success of this approach is documented in a Solar (Turbomach) engineering report. With respect to the T-62T-2D engine a two-piece combustor shroud is used to provide an additional containment barrier in the event of turbine failure. Overspeed and overtemperature safety devices are provided to sense out of tolerance conditions which may be caused by a rotating part failure.

The ESU is a microprocessor unit that is programmed to control and monitor the engine. ESU control functions include engine start sequence through to operation, and malfunction indication and shutdown during start, and during operation. The BITE indicators incorporated into the Control Panel Assembly provides a visual indication of the malfunction that occurred at the time of an unscheduled shutdown. These indications include overspeed, overtemperature (high EGT), and low oil pressure conditions. In addition, indications of time out (start sequence failure) and processor failure (ESU internal failure) are provided.

## HAZARD CONTROL SUMMARY

### Power Section

The T-62T-2D power section is provided with an overspeed sensing device which initiates automatic engine shutdown before it can achieve destructive speed levels. Overtemperature and low oil pressure sensors are also provided to cause automatic engine shutdown for out of tolerance conditions. Turbine wheel containment is achieved by the selection of materials with physical properties conducive to high margins of safety at engine operating conditions. Structural details of the turbine nozzle assembly, combustor liner, combustor housing, and combustor shroud provide a series of concentric barriers for the containment of fragments which may result from a failed wheel and for the dissipation of the kinetic energy from such a failure.

A combustor drain is provided to permit draining of any unburned fuel during engine shutdown.

A fuel drain tank assembly is provided to collect any residual fuel, lube oil, or water condensation accumulated during engine operation. These residuals are aspirated from the drain tank to the engine exhaust using XM52 system equipment.

The reduction drive and accessory drive housings are designed to contain all components in the event of a malfunction of the lube oil pump or possible gear, bearing, or shaft failures.

## Fuel System

Cracked or broken fuel lines may allow fuel to leak. Periodic inspection is recommended to check for the occurrence of this hazard. Should a major leak occur during operation the engine will shutdown due to fuel starvation (flame out), or by the action of the speed sensing device detecting an underspeed condition.

## Lubrication System

A cracked or broken oil drain line may allow lube oil to escape. Periodic inspection is recommended to check for this occurrence. Loss of oil due to this condition or due to a malfunctioning oil pump, cracked oil passages, or breaks in the reduction drive housing will cause an automatic engine shutdown due to a low oil pressure condition detected by the oil pressure sensor.

## Electrical System

A single element themocouple extends into the exhaust gas stream and senses the engine exhaust gas temperature. An overtemperature condition sensed by the thermocouple will initiate an automatic engine shutdown. The thermocouple is a component of the engine harness assembly.

The ignition exciter is designed to safely bleed off internal high voltages. Personnel shock hazard is avoided by eliminating stored high voltage electrical potential form the ignition system.

## Electronic Sequence Unit (ESU)

The heart of the ESU is a microprocessor that is programmed to control and initiate a sequence of events necessary for engine operation. The ESU continuously monitors engine conditions such as speed, EGT, and oil pressure.

Before the microprocessor instructs the ESU to initiate a required event, the microprocessor compares input data just received against programmed data representing limit conditions for the required event. From the result of this comparison and program logic, the ESU will initiate the next event or a malfunction shutdown. The ESU will also initiate a shutdown in the event of an internal processor failure.

Failure Modes Analysis

Table I shows a summary of failure modes which may bear upon possible hazard conditions. Designations for hazard probabilities and hazard severities are in accordance with MIL-STD-882A.

Table 1. Failure Mode Analysis Summary

| Item Name | λ, Per $10^6$ HRS | Failure Mode | Failure Effect | Control Measures | Hazard Severity | Hazard Problem |
|---|---|---|---|---|---|---|
| Turbine Nozzle | 50 | Corroded, Clogged, Cracked | Set will not start, or set will shut down. | Start sequence failure, underspeed, overtemp protection. | III | D |
| Rotor Assembly | 170 | Broken, Seized, Excessive clearance | See above | Start sequence failure, overtemp protection, structural containment of turbine wheel fragments. | IV | D |
| Diffuser | 40 | Cracked, distorted | Set will shut down | Overtemp protection | IV | D |
| Air Inlet Housing | 40 | Cracked, distorted | See above | See above | IV | D |
| Combustor Shroud Assy | 20 | Cracked | None | N/A | IV | D |
| Combustor Cover Assy | 5 | Cracked | None | N/A | IV | D |
| Combustor Housing | 20 | Cracked, Leaking | Set will shut down | Overtemp protection | IV | D |
| Combustor Liner Assy | 80 | Thermal damage, distorted | Set will shut down | Overtemp, speed protection | IV | D |
| Start Fuel Nozzle | 20 | Clogged | Set will not start | Start sequence failure | IV | D |
| Fuel Manifold Assy | 25 | Cracked, Fuel leak | Performance loss, set shutdown | Speed protection. Material selection, conservative design, periodic inspection. | III | D |
| Spark Plug | 40 | Shorted, Open | No Start | N/A | IV | D |

?? DOC NO 0022b

| Item Name | λ, Per $10^6$ HRS | Failure Mode | Failure Effect | Control Measures | Hazard Severity | Hazard Problem |
|---|---|---|---|---|---|---|
| ..ain Valve Assy, Com-...tor | 20 | Stuck open stuck shut | Open - May not start Shut - may cause set shutdown | Open - Sequence Failure. Shut - Overtemp protection. conservative design, structural protection against hot start in combustor assembly | IV | D |
| ..in Fuel Tubing | 5 | Crimped, leaking | Performance loss, shutdown | Material selection, combustor assembly structural protection. Sequence failure | IV | E |
| ..art Fuel Tubing | 5 | Crimped, leaking | Start sequence failure | Material selection, structural protection, sequence failure. | IV | E |
| ..ce Restrictor | 10 | Plugged | No restart after shutdown. | Overtemp protection | IV | D |
| | | Leaking | No start | Sequence failure | | |
| ..el Drain Tank Assembly | 25 | Leaks, Crimped line | None | Material selection | IV | D |
| ..lenoid Bleed Air Valve | 40 | Stuck Open, Stuck Closed | Engine will not start, Bleed air unavailable | Sequence failure; EGT meter indication and manual shutdown | IV | D |
| ..gine Harness Assembly | 40 | Frayed wires, open connection | No start or shutdown | ESU will initiate shutdown | IV | D |
| ..el Control Assembly | 80 | Fuel pump malfunction, acceleration control faulty. | No start or shutdown | Speed and overtemp protection. | IV | D |

~ DOC NO 0022b

Table 1. Failure Mode Analysis Summary

| Item Name | λ, Per $10^6$ HRS | Failure Mode | Failure Effect | Control Measures | Hazard Severity | Hazard Problem |
|---|---|---|---|---|---|---|
| ...uction Drive Assy | 40 | Internal failure, cracked housing | No start or shutdown | Speed, overtemp, and oil pressure protection | IV | D |
| ...cessory Drive Assy | 20 | Broken spline | No start or shutdown | Speed and sequence fail protection | IV | D |
| ...ition Cable | 80 | Open, short | No start | None | IV | D |
| ...ition Exciter | 40 | Open, short | No start | None | IV | D |
| ...w Oil Pressure Switch | 10 | Open, short | No start or shutdown | ESU will initiate shutdown | IV | E |
| ...gh Oil Temp Switch | 10 | Open, short | No start or shutdown | ESU will initiate shutdown | IV | E |
| ...in Solenoid Valve | 10 | Electrical failure, Valve stuck closed | Shutdown | Speed protection | IV | E |
| | | Valve stuck open | Valve will not close on shutdown signal | Emergency shut off will curtail fuel supply-back up feature | | |
| ...rt Solenoid Valve | 10 | Electrical failure valve stuck closed | No start | Sequence Control | IV | E |
| | | Valve stuck open | Overtemp or time out condition | ESU will initiate shutdown | | |
| ...el Inlet Filter | 5 | Plugged | No start due to insufficient fuel | ESU will initiate shutdown | IV | E |
| | | Open | Possible contamination may degrade performance | | | |

... 005 NO 0023...

Table 1. Failure Mode Analysis Summary

| Item Name | $\lambda$, Per $10^6$ HRS | Failure Mode | Failure Effect | Control Measures | Hazard Severity | Hazard Problem |
|---|---|---|---|---|---|---|
| -gnetic Pickup | 20 | Open, shorted | No start or shutdown | ESU will initiate shutdown for loss of signal or intermittent signal | IV | D |
| -ectronic Sequence Unit | 300 | Internal failure | Set will not start or will shut down | Sequence failure, ESU internal monitoring | IV | D |

## APPENDIX E - DISTRIBUTION LIST

| Addressee | No. of Copies |
|---|---|
| Commander<br>U.S. Army Test and Evaluation Command<br>ATTN: AMSTE-ST-S<br>Aberdeen Proving Ground, MD 21005-5055 | 4 |
| Commander<br>U.S. Army Tank-Automotive Command<br>ATTN: AMSTA-CZ<br>Warren, MI 48397-5000 | 1 |
| Commander<br>U.S. Army Materiel Command<br>ATTN: AMCSF-E<br>5001 Eisenhower Ave<br>Alexandria, Va 22333-0001 | 10 |
| Commander<br>U.S. Army Armament Research, Development, and Engineering Center<br>ATTN: SMCAR-SFS<br>Picatinny Arsenal, NJ 07806-5000 | 1 |
| Commander<br>U.S. Army Natick Research, Development, and Engineering Center<br>ATTN: STRNC-S<br>Natick, MA 01760-5000 | 1 |
| Commander<br>U.S. Army Missile Command<br>ATTN: AMSMI-XO<br>Redstone, AL 35898-5000 | 1 |
| Commander<br>U.S. Army Belvoir Research, Development, and Engineering Center<br>ATTN: STRBE-Q<br>Fort Belvoir, Va 22060-5606 | 1 |
| Commander<br>U.S. Army Laboratory Command<br>ATTN: AMSLC-SO<br>Adelphi, MD 20783-1145 | 1 |
| Commander<br>U.S. Army Armament, Munitions and Chemical Command<br>ATTN: AMSMC-SFS<br>Rock Island, Il 61299-6000 | 1 |

| Addresses | No. of Copies |
|---|---|
| Commander<br>U.S. Army Communications and Electronics Command<br>ATTN: AMSEL-SF-MS<br>Fort Monmouth, NJ 07703-5007 | 1 |
| Commander<br>U.S. Army Safety Center<br>ATTN: PESC-SE<br>Fort Rucker, AL 36362 | 2 |
| Commander<br>U.S. Army Chemical Research, Development, and Engineering Center<br>ATTN: SMCCR-SFS<br>Aberdeen Proving Ground, MD 21010-5423 | 1 |
| Commander<br>U.S. Army White Sands Missile Range<br>ATTN: STEWS-DP-E<br>White Sands, Missile Range, NM 88002 | 1 |
| Commander<br>U.S. Army Yuma Proving Ground<br>ATTN: STEYP-SAF<br>Yuma, AZ 85364-9102 | 1 |
| Commander<br>U.S. Army Dugway Proving Ground<br>ATTN: STEDP-SA<br>Dugway, UT 84022-6302 | 1 |
| Commander<br>U.S. Army Defense Ammunition Center and School<br>ATTN: SMCAC-DEN<br>Savanna, IL 61074-9639 | 1 |
| Project Manager, TRADE<br>ATTN: AMCPM-TND-SP<br>Naval Training Center<br>Orlando, FL 32813-7100 | 1 |

| Addressee | No. of Copies |
|---|---|
| Director<br>U.S. Army Ballistic Research Laboratory<br>ATTN: SLCBR-DD-T (STINFO)<br>Aberdeen Proving Ground, MD 21005-5066 | 2 |
| Commander<br>U.S. Army Combat Systems Test Activity<br>ATTN: STECS-AD-A<br>STECS-SO<br>Aberdeen Proving Ground, MD 21005-5059 | 1<br>6 |
| Administrator<br>Defense Technical Information Center<br>ATTN: DDA<br>Cameron Station<br>Alexandria, Va 22304-6145 | 2 |

Distribution unlimited.