NUREG/CR-2169

TRANSEAVER/ TRANsport-by-SEA-VERification

Phase 1: System Conceptual Design

Prepared by B. R. Peterson, D. L. Small, O. L. Green, R. W. Griebe

Energy Incorporated

U.S. Arms Control and Disarmament Agency

Prepared for
U.S. Nuclear Regulatory
Commission

NOTICE

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, or any of their employees, makes any warranty, expressed or implied, or assumes any legal liability or responsibility for any third party's use, or the results of such use, of any information, apparatus product or process disclosed in this report, or represents that its use by such third party would not infringe privately owned rights.

Available from

GPO Sales Program
Division of Technical Information and Document Control
U. S. Nuclear Regulatory Commission
Washington, D. C. 20555

Printed copy price: $5.50

and

National Technical Information Service
Springfield, Virginia 22161

NUREG/CR-2169

TRANSEAVER/ TRANSport-by-SEA-VERification

Phase 1: System Conceptual Design

Manuscript Completed: May 1981
Date Published: June 1981

Prepared by
*B. R. Peterson, D. L. Small, O. L. Green, R. W. Griebe

*Energy Incorporated
P. O. Box 736
Idaho Falls, ID 83401

Under Subcontract to
U.S. Arms Control and Disarmament Agency
320 21st Street, NW
Washington, D.C. 20451

Prepared for
Division of Safeguards
Office of Nuclear Material Safety and Safeguards
U.S. Nuclear Regulatory Commission
Washington, D.C. 20555
NRC FIN B7302

ABSTRACT

A conceptual design for TRANSEAVER, Transport by Sea Verification, has been completed which shows the system could be a cost effective way to enhance safeguarding strategic and special nuclear materials during transport at sea. Applicable federal regulations and international guidelines have been considered with the expectation that TRANSEAVER will assist in meeting legal and regulatory considerations when used to monitor shipments. Utilizing existing RECOVER components and commercially available sensors, TRANSEAVER's link to a land-based command console is via MARISAT ship-to-shore communications equipment. Licensed shipping casks are enclosed in a security container and placed into a required closed van cargo container for a multiple boundary configuration which allows effective use of multiple sensor configurations. Any deviation from planned course or attempted tampering with the protected cargo automatically produces an Alerting Report at the command console.

TABLE OF CONTENTS

PAGE

ABSTRACT..iii

TABLE OF CONTENTS...v

LIST OF TABLES..ix

LIST OF FIGURES...xi

ABBREVIATIONS AND SYMBOLS...................................xiii

1.0 INTRODUCTION..1

2.0 AN OVERVIEW OF APPLICABLE REGULATIONS AND LEGAL CONSIDERATIONS..3

3.0 THE FEDERAL REGULATORY PROGRAM..........................4

3.1 Regulatory Agencies.....................................4
3.2 The Nuclear Regulatory Commission and Regulations.......4

3.2.1 Regulations for Ensuring Adequate Containment........5
3.2.2 Regulations for Safeguarding Nuclear Materials........5

3.3 The Department of Transportation and Its General Packaging and Shipment Requirements.......................9
3.4 The Department of Energy and Its Physical Protection Standards....................................11
3.5 The State Department....................................11

4.0 INTERNATIONAL AGENCIES..................................13

4.1 The International Atomic Energy Agency..................13
4.2 Inter-Governmental Maritime Consultative Organization....15
4.3 The Nuclear Energy Agency...............................15

5.0 THE TRANSEAVER SYSTEM...................................17

5.1 System Concept..17
5.2 System Operation..21
5.3 System Location...21
5.4 Non-Recover Off-the-Shelf Components....................23

5.4.1 Universal Teleprinter Interface (UTI).................23
5.4.2 Communications Terminal (CT)..........................23
5.4.3 Navigational Terminal (NT)............................23

TABLE OF CONTENTS (continued)

PAGE

6.0 SYSTEM SPECIAL INTERFACES....................................25

6.1 Sensor-to-MU Interfaces....................................25
6.2 Fiber Optic Seal Interface....................................25
6.3 X-Out-of-N Voting Circuit....................................28
6.4 Communications Interface Unit (CIU)....................................28
6.5 Amplifier and Comparator Interface....................................28
6.6 Power Circuitry....................................28
6.7 Fiber Optic Link Option....................................31

7.0 PROTECTION OF THE ELECTRONIC GEAR....................................34

8.0 SELECTION OF THE MONITORED SENSORS....................................38

8.1 Basic Criteria....................................40
8.2 Sensor Types/Locations....................................41
8.3 Sensor Specifications....................................45
8.4 Sensor Configurations....................................45

8.4.1 Passive IR Motion Detectors....................................45
8.4.2 ERMS (Seal)....................................47
8.4.3 Proximity Detector....................................47
8.4.4 Vibration Sensor....................................47
8.4.5 Temperature Sensor....................................47
8.4.6 Pressure Sensor....................................47

8.5 Related Considerations....................................48

8.5.1 Security of the Sensors....................................48
8.5.2 Flexibility of the Design....................................48

8.5.2.1 Flexibility vs. Protection Level....................................48
8.5.2.2 Flexibility vs. Cargo Material....................................49

8.6 Impact on Cask Certification....................................49
8.7 Impact on Transportation Operations....................................51

9.0 SELECTION OF SHIPPING CASKS....................................52

10.0 SCHEDULE AND COST ESTIMATES....................................56

10.1 Estimated Program Costs....................................56
10.2 Estimated Operation Costs....................................56
10.3 Amortized System Cost Per Shipment....................................58
10.4 Additional Cost Considerations....................................59

TABLE OF CONTENTS (continued)

PAGE

11.0 OTHER DEDICATED COMMUNICATIONS SYSTEMS....60
11.1 Ship To Shore Communications....60
11.2 Truck, Train, and Aircraft Communications....60

12.0 CONCLUSIONS....62

REFERENCES....63

BIBLIOGRAPHY....64

APPENDIX A - NRC REGULATIONS....A-1

APPENDIX B - DOT REGULATIONS....B-1

APPENDIX C - TRANSEAVER FUNCTIONAL REQUIREMENTS....C-1

1. Functional Description....C-1

1.1 MU Functional Description....C-3
1.2 OSM Functional Description....C-4
1.3 RVU Functional Description....C-6
1.4 PVU Functional Description....C-8
1.5 CIU Functional Description....C-9
1.6 UTI Functional Description....C-11
1.7 CT Functional Description....C-12
1.8 NT Functional Description....C-13

2. Data and Software Description....C-13

3. Interface Description....C-13

3.1 TRANSEAVER-Sensor Interface....C-30
3.2 Intra-TRANSEAVER Interfaces....C-30
3.3 TRANSEAVER-Inspector Interface....C-30

3.3.1 Alert Notification....C-34
3.3.2 Automatic Operation Interface....C-43
3.3.3 Demand Operation Interface....C-44
3.3.4 TRANSEAVER Subsystem Installation....C-44
3.3.5 Access Control....C-46

APPENDIX D - TRANSEAVER GENERAL SERVICE REQUIREMENTS....D-1

1. Environmental Requirements....D-1

2. Tamper Indication and Resistance Requirements....D-1

TABLE OF CONTENTS (continued)

PAGE

3. Maintainability Requirements....................................D-1

4. Safety Requirements...D-1

5. Packaging Requirements..D-6

6. Reliability and Survivability Requirements......................D-6

7. Reliability Goals...D-9

APPENDIX E - PROJECT QUALITY ASSURANCE PLAN..............................E-1

LIST OF TABLES

TABLE	TITLE	PAGE
6-1	TRANSEAVER LOAD CHART	32
7-1	REQUIRED TAMPER INDICATION/RESISTANCE MEASURES - SYSTEM ELEMENT	35
7-2	REQUIRED TAMPER INDICATION/RESISTANCE MEASURES - SYSTEM INTERFACES	37
8-1	TYPES OF SENSORS CONSIDERED FOR TRANSEAVER	42
8-2	MATRIX OF SENSOR TYPES/LOCATION	43
8-3	DETECTION SPECIFICATIONS FOR SENSOR MODELS	46
8-4	MATRIX OF SENSOR TYPES/LOCATIONS FOR THE MINIMUM PROTECTION DESIGN	50
9-1	LIST OF NRC CERTIFICATE NUMBERS FOR CASKS LICENSED TO CARRY PU AND U (FROM NUREG 0383, REV. 2, OCT. 79)	53
9-2	DESCRIPTION OF CASKS IDENTIFIED AS CANDIDATES FOR THE PHASE 1 TRANSEAVER CARGO	54
9-3	PROCUREMENT INFORMATION FOR TWO LICENSED SSNM CASKS	55
C-1	REQUIRED TRANSEAVER DATA ITEMS	C-15
C-2	IDS MODULE DESCRIPTIONS	C-20
C-3	INTRA-TRANSEAVER INTERFACE CHARACTERISTICS	C-31
C-4	INTRA-TRANSEAVER DATA ITEM TRANSMISSION REQUIREMENTS	C-32
C-5	PARTIAL LISTING OF RVU DISPLAYS AND REPORTS	C-35
C-6	PARTIAL LISTING OF PVU DISPLAYS	C-37
C-7	PARTIAL LISTING OF INSPECTOR COMMANDS TO RVU	C-39
C-8	PARTIAL LISTING OF INSPECTOR COMMANDS TO PVU	C-41
D-1	ENVIRONMENTAL REQUIREMENTS	D-2
D-2	REQUIRED TAMPER INDICATION/RESISTANCE MEASURES - SYSTEM ELEMENTS	D-3
D-3	REQUIRED TAMPER INDICATION/RESISTANCE MEASURES - SYSTEM INTERFACES	D-5

LIST OF TABLES (continued)

TABLE TITLE PAGE

D-4 SAFETY REQUIREMENTS..D-7

D-5 PACKAGING MAXIMUM SIZES (INCLUDING BATTERIES)................D-8

D-6 TRANSEAVER RELIABILITY GOALS................................D-10

LIST OF FIGURES

FIGURE	TITLE	PAGE
5-1	TRANSEAVER Overall System Design - Option 1	18
5-2	TRANSEAVER Overall System Design - Option 2	19
5-3	Protection Conceptual Arrangement	22
6-1	Typical MU - Sensor Arrangement	26
6-2	Fiber Optic Seal Interface	27
6-3	X-Out-of-N Voting Circuit	29
6-4	Amplifier and Comparator Circuit	30
6-5	Power Schematic	33
8-1	Shipment Construction	39
8-2	Possible Locations for Monitorable Sensors	44
10-1	Estimated Total Program Cost Through Demonstration	57
C-1	Software Block Diagram	C-14

ABBREVIATIONS AND SYMBOLS

AC	Alternating Current
ACDA	Arms Control and Disarmament Agency (United States)
AEC	Atomic Energy Commission
ANSI	American National Standards Institute
CFR	Code of Federal Regulations
CIU	Communications Interface Unit
CT	Communications Terminal
CVCC	Closed Van Cargo Container
DC	Direct Current
DOE	Department of Energy
DOT	Department of Transportation
ERMS	Electronic Remote-Monitorable Seal
HEU	Highly Enriched Uranium
IAEA	International Atomic Energy Agency
IEEE	Institute of Electrical and Electronic Engineers
IMCO	Inter-Governmental Maritime Consultative Organization
INMARSAT	Future MARISAT Communications System
ISO	International Standards Organization
MARISAT	Satellite Communications System
MU	Monitor Unit
NEA	Nuclear Energy Agency
NRC	Nuclear Regulatory Commission
NT	Navigational Terminal
OSM	On-Site Multiplexor
Pu	Plutonium

PVU	Portable Verification Unit
RAM	Random Access Memory
RECOVER	Remote Continual Verification
RVU	Remote Verification Unit
SC	Security Container
SCC	System Control Center (existing dial-up access to MARISAT)
SNM	Special Nuclear Material
SSNM	Strategic Special Nuclear Material
TRANSEAVER	Transport by Sea Verification
TRANSIT	Navigational Tracking Satellite
TT&C	Tracking, Telemetry, and Command Center (part of MARISAT)
UHF	Ultra High Frequency (300 Mhz-3 Ghz)
UL	Underwriters Laboratory (United States)
UPS	Uninterruptible Power Supply
UTI	Universal Teleprinter Interface

1.0 INTRODUCTION

Economic practicalities of the nuclear fuel cycle dictate a continuing and growing requirement for sea transport of nuclear materials. Recent reports published by Sandia Laboratories and the General Accounting Office (GAO) of the U.S. Government regarding the evaluation of policies and practices of the Nuclear Regulatory Commission and the Departments of Energy and Transportation suggest that security of sea shipments of nuclear materials can be improved.[1,2]

One way to improve the security of these shipments would be to provide a remote shipment status monitoring capability similar to that provided for fixed sites by the RECOVER system.

The RECOVER system has been developed to provide the International Atomic Energy Agency with the capability to continuously monitor safeguards devices deployed at nuclear facilities worldwide from the IAEA Headquarters in Vienna. This provides continuity of knowledge between visits to facilities by IAEA inspectors. That RECOVER system has been undergoing testing during the last year through an international program. The successful performance of the system has provided the impetus for study on expanding the use of this technology to monitoring shipments by sea. Therefore, the Nuclear Regulatory Commission and the Arms Control and Disarmament Agency have joined resources on investigating the feasibility of a concept called TRANSEAVER, TRANsport-by-SEA-VERification.

The TRANSEAVER concept combines RECOVER-type components with MARISAT (MARItime SATellite) equipment, penetration resistant shipping containers, and remotely monitorable sensors to provide continual monitoring of the locations and the integrity of nuclear material containers in seaborne shipment. By coupling RECOVER-type components to MARISAT equipment, deviation from planned course or attempted tampering of the cargo produces an Alerting Report upon demand at a central command console. The TRANSEAVER system would be comprised of selected containment and surveillance devices, RECOVER monitoring units, and RECOVER multiplexors to transmit pertinent data in a secure fashion to the ground-based command console.

To accomplish the ship-to-shore communications, the on-site multiplexor, which provides shipment status information, is connected to a shipboard terminal of the MARISAT system. The remote verification unit, which provides a display of sensor status at a remote, shore-side location, can then communicate with the on-site multiplexor by dialing the ship through the MARISAT satellite communication system. The Maritime Satellite system has been designed specifically to provide rapid and reliable communication services to commercial shipping and offshore industries.

MARISAT terminal equipment has been used successfully by more than 300 ships over the past four years. It can provide ship navigational data automatically in real time to the worldwide telephone network through the MARISAT satellite system. Therefore, the ship at sea can be linked directly and quickly via MARISAT with shore points anywhere in the world.

Commercially available shipping containers used in conjunction with the state-of-the-art containment and surveillance devices planned for this program appear to be compatible with existing Nuclear Regulatory Commission and Department of Transportation requirements and guidelines. In picking the shipping cask, consideration has been given to protective containers of different design.

Various types of sensors are proposed to monitor the integrity and location of the shipping container using several criteria. These criteria included the compatibility with the shipping container as well as the RECOVER monitoring units. In addition, the ability of the sensors and the monitoring equipment to withstand environmental characteristics typical of those to be endured during storage on a vessel underway at sea has also been considered. The level of security as well as commercial availability, reliability, survivability, cost-effectiveness, tamper resistance, and vulnerability, have been considered, not only with regard to use with the monitoring units, but also with regard to their impact on the transportation operations and/or tamper resistance of the closed shipping container.

One of the major objectives of the TRANSEAVER system is to increase safeguards on shipments of nuclear and other sensitive materials while maintaining compliance with current federal regulations and guidelines for such shipments. TRANSEAVER meets the physical protection measure which includes the provision of continuous two-way radio communication and frequent telephone communication. It also submits the package and its shipping cask to frequent and periodic examination of the seals together with a continuous surveillance of the cargo hold.

Implementation of the TRANSEAVER system will not only facilitate compliance with the guidelines for physical protection of nuclear material under shipment but also will provide increased assurance of the timely detection of diversion of nuclear materials during international transport.

2.0 AN OVERVIEW OF APPLICABLE REGULATIONS AND LEGAL CONSIDERATIONS

A general comment must be made regarding the legal considerations, both federal and international, that apply to the TRANSEAVER project. The regulations that apply to TRANSEAVER fall into two main areas of protection considerations:

1. Regulations designed to ensure nuclear safety, and

2. Regulations for safeguarding nuclear materials.

Regulations pertaining to nuclear safety have been promulgated by the Nuclear Regulatory Commission, the Department of Transportation, and the International Atomic Energy Agency. In Phase I of this project only licensed shipping containers have been considered. Two small radioactive materials packages (casks) suitable for this project have been licensed by the Nuclear Regulatory Commission and will continue to be available at least through November 1982. As a result, it will not be necessary to cover in detail the regulations applicable to packaging standards. However, at a future date the selection of shipping containers may change, particularly if spent fuel is to be monitored by the TRANSEAVER system, and an examination of specific Nuclear Regulatory Commission and Department of Transportation packaging standards would then be required. Those regulations that are applicable to the selection of adequate packaging are included in Appendices A and B for reference.

Regulations that pertain to safeguarding nuclear materials are more directly related to the TRANSEAVER project. Therefore, these regulations, both federal and international, must be covered in greater detail. A general legal overview indicates that the TRANSEAVER concept can be implemented while maintaining compliance with federal regulations and international recommended guidelines.

Thus, Sections 3.0 and 4.0 will cover relevant legal considerations with an emphasis on regulations that pertain to safeguarding nuclear materials in transit. In considering the relevant legal issues, it was necessary to use the following assumptions:

1. Highly enriched uranium (HEU) and plutonium (Pu) have been designated as the cargo for Phase I of the TRANSEAVER contract. The legal research completed for this phase pertains primarily to HEU and Pu. In some cases, however, referenced regulations have a broader scope and therefore might apply to future TRANSEAVER cargo shipments.

2. In Phase I of the TRANSEAVER project, the actual quantity of cargo has not been identified. Therefore, safeguards regulations referenced in this report are those which apply to special nuclear material quantities that require the most stringent protection. If smaller quantities of special nuclear material are shipped, other regulations requiring less stringent protection measures may be applicable.

3.0 THE FEDERAL REGULATORY PROGRAM

There are three basic considerations that pertain to the transportation of radioactive materials:

1. Nuclear safety of the radioactive material;

2. Adequate control of the radiation emitted by the material; and

3. Prevention of nuclear criticality.

The purpose of the U.S. regulatory program is to promulgate specific requirements and standards that will ensure the protection of the public and environment based on the above considerations.

3.1 Regulatory Agencies

Congress has granted statutory jurisdiction to regulate the transportation of radioactive materials to three federal agencies: the Nuclear Regulatory Commission, the Department of Transportation, and the Department of Energy. In the executive branch of government, the State Department also plays a role in overseeing the shipment of nuclear materials.

3.2 The Nuclear Regulatory Commission and Its Regulations

The Energy Reorganization Act of 1974 abolished the Atomic Energy Commission (AEC) and created the Nuclear Regulatory Commission (NRC). However, the licensing and other regulatory authority granted to the AEC by Congress in the Atomic Energy Act of 1954, as amended, was transferred to the Nuclear Regulatory Commission (P.L. 83-703). Thus, the NRC is now responsible for regulating safety and safeguards in the use of nuclear materials by the nuclear industry.

The transportation of by-product, source, and special nuclear materials is regulated by the NRC. Licensees are responsible for protecting the special nuclear materials they transport by providing appropriate containment and physical protection. The NRC, through its licensing and inspection program, ensures that required actions will be taken.

The rules and regulations of the Nuclear Regulatory Commission can be found in Chapter 1 of Title 10 of the Code of Federal Regulations. The parts of Title 10, Chapter 1 that most directly pertain to the transportation of special nuclear material are Parts 20, 70, 71, and 73. These parts include rules and regulations regarding "Standards for Protection Against Radiation," "Special Nuclear Material," "Packaging of Radioactive Material for Transport and Transportation of Radioactive Material Under Certain Conditions," and "Physical Protection of Plants and Materials." Rather than cover all the regulations, the following discussion focuses only on the regulations that seem to pertain to the implementation of TRANSEAVER. The discussion specifically addresses physical protection of special nuclear material. For a more detailed and balanced understanding of the requirements, the appropriate sections of the Code of Federal Regulations should be consulted. Regulations pertaining to requirements for adequate containment will only be cited.

3.2.1 Regulations for Ensuring Adequate Containment

The regulations that specify guidelines for ensuring nuclear safety are listed in Part 71 -- "Packaging of Radioactive Material for Transport and Transportation of Radioactive Material Under Certain Conditions." Relevant definitions of terms applicable to TRANSEAVER can be found in 10 CFR 71.4. Terms relevant to this project, such as "fissile classification," fissile "material," and "packaging," are cited in Appendix A.

The determination of standards for all packaging relates to the type and quantity of material transported. A system for classifying each radioisotope has been devised by the Nuclear Regulatory Commission. This classification sets out seven transport groups labeled by Roman numerals I through VII. These transport groupings can be found in Appendix C of of 10 CFR 71. Radioisotope quantities in each transport group are classified in order of increasing quantity such as "limited," "Type A," "Type B," and "large" quantity.

To be qualified for transport, any packaging used by the licensee must comply with applicable requirements to the mode of transport as listed in 10 CFR Part 71 and 49 CFR Parts 170-189. Specific exemptions are covered in Sections 71.7 through 71.10 of 10 CFR.

NRC approval is required depending on the Fissile Class and quantity of materials to be shipped (10 CFR §71.11). The NRC general standards for all packaging are listed in Subpart C of 10 CFR 71. As mentioned earlier, the selected casks (Task 3) have been licensed by NRC and therefore comply with these regulations. Applicable sections of Subpart C are listed in Appendix A.

3.2.2 Regulations for Safeguarding Nuclear Materials

Along with the importance of ensuring the nuclear safety of licensed materials, protection of certain special nuclear material in transit is vital. Certain quantities of strategic special nuclear material (SSNM) require physical protection against theft and sabotage during transit. Specific requirements relating to the physical protection of formula quantities of strategic special nuclear material in transit can be found in 10 CFR 73.25 to 10 CFR 73.36. These regulations apply to a licensee (10 CFR 70) who imports, exports, transports, or delivers to a carrier for transport of a formula quantity of SSNM in a single shipment or takes delivery of a single shipment, containing a formula quantity of SSNM, free on board (f.o.b.) These regulations, applicable to the TRANSEAVER project, address physical protection of "special nuclear material" in transit. Specific definitions for this material can be found in Section 73.2 of 10 CFR. Relevant citations can be found in Appendix A.

Since the regulations in 10 CFR part 73 are directly related to the TRANSEAVER project, specific sections will be cited and discussed. The major focus of this discussion is whether or not the TRANSEAVER system can be used in compliance with existing requirements for establishing and maintaining a physical protection system for transporting special nuclear material.

In Section 73.20 of 10 CFR, the general performance objective and requirements are stated. Each licensee, ". . . shall establish and maintain or make arrangements for a physical protection system which will have as its objective to provide high assurance that activities involving special nuclear material are not inimical to the common defense and security and do not constitute an unreasonable risk to the public health and safety."

Performance guidelines specifying fulfillment of this objective are covered in Section 73.25. Some of the requirements include (emphasis added):

Section 73.25 Performance capabilities for physical protection of strategic special nuclear material in transit.

(iii) Maintaining knowledge of the status and position of the strategic special nuclear material en route; and . . .

(2) Detect and delay any unauthorized attempt to gain access or introduce unauthorized materials by stealth or force into the vicinity of transports and strategic special nuclear material using the following subsystems and subfunctions.

(ii) Access detection subsystems and procedures to detect, assess, and communicate any unauthorized penetrations (or such attempts) of controlled access area by persons, vehicles, or materials so that the response will satisfy the general performance objective and requirements of §73.20(a).

(2) Detect attempts to gain unauthorized entry or introduce unauthorized materials into transports by stealth or force using the following subsystems and subfunctions:

(i) Transport features to delay access to strategic special nuclear material sufficient to permit the detection and response system to function . . .

(ii) Inspection and detection subsystems and procedures to detect unauthorized tampering with transports and cargo containers; and

(iii) Surveillance subsystems and procedures to detect, assess, and communicate any unauthorized presence of persons or

> materials and any unauthorized attempt to penetrate the transport . . .
>
> (4) Detect attempts to remove strategic special nuclear material from transports by stealth or force using the following subsystems and subfunctions:
>
> (i) Transport features to delay unauthorized strategic special nuclear material removal attempts sufficient to assist detection and permit a response to satisfy the general performance objective and requirements of §73.20(a); and . . .
>
> (ii) Detection subsystems and procedures to detect, assess and communicate any attempts at unauthorized removal of strategic special nuclear material . . .
>
> (d) Respond to safeguards, contingencies, and emergencies to assure that the two capabilities in paragraphs (b) and (c) of this section are achieved and to engage and impede adversary forces until local law enforcement forces arrive. To achieve this capabillity, the physical protection system shall:
>
> (1) Respond rapidly and effectively to safeguard contingencies and emergencies using the following subsystems and subfunctions:
>
> (iv) Equipment and procedures to enable responses to security-related incidents sufficiently rapid and effective to achieve the predetermined objective of each action.
>
> (2) Transmit detection, assessment, and other response-related information using the following subsystems and subfunctions:
>
> (ii) Equipment and procedures for two-way communications betweeen the escort commander and the movement control center to rapidly and accurately transmit assessment information and requests for assistance by local law enforcement forces and to coordinate such assistance.
>
> (iii) Communications equipment and procedures for the armed escorts and the movement control center personnel to notify local law enforcement forces of the need for assistance. (emphasis added)

TRANSEAVER is designed to aid in providing the physical protection measures highlighted in these regulations. This system, by providing frequent reporting to a ground-based command console, will have the capability to maintain knowledge of both the status and position of the nuclear material during transit, §73.25(b)(iii). Any unauthorized penetrations (or attempts to do so) are to be detected and communicated by the TRANSEAVER project,

§73.25(b)(iii). Detection of unauthorized tampering with the cargo will automatically produce an Alerting Report at a command console, §73.25(c)(ii). The sensors are proposed to monitor the integrity and location of the shipping container which would enable rapid and effective communication to safeguards contingencies and emergencies, §73.25(d)(1)(iv).

Section 73.26 of 10 CFR deals with physical protection of transportation systems, subsystems, components, and procedures. Section (1) specifies regulations for the shipment of SSNM by sea:

> (1) Shipments shall be made only on container-ships. The strategic special nuclear material container(s) shall be loaded into exclusive use cargo containers conforming to American National Standards Institute (ANSI) MH5.1 or International Standards Organization (ISO) 1496. Locks and seals shall be inspected by the escorts whenever access is possible.
>
> (7) Ship-to-shore communications shall be available, and a ship-to-shore contact shall be made every six hours to relay position information and the status of the shipment.

In Phase 1 of the TRANSEAVER project, the special nuclear material payload will be shipped in a closed van cargo container. This container, which complies with ANSI MH5.1.-1979, will be used exclusively for TRANSEAVER cargo. TRANSEAVER provides ship-to-shore communications and allows for ship-to-shore contact every six hours §73.26(1)(7). More frequent contact (e.g., every hour) is also feasible.

Finally, in Section 73.37 of 10 CFR, regulations concerning transportation of irradiated reactor fuel are covered. Relevant portions of these regulations are cited below. As the TRANSEAVER project may apply to irradiated fuel shipments in the long term, these regulations should be addressed at this time.

According to the performance objectives in §73.37(a),

> (1) Each licensee who transports or delivers to a carrier for transport, in a single shipment, a quantity of irradiated reactor fuel in excess of 100 grams in net weight of irradiated fuel, exclusive of cladding or other structural or packaging material, which has a total external radiation dose ratio in excess of 100 rems per hour at a distance of 3 feet from any accessible surface without intervening shielding, shall establish and maintain, or make arrangements for, and assure the proper implementation of, a physical protection system for shipments of such material that will achieve the following objectives:

(i) Minimize the possibilities for radiological sabotage of spent fuel . . .

Specific objectives of a physical protection system include provisions for ". . . early detection and assessment of attempts to gain unauthorized access to, or control over, spent fuel shipments;" §73.73(a)(2)(i); and ". . . notification to the appropriate response focus of any spent fuel shipment sabotage attempts . . ." §73.73(a)(2)(ii).

Under general requirements for shipments by sea, Section 73.73(e), specific provisions applicable to TRANSEAVER include:

(3) Escorts have the capability of communicating with the communications center and local law enforcement agencies through the use of a radiotelephone or other NRC-approved equivalent means of two-way voice communication.

The TRANSEAVER system, which will be comprised of selected containment and sophisticated surveillance devices, has the potential to serve as a sabotage deterrent. The remote-monitorable sensors will provide frequent reporting and allow for early detection of tampering or any attempt to gain unauthorized access to the cargo. The TRANSEAVER system, by providing frequent communication capability, does not require an escort to be responsible for contacting a communications center as stated in §73.73(e)(3). TRANSEAVER, in comparison to two-way communications, would provide a better system for frequent monitoring of irradiated fuel shipments.

Examination of the NRC's physical protection regulations in Part 73 of Title 10 CFR indicates that the proposed TRANSEAVER project will help to meet many of the federal requirements for shipping nuclear materials by sea. The proposed system will help to provide nuclear safety assurances and to verify physical protection of radioactive material by using sophisticated monitoring equipment for frequent communication. TRANSEAVER, in supplementing current safeguard methods, also provides an increased assurance of detecting attempts to divert nuclear materials during international transport.

3.3 The Department of Transportation and Its General Packaging and Shipment Requirements

The Department of Transportation (DOT) has overlapping jurisdiction over safety in packaging and transportation of radioactive materials under the following statutes:

Department of Transportation Act
(P.L. 89-670)

Transportation of Explosives and other Dangerous Materials Act
(18 U. S. C. 831-835)

Hazardous Materials Transportation Safety Act of 1974
(P.L. 93-633)

Federal Aviation Act of 1958
(49 U. S. C. 1421-1472(b))

These statutes vest in the Secretary of Transportation the regulatory responsibility for safety in transporting radioactive materials by all modes of transport (rail, highway, air, and water). The safety standards for transportation, as set forth in Department of Transportation regulations (49 CFR Parts 170-178), are based on two considerations:

(1) Protection of the public from external radiation, and

(2) Assurance that the contents are unlikely to be released during either normal or accident conditions of transport or, if the container is not designed to withstand accidents, that its contents are so limited in quantity as to preclude a significant radiation safety problem if released.

DOT regulations are applicable to transportation of radioactive material in interstate and foreign commerce, while Nuclear Regulatory Commission packaging standards apply to shipments of source, by-product, and special nuclear material by Nuclear Regulatory Commission licensees. In order for the development and implementation of a consistent and comprehensive set of regulations, the DOT and NRC entered into a Memorandum of Understanding in 1966, which has been superseded by revisions. The most recent version of the Memorandum of Understanding is dated July 2, 1979. According to the latter versions of the memorandum, the NRC is responsible for developing and implementing performance standards for package designs for Type B fissile and large quantity packages. The DOT is responsible for developing and implementing safety standards for handling and storage of all radioactive material packages while in possession of a common, contract, or private carrier, as well as standards for Type A packages.[4]

The regulations as prescribed in Sections 173.391 through 173.396 of 49 CFR pertain to the packaging design, size, and required specific features. These requirements have already been addressed during the licensing phase for the container (cask) and do not need examination in this report. As mentioned in Section 2.0 of this report, an NRC-certified cask will be used by the TRANSEAVER system.

As it may be necessary to become familiar with DOT packaging requirements over the long term (particularly if transport of spent fuel is to be included in the program), specific citations from the relevant sections (§173.391 through 173.396) of 49 CFR have been included in Appendix B.

3.4 The Department of Energy and Its Physical Protection Standards

Regulatory authority is granted to the Department of Energy (DOE) in the following statutes: Atomic Energy Act of 1954, as amended, the Energy Reorganization Act of 1974, and the Nuclear Non-proliferation Act of 1978. It is this agency's policy to physically protect all special nuclear material in DOE custody against theft, sabotage, and other hostile acts. The Secretary of Energy is also required to submit a physical security plan addressing the requirements for security that pertain to the export of nuclear materials to the State Department.

The NRC Office of Nuclear Material Safety and Safeguards works closely with DOE officials to assure that comparable physical protection standards are provided for the shipment of licensed and license exempt special nuclear material. The specific DOE requirements for the physical protection of special nuclear material can be found in DOE Order 5632.2, 2-16-79, "Physical Protection of Special Nuclear Materials."

Standards in Order 5632.2 are separated according to specific category quantities as specified in Section 6(c)(d)(e). Section 8(e) addresses Category I quantities (the same as NRC formula quantities) of special nuclear material and classified configurations of Category II quantities (less than NRC formula quantities) of special nuclear material, in transit. This section forbids transportation by sea. Section 8(e) (1) covers the protection standards for Category II quantities of special nuclear materials in transit. Again, sea transportation is forbidden. Section 8(i) covers the standards for Category III (less than NRC formula quantities) quantities of special nuclear materials in transit. In subsection 1, the following methods of transportation are considered: truck, rail, air, or water in commercial for-hire vehicles. The following requirements in this section apply to the TRANSEAVER project:

(2) Packages shall be sealed.

(3) Shipments, excluding shipments of laboratory analysis samples, shall be made under arrangements which provide the capability to trace and identify, within 24 hours of request, the precise leg of a journey where a shipment went astray in the event of its non-arrival at destination within the prescribed time-frame. (emphasis added)

In regard to these requirements, TRANSEAVER will provide frequent reporting upon demand and thus allow the capability to trace the position and status of nuclear cargoes shipped by sea. Packages to be used have been licensed by the Nuclear Regulatory Commission and thus meet requirement for seals.

3.5 The State Department

The Nuclear Regulatory Commission is precluded from issuing an export license for any source material or special nuclear material unless it has been notified by the Secretary of State that, in the judgment of the

Executive Branch, the proposed export is not inimical to the common defense and security (P. L. 95-242 Section 126(1)). The Secretary of State is responsible for establishing orderly and expeditious procedures, which are mutually agreeable to the Secretaries of Energy, Defense, and Commerce, the Director of the Arms Control and Disarmament Agency, and the Nuclear Regulatory Commission, for the preparation of the Executive Branch judgment on export applications.

4.0 INTERNATIONAL AGENCIES

On an international basis, recommended guidelines for the safe transport of radioactive materials have been established by the International Atomic Energy Agency.(IAEA). The first efforts of the IAEA resulted in the publication of "Recommendations for the Physical Protection of Nuclear Material" in 1972. Many IAEA member states and world organizations participated in preparing these recommendations. Another international organization, the Inter-Governmental Maritime Consultative Organization (IMCO), has been concernea with nuclear materials since 1967. This organization comes under the auspices of the United Nations and has developed operational guidelines related to the transoceanic shipment of nuclear materials.

A third international agency involved with international transport of nuclear materials by sea is the Nuclear Energy Agency (NEA). This agency is affiliated with The Organization for Economic Cooperation and Development.

Even though these international agencies have adopted recommended guidelines, the responsibility for the establishment and operation of a comprehensive physical protection system for transporting nuclear materials rests entirely with the government of a particular country. Physical protection is a matter of international concern; however, international cooperation is not mandatory and agency guidelines are only "recommended." Since the U.S. government has recognized the work of international arencies to some extent, relevant operations and guidelines will be addressed in the following sections.

4.1 The International Atomic Energy Agency

It is the intent of IAEA and member countries to achieve high standards of safety for the international transport of radioactive and fissile materials. A document published in 1979 entitled IAEA Safety Standards (No. 6) covers recommendea regulations for the safe transport of radioactive materials. Sections in this edition cover packaging and package design requirements, transport arrangements for low specific activity material and low-level solid radioactive material, activity limits for Type A and B packages, controls for transport and storage in transit, provisions for fissile materials, and test and inspection procedures. It is the purpose of these regulations to establish safety standards primarily for packaging and packages. As mentioned earlier in this report, the selected casks for TRANSEAVER have been licensed by the NRC. Thus, the packaging to be used for TRANSEAVER complies with NRC regulations and, where referenced in the CFR, IAEA regulations. It will not be necessary to cover these regulations at this time.

The IAEA has also recognized the importance of physical protection of nuclear materials in an international setting. To facilitate the establishment and operation of a comprehensive physical protection system, international cooperation becomes of vital importance to achieve an effective program. The IAEA does not have the power to mandate actions by nation states for the physical protection of nuclear material in use, transit, and storage. The IAEA, however, has developed recommended measures for use by states as required in their particular physical protection system. The recommended measures are intended for nuclear shipments; relevant recommendations from the document INFCIRC/225/Rev. 1, "The Physical Protection of Nuclear Material," will be cited and discussed below.

Section 6. Requirements for Physical Protection of Nuclear Material in Transit

6.2.4 Provision of locks and seals

6.2.4.1 Unless there are overriding safety considerations, the packages containing nuclear material should be carried in closed, locked vehicles, compartments, or freight containers. However, carriage of packages weighing more than 2000 kg that are locked or sealed should be allowed in open vehicles.

6.2.8 Communication

6.2.8.1 Domestic physical protection measures should include provision of continuous two-way radio communication or frequent telephone communication between the vehicle and the shipper, receiver, and/or shipper/receiver designee.

6.2.10 Escorts or guards

6.2.10.1 . . . if the packages, vehicle, cargo hold, or compartment are locked and sealed, frequent and periodic examination of seals together with continuous surveillance of the cargo hold when the vehicle is not in motion should be allowed in place of package surveillance.

6.3 Requirements for Category I Material (same as NRC formula quantity) Related to the Mode of Transport

6.3.4 Shipment by sea

6.3.4.2 The shipment should be placed in a secure compartment or container which is locked and sealed. Locks and seals should be periodically inspected in transit.

6.4 Requirements for Category II (less than NRC formula quantity) Material in Transit

6.4.3 Provision of locks and seals

6.4.3.1 Unless there are overriding safety considerations, the packages containing material should be carried in closed, locked vehicles, compartments, or freight containers.

However, carriage of packages weighing more than 2000 kg that are locked or sealed shall be allowed.

6.4.6 Measures after shipment

6.4.6.1 The receiver should check the integrity of the packages, locks, and seals and accept the shipment immediately upon arrival. He should notify the shipper of the arrival of the shipment immediately or of non-arrival within a reasonable interval after the estimated time of arrival at its destination.

6.4.7 Communication

6.4.7.1 Domestic physical protection measures should include provision of frequent telephone communication between the vehicle and the shipper, receiver, and/or shipper/receiver designee.

6.5 Requirements for Category III Material (less than NRC formula quantity) in Transit

6.5.2.1 Where practicable, locks and seals should be applied to vehicles or freight containers.

These recommended measures are based on the current state of the art in physical protection hardware and systems. The proposed TRANSEAVER system not only complies with IAEA's recommendations but also supplements the proposed measures. TRANSEAVER goes beyond "two-way radio communication or frequent telephone communication between the vehicle and the shipper" by providing frequent reporting without human intervention. Any deviation from a planned course or any unauthorized tampering with cargo automatically produces an Alerting Report at a command console. TRANSEAVER uses more sophisticated physical protection hardware and systems than are reflected in IAEA's recommended measures.

4.2 Inter-Governmental Maritime Consultative Organization

The Inter-Governmental Maritime Consultative Organization (IMCO), based in London, is a specialized international agency of the United Nations. IMCO is an international body set up to handle maritime matters, including issues such as improving shipping operations in international waters. This agency has adopted an international maritime dangerous goods code. As with other international organizations, specific requirements, codes, and guidelines are not enforceable and therefore serve only as recommendations. IMCO's recommended codes can be found in Appendix D.

4.3 The Nuclear Energy Agency

The Nuclear Energy Agency, an affiliation of the Organization for Economic Cooperation and Development, is in the process of preparing a study on the transport of radioactive materials. The document, entitled "Regulations Governing the Transport of Radioactive Materials," is scheduled to be available in 1981.

5.0 THE TRANSEAVER SYSTEM

TRANSEAVER is an extension of the RECOVER system being developed by ACDA. As described herein, the extension incorporates the MARISAT satellite communications system, specially selected casks and containers, a sa..llite navigational system for tracking, and sensors specially selected for protection of shipments during transit. These extensions compose a system to aic n safeguarding shipments of special nuclear materials.

TRANSEAVER is conceived as a system to protect a cargo from and to rapidly report any attempt to tamper with or divert that cargo. The system was designed to make unauthorized access difficult, to make unauthorized movement of the cargo difficult, and to detect any attempt at either of these. Unauthorized access and movement are made difficult because of the physical design of the cask and container. A variety of sensors couplec to the reporting and transmitting system detect unauthorized activities.

Therefore, the TRANSEAVER system includes the safeguarded containers and shipping casks, as well as the instrumentation, communicatiun, and monitoring systems. This expanded system scope has led to improvements not possible with a more isolated program, e.g., communications are maintained even when the containers are empty to protect against unauthorized system inspection.

5.1 System Concept

TRANSEAVER consists of the hardware and software that will enable a central facility to query the status of safeguards devices installed on nuclear shipments throughout the world using, in part, existing communications networks, as shown in Figures 5-1 and 5-2. Two options are presented; the prime difference is the Communications Interface Unit (CIU), which is added in Option 2. The TRANSEAVER system elements, which are the same as used in RECOVER, include one computer-based Remote Verification Unit (RVU) at the central facility; Portable Verfication Units (PVUs) used for installation and diagnosis; an On-Site Multiplexor (OSM) with each nuclear shipment; and, for each OSM, many Monitoring Units (MU) which are each attached to a safeguards device. TRANSEAVER elements differing from RECOVER include the Communication Terminal, the Universal Teleprinter Interface (UTI), the Navigational Terminal, TRANSIT and MARISAT satellites, and, for Option 2, the CIU. Special sensors will also be selected for TRANSEAVER.

Routine communications between an RVU and the safeguards devices will consist of polls originating at the RVU (see Figure 5-1). An RVU will place calls (either automatically or upon manual request) to each OSM. Each OSM, having previously interrogated its set of MUs, will report its data to the RVU. The data reported will include status of the proper functioning of the monitored safeguards devices, indications of the output of those safeguards devices, and status of the functioning of the OSM and MUs. All system communications except TRANSIT navigational data shall be encrypted to assure security (i.e., to prevent unauthorized knowledge of the data) and validity (i.e., to prevent unauthorized manipulation of the

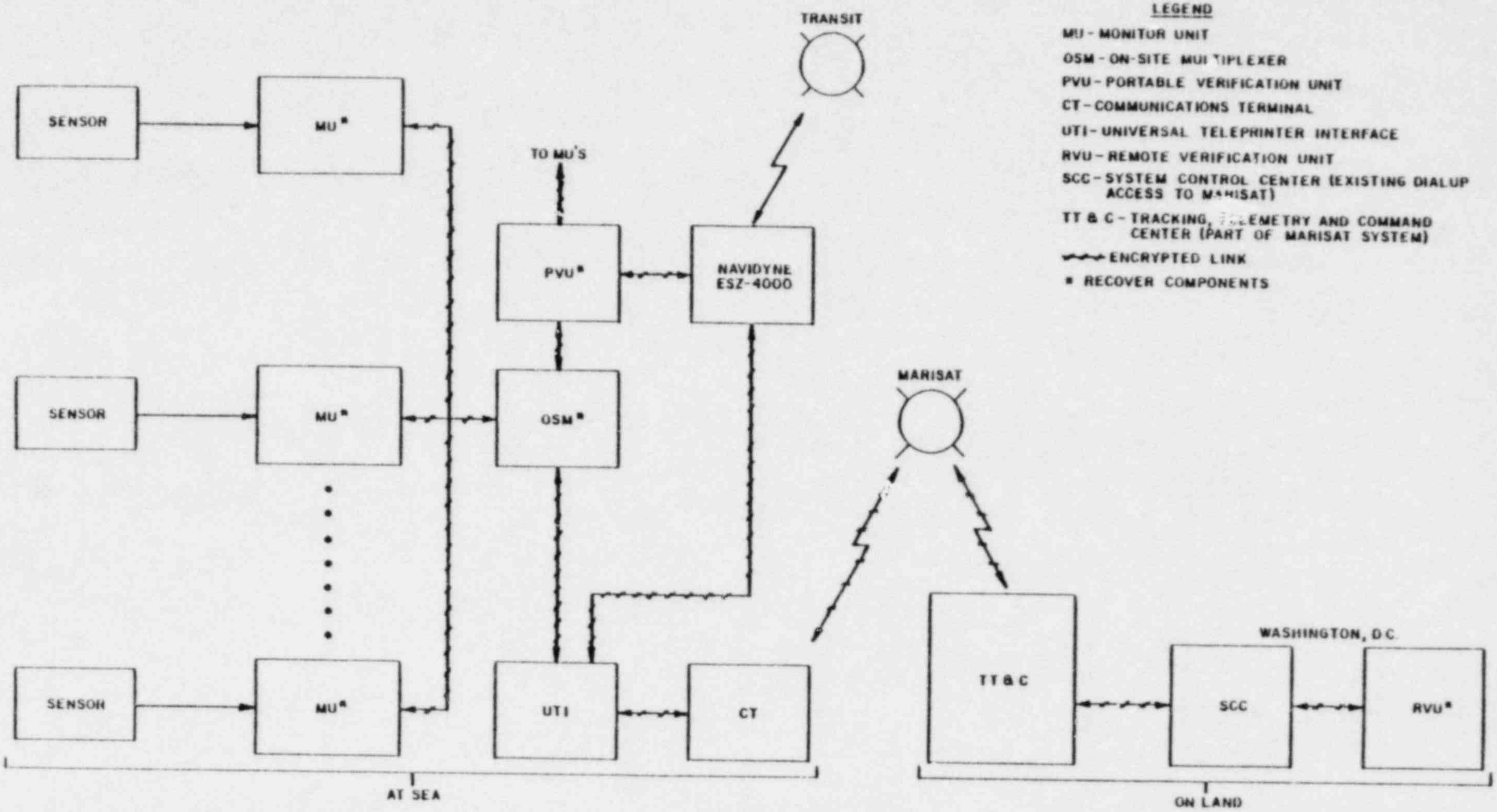
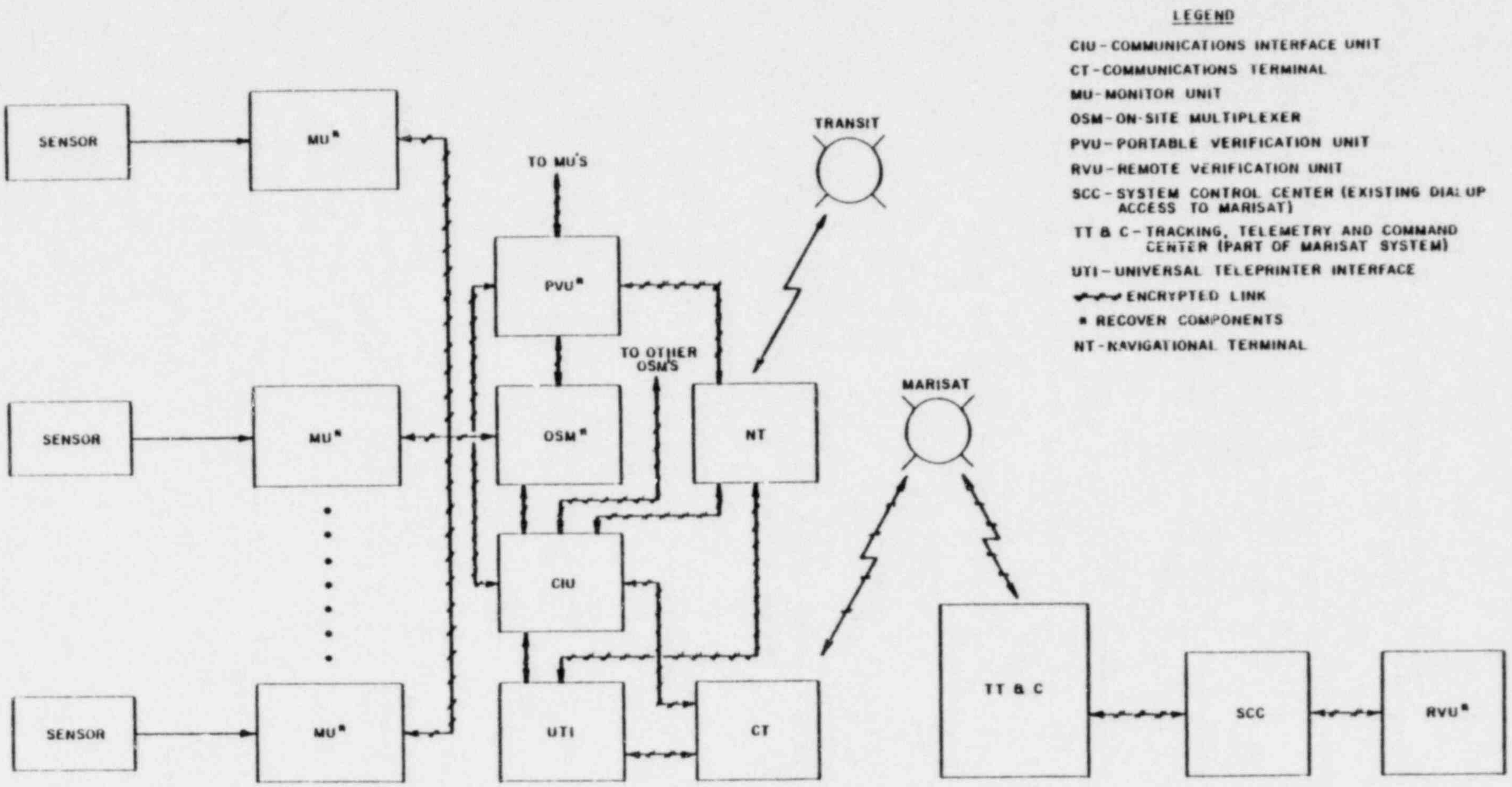

LEGEND
MU - MONITOR UNIT
OSM - ON-SITE MULTIPLEXER
PVU - PORTABLE VERIFICATION UNIT
CT - COMMUNICATIONS TERMINAL
UTI - UNIVERSAL TELEPRINTER INTERFACE
RVU - REMOTE VERIFICATION UNIT
SCC - SYSTEM CONTROL CENTER (EXISTING DIALUP ACCESS TO MARISAT)
TT & C - TRACKING, TELEMETRY AND COMMAND CENTER (PART OF MARISAT SYSTEM)
ENCRYPTED LINK
* RECOVER COMPONENTS
TRANSIT
SENSOR
MU*
SENSOR
MU*
SENSOR
MU*
TO MU'S
PVU*
NAVIDYNE ESZ-4000
OSM*
UTI
CT
MARISAT
TT & C
WASHINGTON, D.C.
SCC
RVU*
AT SEA
ON LAND

Figure 5-1 TRANSEAVER Overall System Design - Option 1 -



LEGEND

CIU - COMMUNICATIONS INTERFACE UNIT

CT - COMMUNICATIONS TERMINAL

MU - MONITOR UNIT

OSM - ON-SITE MULTIPLEXER

PVU - PORTABLE VERIFICATION UNIT

RVU - REMOTE VERIFICATION UNIT

SCC - SYSTEM CONTROL CENTER (EXISTING DIAL UP ACCESS TO MARISAT)

TT & C - TRACKING, TELEMETRY AND COMMAND CENTER (PART OF MARISAT SYSTEM)

UTI - UNIVERSAL TELEPRINTER INTERFACE

⇝ ENCRYPTED LINK

* RECOVER COMPONENTS

NT - NAVIGATIONAL TERMINAL

Figure 5-2 TRANSEAVER Overall System Design - Option 2 -

data). In addition, the system elements shall be designed to provide resistance to, and indication of, attempted physical or operational tampering.

The CIU added for Option 2 provides a threefold enhancement, is described below, and is the recommended configuration. First, to reduce operational costs and to allow more lengthy (more than one hour average) intervals to exist between RVU-to-OSM polls, the CIU would interrogate the OSM continually and initiate a call to the RVU when an alarm is discovered. In short, the CIU could call "help." This feature, though, does not preclude the RVU-initiated poll.

Second, the CIU would be able to compare navigational data with a preprogrammed route and send an alarm if the ship's course alters significantly. Allowance can be made for course changes during transit by manual input through the RVU.

Third, if more than one shipment is aboard a ship, each will have its own set of sensors, monitor units, and OSMs. The CIU will be the focal unit to which multiple OSMs communicate.

If Option 1 were used, the intelligence for the navigational comparison would reside in the RVU and the "call help" feature could be supplanted by more frequent RVU-to-OSM polls or by OSM software modification. However, multiple OSM communication to the UTI without equipment modification is not possible. During the rest of this report, Option 2, Figure 5-2, is the assumed configuration.

The hardware configuration of the CIU is essentially the same as the OSM. The software shall be developed during Phase II. Conceptual software modules and interactions are detailed in Appendix C.

To enhance the timely reporting of events, the rate of RVU polling individual OSMs and of an OSM polling individual MUs will be variable and dependent on the OSM or MU being polled. These polling rates shall be established when the OSM or MU is installed and may be altered by authorized personnel as events may warrant.

The Portable Verification Unit (PVU) shall be used locally by authorized personnel to interrogate an OSM, to establish or alter OSM operating parameters (e.g., polling rates or significant event definition), and to support the installation and checkout of TRANSEAVER hardware.

The TRANSEAVER system architecture shall be flexible to accommodate different shipment configurations and evolving requirements. Further, it shall be designed to minimize communication costs, to resist operational tampering, and to isolate TRANSEAVER system faults. Individual on-ship TRANSEAVER elements shall be designed to provide safe, reliable, simple, and nonintrusive installation and operation.

5.2 System Operation

Each shipment using TRANSEAVER will be provided with multiple sensors of varying types. Each sensor will report any alarm condition to its Monitor Unit (MU). The MUs for a given shipment will be interconnected in a daisy-chain fashion on a shared serial line; they will be polled by and report to an On-Site Multiplexor (OSM). Each shipment (defined as a single protective container) includes one OSM. Many shipments, and thus many OSMs, can be aboard a ship. The OSMs from the various shipments converge to a single, multiple-purpose Communications Interface Unit (CIU).

The CIU (1) frequently polls the OSMs. If an alarm is detected, the CIU calls through the MARISAT system and reports the alarm to the Remote Verification Unit (RVU); (2) recognizes poll requests from the RVU and responds with the current status of the connected OSMs; and (3) collects navigational data and makes comparisons with a preplanned course. Significant deviations between the two are reported as alarms. The TRANSEAVER conceptual design for the instrumentation, communication, and monitoring systems has been shown as Figure 5-2.

The RVU is the headquarters for collecting and displaying data from all monitored ships around the world. The Navigational Terminal (NT), Universal Teleprinter Interface (UTI), and Communications Terminal (CT) are on-board devices needed to communicate to the TRANSIT and MARISAT satellite systems and are discussed in more detail later. The Portable Verification Unit (PVU) initializes MUs, OSMs, and CIUs; performs checks during operation; and debugs.

5.3 System Location

Each shipment will consist of an NRC-qualified cask inside a protective container, which is mounted on a skid. The skid will be placed in a standard shipping container, as shown conceptually in Figure 5-3. The shipment is divided into four regions: Region A is between the shipping container and the protective container; Region B is within the walls of the protective container; Region C is between the protective container and the cask; and Region D is within the walls of the cask. Sensors will be selected to monitor phenomena that could occur in each region.

Certain MUs and their sensors are mounted in Region C to detect activities in Regions B, C, and D. These MUs, having several layers of tamper indication, are very secure. The shared serial data line attached to the cask provides a breakwire detector: the OSM will detect any interruption of data on this line.

Additional MUs are mounted in Region A to detect phenomena in Regions A and B. Though less secure than those in Region C, these MUs still have several layers of protection. The OSM associated with the shipment is also located in Region A.

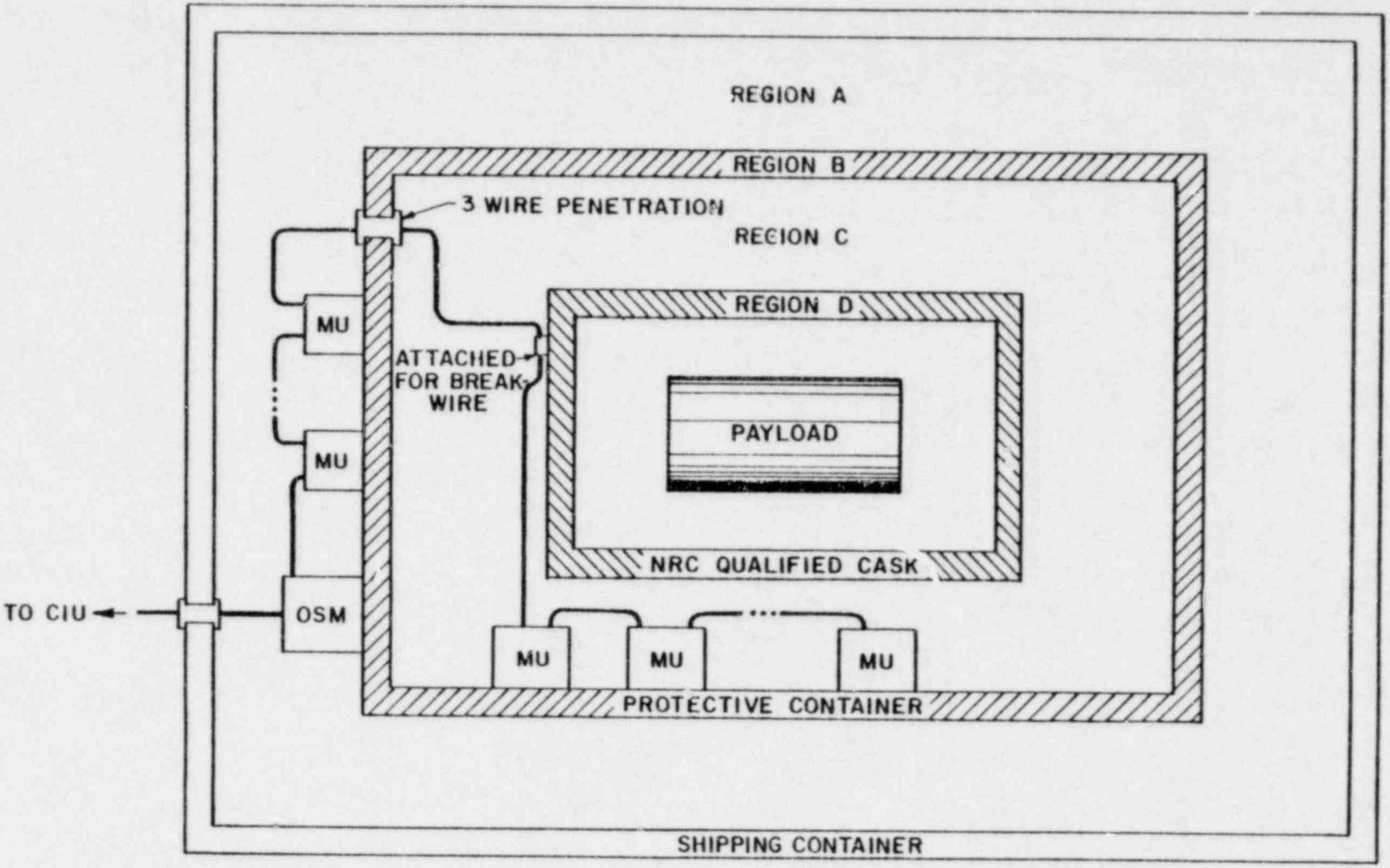


Figure 5-3 Protection Conceptual Arrangement

The prime design criteria for TRANSEAVER is security. Without significantly compromising security, the second most important design criteria is cost effectiveness. This led to the arrangement of a single CIU on a ship to minimize MARISAT communication costs and to act as a gathering point for data from all shipments (via their individual OSMs) on the ship. A single call from the RVU to the ship can acquire all pertinent data for that ship with this arrangement. Because the CIU can also call "help," the frequency of interrogation from RVU to CIU may be lengthened.

The CIU, NT, UTI, CT, and Battery System will be single units on a particular ship and will be mounted in the radio room.

The RVU will be land-based at a central location to be determined.

5.4 Non-Recover Off-the-Snelf Components

Additional components were needed to expand RECOVER's capabilities into the TRANSEAVER system; commercially available units were selected where possible. These included the UTI, the CT, and the NT.

5.4.1 Universal Teleprinter Interface (UTI)

The UTI selected is a unit by the same name produced by COMSAT General Corporation.

The UTI provides the necessary interface between the CT and the CIU. It automatically makes the proper data conversions and also can automatically transmit navigational information (on request) to the RVU if the CIU were disabled.

5.4.2 Communications Terminal (CT)

This unit communicates with the shore-based terminal via the MARISAT satellite system. It consists of a parabolic dish antenna, servo-control systems, communications electronics, and an operating console.

The unit selected is a COMSAT General Model 3055M and is compatible with MARISAT and with RECOVER components (through the UTI).

5.4.3 Navigational Terminal (NT)

The NT must obtain navigational data from the TRANSIT satellites and present that data in usable form to the UTI and CIU. As additional protection the data should be encrypted.

The unit selected is a Navidyne Model ESZ-4000. Navidyne has verbally agreed that the encryption software can be provided in this model.

6.0 SYS[illegible] SPECIAL INTERFACES

Not all the equipment for TRANSEAVL. could be provided off-the-shelf. However, the additional special interfaces are of simple design. The following sections descri[illegible] he conceptual design of these interfaces.

6.1 Sensor-to-MU Interfaces

The sensors selected for each application require special interfaces between them and the MUs. Figure 6-1 shows a typical arrangement. In Region A (the regions were defined in Figure 5-3), two types of detectors are to be used: an infrared motion detector and a capacitance proximity switch. The infrared detectors provide a simple contact closure and can be connected directly to the MU. The proximity sensor is also based on a contact closure. In addition, a two-out-of-three voting circuit that preceeds the MU helps eliminate spurious alarms.

For region B, three types of sensors are to be used: fiber optic seals, temperature sensors, and vibration sensors. The seals interface through a simple latch to the MUs. The temperature sensors are configured in two trains. In a given train, the sensors are spaced so that an attempt to cut the protective container will heat up at least two sensors. A 2-out-of-15 voting circuit helps eliminate spurious alarms. The vibration sensors are piezoelectric devices, which require the signal to be amplified, clipped, and compared to a threshold before being input to the MU.

Pressure sensors and proximity sensors are used for Region C. The protective container will be pressurized and will alarm if depressurized. The pressure sensors are interfaced to the MU through a two-out-of-three voting circuit. The proximity sensor, which is tuned between the cask and shipping container, also uses a two-out-of-three circuit.

Finally, Region D uses fiber optics, temperature sensors, and vibration sensors. The configuration of these sensors is similar to previously described ones, except that temperature sensors use a two-out-of-eight voting circuit.

These interfaces are a typical shipment configuration, and all MUs are daisy-chained to a single OSM. Other arrangements using the same basic components are feasible.

6.2 Fiber Optic Seal Interface

The fiber optic seal can interface to the MU through the latch circuit shown in Figure 6-2. The ACK signal, provided from the MU, latches the fiber-optic data bits to yield MU input bits SD0 through SD7. The Texas Instruments MA723M chip provides the proper supply voltage level.

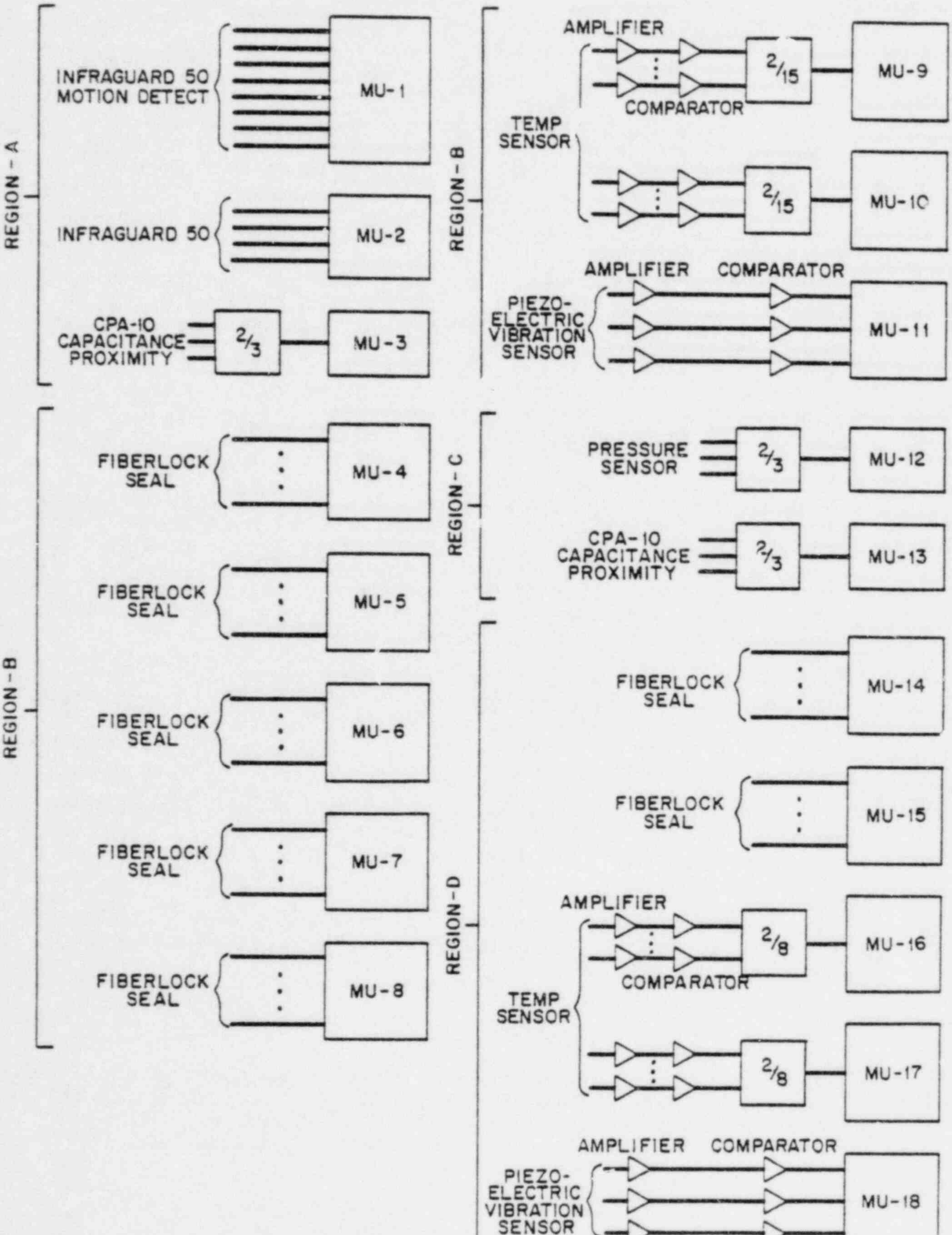


Figure 6-1 Typical Mu-Sensor Arrangement

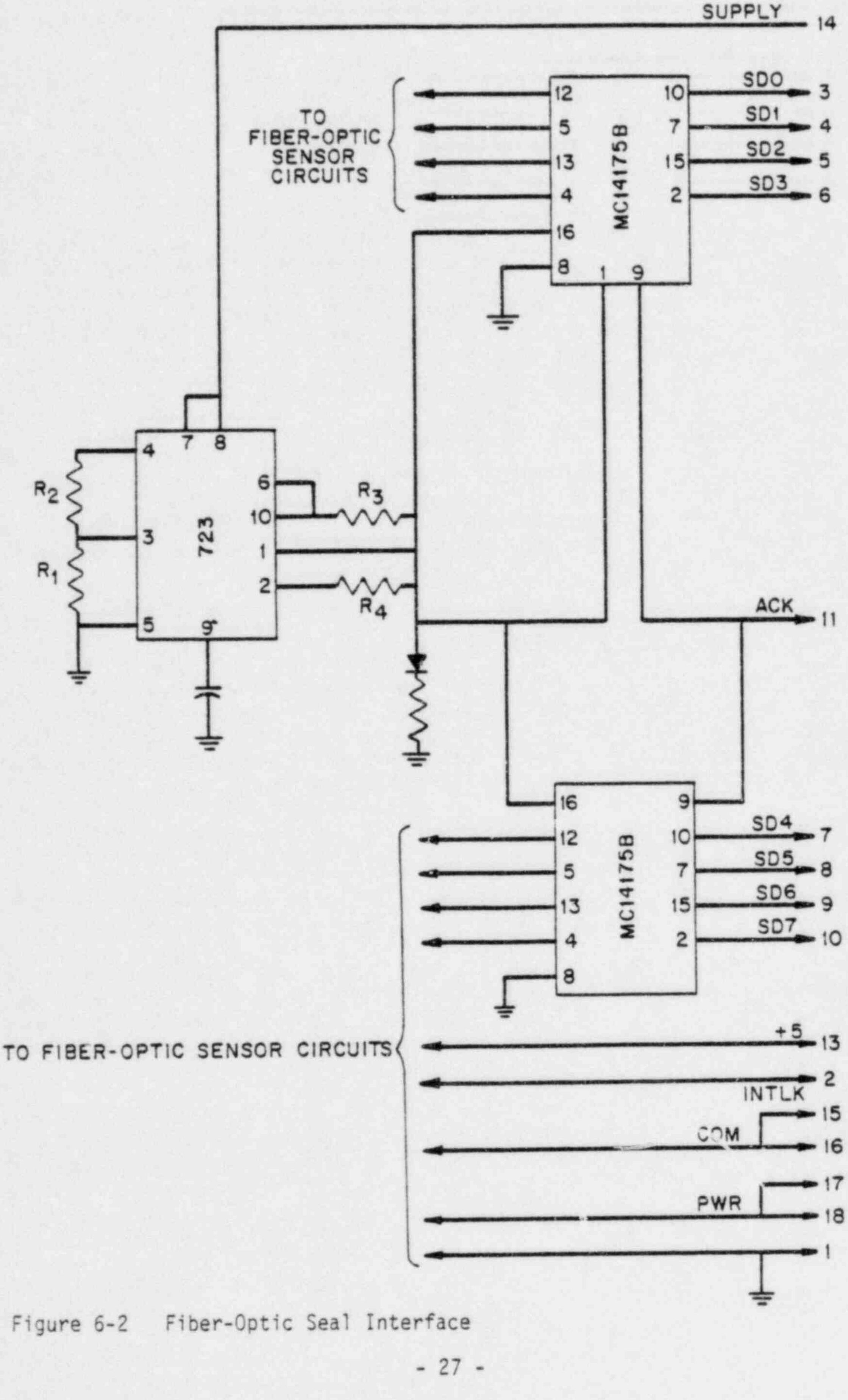


Figure 6-2 Fiber-Optic Seal Interface

6.3 X-Out-of-N Voting Circuit

Figure 6-3 shows the conceptual design of an X-out-of-N voting circuit. N is restricted to be less than or equal to 15. The value of X is set at the switch inputs to the Texas Instruments SN5485. N is set by using N inputs out of the 15 possible, A1 through A15, while leaving the unused inputs open.

The Signetics N8268s will add the three bits at their input to give a two-bit binary representation of the sum. The Signetics N8260s are four-bit adders configured so the input to the 5485 is a four-bit binary representation of the total number of 1's present at A1 through A15. The 5485 compares this total with the binary switch setting and forwards a signal for alarm if the total is greater than the binary switch setting.

6.4 Communications Interface Unit (CIU)

The CIU operates somewhat like the OSMs. The most cost effective approach to designing the CIU includes some minor hardware modifications to the OSMs (originally RECOVER components) and considerable software modifications so these units operate as described in Section 5.2. These design details will be provided during Phase II.

6.5 Amplifier and Comparator Interface

The circuitry of Figure 6-4 can provide the amplification, filtering, and comparing as needed for certain interfaces. The components selected are compatible with the signal power supply voltage that is available. Resistance values can be selected to match the gain to the sensor. The comparator threshold level is adjustable through a potentiometer.

6.6 Power Circuitry

Power for all TRANSEAVER modules may be supplied by two sources, normal and backup. In the normal operating mode, power will be supplied by the ship's vital bus (117 V AC). If the ship's vital bus is lost, the TRANSEAVER uninterruptible power supply (UPS) will switch to a bank of batteries to continue power. This DC power will be converted to 115 V AC by an inverter in the UPS and will continue to supply the power requirements of TRANSEAVER for one hour. Transfer to battery power is completely automatic and will not cause interruption or discontinuity in system security.

The major power drain is for the antenna positioning motors, not the electronics. Battery supply of this amount of energy is feasible only for short duration hauls. However, the UPS proposed would provide essentially the same feature by:

(1) Battery backup in case of power failure or tampering.

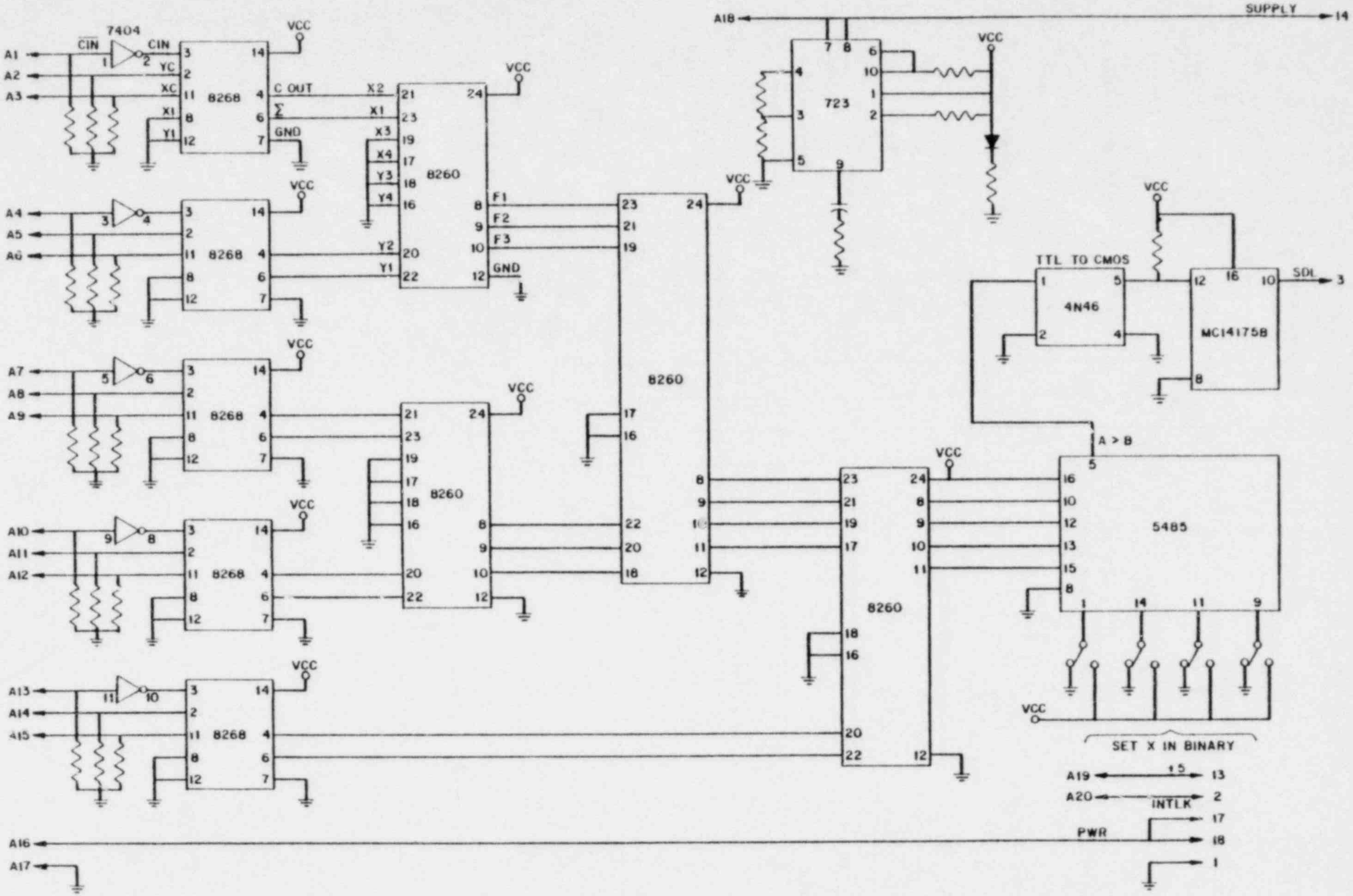


Figure 6-3 X-Out-of-N Voting Circuit

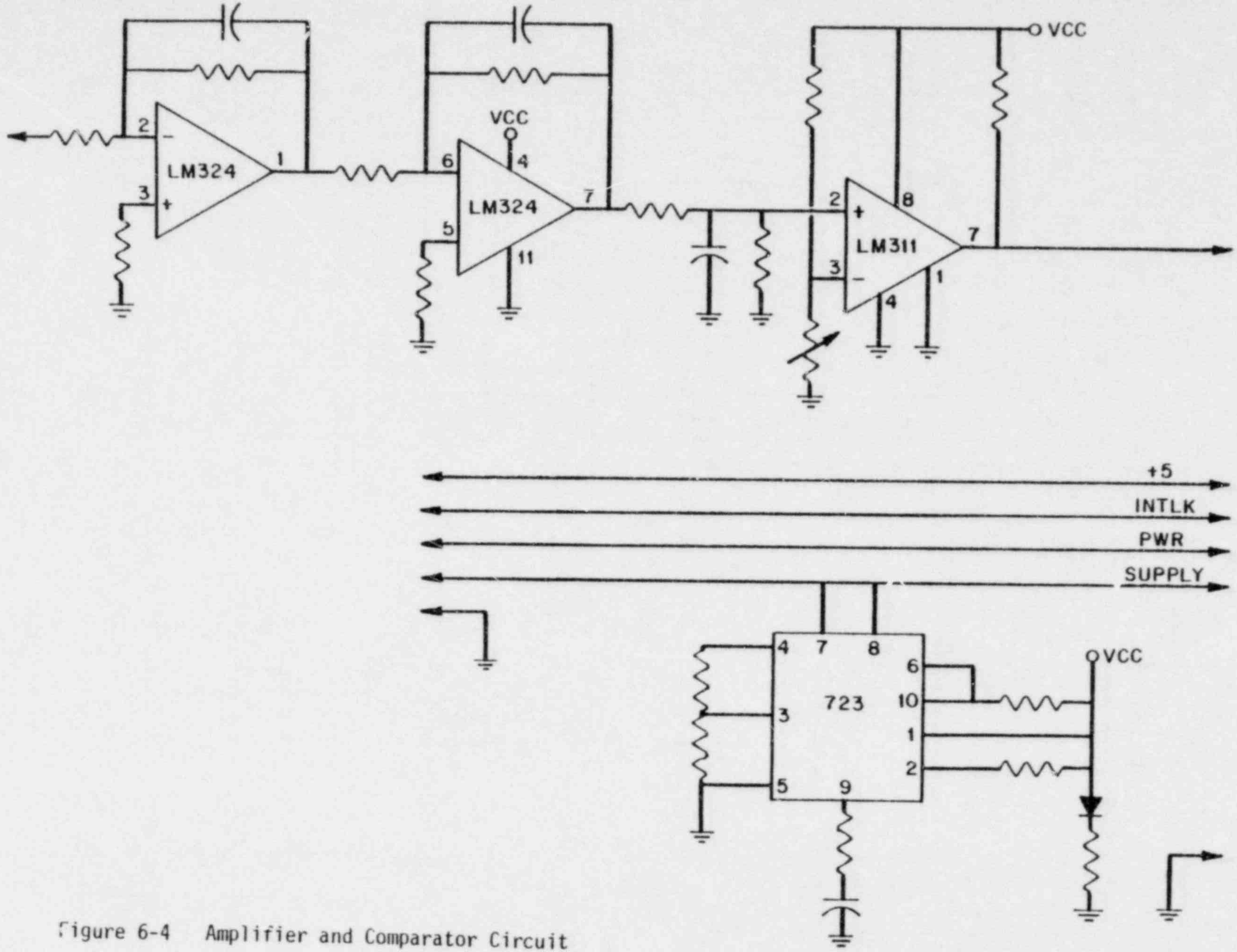


Figure 6-4 Amplifier and Comparator Circuit

(2) UPS protection from tampering.

(3) Protection from shorting the power source.

If the loss of the vital bus lasts more than ten minutes, the CIU will initiate an automatic distress call. A loss of the vital bus for more than ten minutes is considered either an act of sabotage or a genuine indication of a ship in distress. In either event the UPS can power TRANSEAVER for one hour, which allows placement of a distress call via the CT. Additionally, both the OSM and MU use integral batteries to protect their memories. The OSM and MU, after operating normally on internal battery for a short time, automatically reduce power consumption to a base level required to protect their memories.

Power requirements are shown on Table 6-1. The power supply block diagram is Figure 6-5. The UPS output breaker is equipped with a timer and auto-reclosing feature to continue service afte·· a momentary fault and to enhance system reliability.

6.7 Fiber Optic Link Option

Using fiber optics for the data link between the OSM and MUs would increase security: undetected access to this link would be very difficult and the breakwire concept would be more effective. However, this portion of the electronics is already heavily protected and the relatively high cost of fiber optics for a large number of MUs is not attractive. Therefore, this option is not recommended.

TABLE 6-1

TRANSEAVER LOAD CHART

Item	Number Each	V.A.* Required/Unit	V.A.*
Monitor Unit (MU)	30	1	30
On-Site Multiplexor (OSM)	10	25	250
Universal Teleprinter Interface (UTI)	1	1,850	1,850
Communications Terminal (CT)	1		
Communications Interface Unit (CIU)	1	100	100
Navigational Terminal (NT)	1	120	120
Charging Current to MU	30	.05	1.5
Charging Current to OSM	10	25	250
TOTAL	———	———	2,602

* V.A. is defined as volts times amps. Actual wattage would be established by including a power factor.

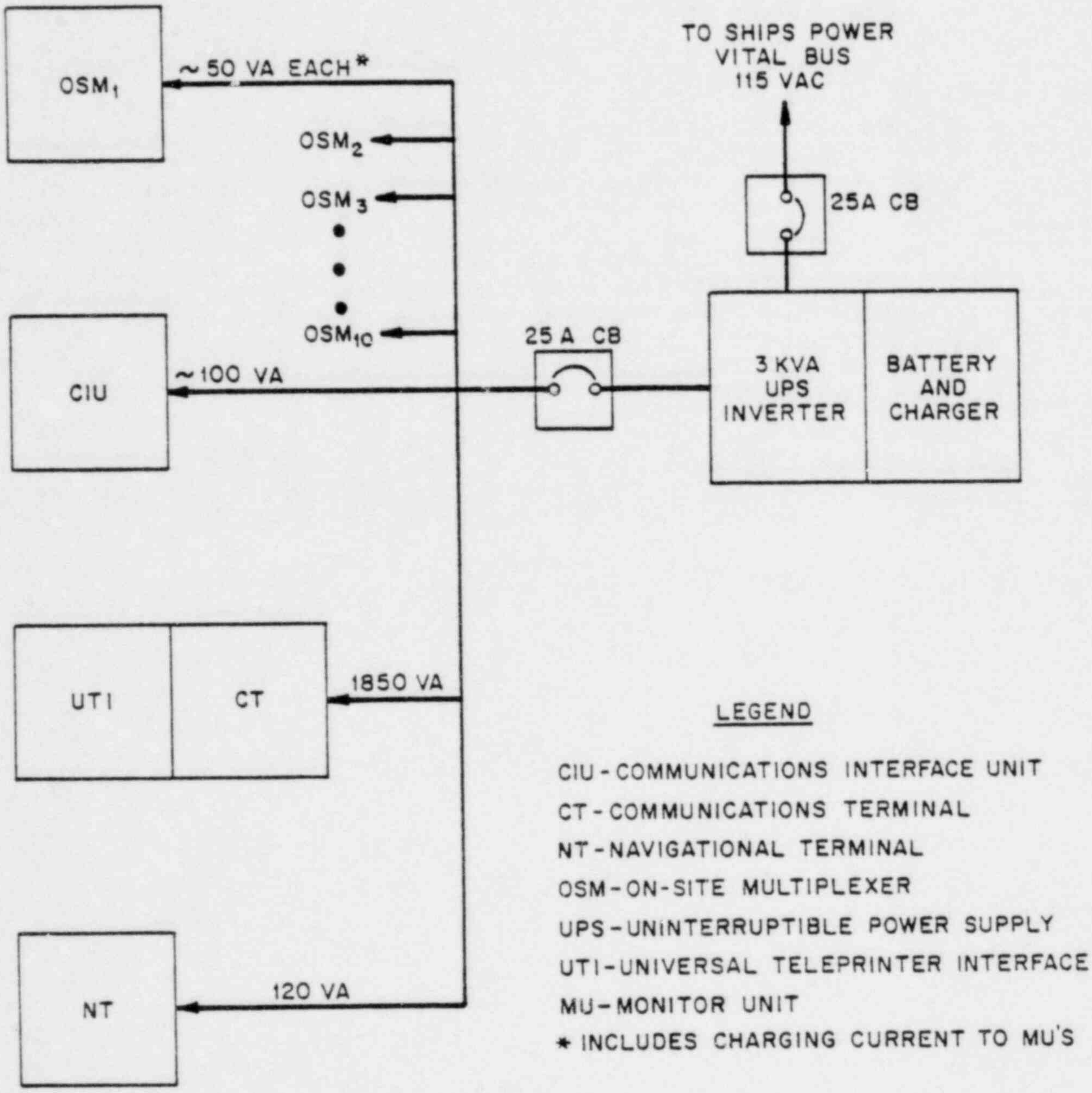

TO SHIPS POWER
VITAL BUS
115 VAC
25A CB
OSM$_1$
~50 VA EACH*
OSM$_2$
OSM$_3$
OSM$_{10}$
25 A CB
CIU
~100 VA
3 KVA
UPS
INVERTER
BATTERY
AND
CHARGER
UTI
CT
1850 VA
NT
120 VA
LEGEND
CIU - COMMUNICATIONS INTERFACE UNIT
CT - COMMUNICATIONS TERMINAL
NT - NAVIGATIONAL TERMINAL
OSM - ON-SITE MULTIPLEXER
UPS - UNINTERRUPTIBLE POWER SUPPLY
UTI - UNIVERSAL TELEPRINTER INTERFACE
MU - MONITOR UNIT
* INCLUDES CHARGING CURRENT TO MU'S

Figure 6-5 Power Schematic

7.0 PROTECTION OF THE ELECTRONIC GEAR

The RECOVER system employs tamper indication/resistance measures on its components and interfaces. The components added to RECOVER to form TRANSEAVER must also feature similar measures. Tables 7-1 and 7-2 list the measures to be taken.

The CIU will contain self-protection and system protection in the same manner as the OSMs.

The communications equipment will use the capabilities of the system, where feasible, for protection. Six categories are identified in Table 7-1: Power Status Sensing/Reporting; Memory Protection Upon Power Off; Physical Penetration Detection; Critical Memory Erasure Upon Penetration, Detect and Record Abnormal Opening of Housing; and Detect and Record Normal Opening of Housing. Memory protection will be via battery backup. Critical memory erasure upon penetration will provide destruction of such sensitive memory as encryption keys, special software, etc. The remaining four categories of protection will be provided by monitoring the communications gear with sensors and tying them into TRANSEAVER via MUs.

TABLE 7-1

REQUIRED TAMPER INDICATION/RESISTANCE MEASURES - SYSTEM ELEMENT

	System Element						
Requirement	Monitoring Unit	On-Site Multiplexor	Communication Interface Unit	Portable Verification Unit	Remote Verification Unit	Communications Equipment	Remarks
PHYSICAL MEASURES							
Power Status Sensing/ Reporting	Yes	Yes	Yes	No	N/A	Yes	Detect disconnect
Memory Protection Upon Power Off	Yes	Yes	Yes	Yes	Yes	Yes	Survive power loss
Protective Potting	Total**	Selected Modules	Selected Modules	Selected Modules	No	No	Encryption keys protected
Physical Penetration Detection	N/A**	Yes	Yes	Yes	No	Yes	Detect intr[illegible]n
Critical Memory Erasure Upon Penetration	N/A**	Yes	Yes	Yes	No	Yes	Protect encryption keys
Detect and Record Abnormal Opening of Housing	N/A**	Yes	Yes	Yes	No	Yes	Detect intrusion
Detect and Record Normal Opening of Housing	N/A**	Yes	Yes	Yes	No	Yes	Record rate of inspection
OPERATIONAL MEASURES							
Record Unsuccessful Transaction* Attempt	Yes	Yes	Yes	Yes	Yes	No	Detect possible intruder
Record Successful Transaction* Activity	Yes	Yes	Yes	Yes	Yes	No	Record rate of use

TABLE 7-1, Continued

	System Element						
Requirement	Monitoring Unit	On-Site Multiplexor	Communication Interface Unit	Portable Verification Unit	Remote Verification Unit	Communications Equipment	Remarks
Limit Transaction* Rate	Yes (1 per sec)	Yes (1 per 10 sec)	Yes (1 per 5 min)	Yes (after 3 unsuccessful attempts)	Yes (after 3 unsuccessful attempts)	N/A	Protect from forced cycling or tie-up
Record Invalid Transaction* Responses	N/A	Yes	Yes	Yes	Yes	N/A	Detect possible intruder
Log Transaction* and Activities	N/A	N/A	N/A	Yes	Yes	N/A	Record rate of transactions
Prohibit Changing of Logs and Historical Data	N/A	N/A	N/A	Yes	Yes	N/A	Protect records

* A transaction is a poll for the CIU, OSM, and MU or a logon for the RVU/PVU.

** MU will be potted thereby requiring physical destruction to penetrate.

TABLE 7-2

REQUIRED TAMPER INDICATION/RESISTANCE MEASURES - SYSTEM INTERFACES

Requirement	MU-Sensor	MU-OSM	MU-PVU	NT-PVU	NT-CIU	NT-UTI	UTI-CT	OSM-PVU	OSM-CIU	CIU-RVU	PVU-RVU	PVU-Inspector	RVU-Inspector
PHYSICAL MEASURES													
Detect Physical Disconnect	Yes	Yes	No	No	No	No	Yes*	No	No	Disconnect Part of Normal Operations	No	N/A	N/A
OPERATIONAL MEASURES													
Encrypt Communications	No	Yes	Yes	Yes	Yes	Yes	Optional	Yes	Yes	Yes	No	No	No
Password Access Protection	No	Optional	Optional	Optional	No	No	Optional	Optional	Optional	Optional	Optional	Yes	Yes

*Common enclosure

8.0 SELECTION OF MONITORED SENSORS

Monitored sensors are selected and configured so as to detect intrusion into any part of the defined cargo space. Nine criteria condition the design of the sensor system. These criteria require consideration of relevant safeguards issues, of sensor and cargo-space parameters, and of several related items.

A special condition imposed on the Phase I effort is that the cargo shall be strategic special nuclear material (SSNM), i.e., strategic quantities of highly enriched uranium (HEU) and/or plutonium (Pu). This condition has a significant impact on the cargo configuration (and hence on the design of the sensor system) for two reasons:

(1) SNM casks are relatively small and unprotected and therefore could be easily enclosed in a substantial security container.*

(2) According to the United States Code of Federal Regulations, Title 10, Chapter 1, Part 73, Section 73.26, Paragraph (1) Shipment by Sea, Subparagraph (1), "Shipments shall be made only on container-ships. The strategic special nuclear material container(s) shall be loaded into exclusive use cargo containers conforming to American National Standards Institute (ANSI) MH5.1 or International Standards Organization (ISO) 1496."

These two considerations lead to a cargo configuration as depicted in Figure 8-1. All dimensions are approximate since the detailed mechanical design will take place during Phase 2. The casks shown are of a specific type; other arrangements are possible. A closed van cargo container (ANSI MH5.1.1M-1979) is the outer cargo boundary; the van's load consists of (probably two) steel security containers, locked and sealed; within each security container is a small number of licensed casks, each containing its SNM payload. This cargo configuration is the physical starting point for the design of the sensor system.

The proximity sensors require the protective container to be electrically insulated from the shipping container. Wood in the skid construction to hold the protective container in place serves as electrical insulation.

An instrumentation housing forms an integral part of the protective container, which provides protection for the electronic equipment and allows the equipment to protect itself.

*It has not yet been determined whether the larger, heavier, and thicker casks used for nuclear (spent) fuel and radwaste require security containers.

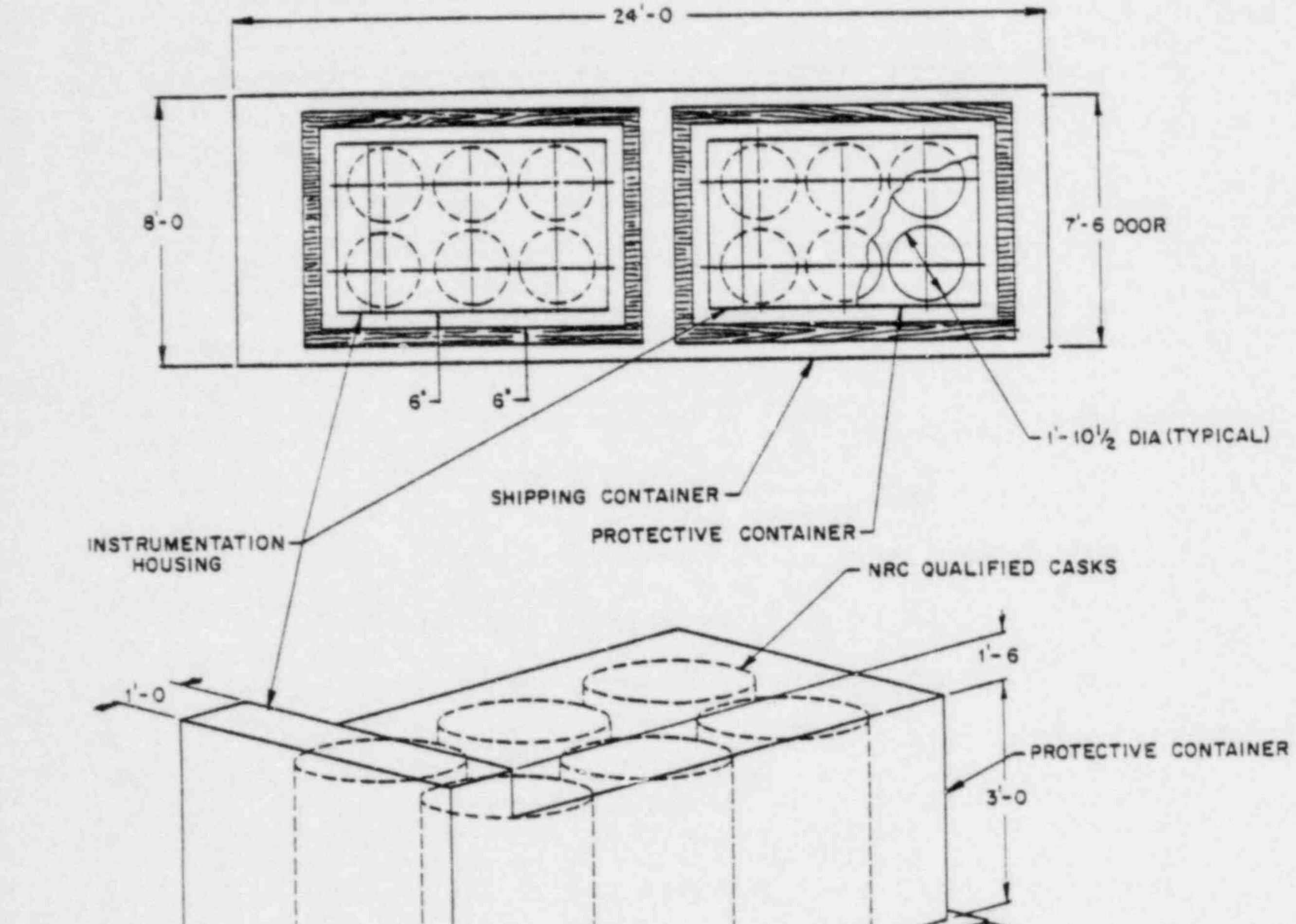


Figure 8-1 Shipment Construction

8.1 Basic Criteria

The primary goal in the selection process was to select sensors that could indicate whether the cargo is intact and whether the cask integrity has not been compromised. The selection philosophy included but was not limited to consideration of the following criteria:

(1) Compatibility with RECOVER, MARISAT, and the cask

(2) Survivability and power requirements

(3) Level of security provided

(4) Commercial availability

(5) Reliability

(6) Cost

(7) Tamper-resistance/indication

(8) Effect of sensor installation on cask licensability

(9) Impact on transportation operations

The interpretation of two phrases in the first sentence of the Task 4 Statement of Work deserves comment. The phrase "cargo is intact" is taken to mean that the cargo container has not been removed from its shipping location. The phrase "cask integrity has not been compromised" is assumed to mean that the integrity of the security container has not been compromised nor has an effort to penetrate it been detected.

All nine selection criteria bear on the actual sensor selection process; however, several of the criteria also relate to matters that require separate discussions. Criterion 7, Tamper-Resistance/Indication, requires clarification of how the sensors are protected from, and give indication of, efforts to neutralize their intended functions. Criterion 8, Effect of Sensor Installation on Cask Licensability, requires clarification of this issue. Criterion 9, Impact on Transportation Operations, also needs to be addressed.

The other criteria relate directly to the sensor selection process: Criteria 1, 3, and 8 bear strongly on the sensor locations and configurations while Criteria 2, 4, 5, and 6 assist in the optimal selection of actual hardware. Criteria 1 and 7 are also kept in view at this point.

Sensors are selected by adapting standard intrusion detection techniques to the particular physical conditions existing in the vicinity of each cargo containment barrier.

8.2 Sensor Types/Location

A sensor type/location matrix yielding adequate security is derived by considering which types of sensors are most effective at each potential location. Insofar as possible, two different sensor types are provided at each location.

Table 8-1 lists the types of sensors that were considered for use at various locations in the Phase I TRANSEAVER cargo configuration.

Figure 8-2 shows schematically the locations where sensors can be placed. Table 8-2 is a matrix which shows the sensor types that were selected for each location. These selections were made based on the criteria in Section 8.1 and also on the following considerations:

(1) Electronic remote-monitorable seals should be used at each normal access point so as to guard against collusion between an adversary and an insider.

(2) The space between the closed van and the security container allows intrusion detection by means of motion detectors.

(3) The security container can be electrically insulated from the closed van, and a proximity detector can be used to detect approach to the security container as a backup to the motion detectors.

(4) The space between the security container and the SNM casks is pressure-isolated from the exterior of the security container. Therefore, the interior of the security container can be evacuated or pressurized, and a pressure sensor will detect penetration.

(5) A single cable connects the RECOVER Monitor Units (MUs) (which are inside the security container) to the On-Site Multiplexor (OSM) (which is mounted on the outside surface of the security container). This cable can be secured to the outside of each SNM cask so that removal of any cask will require either breaking of the cable (which generates an alarm) or extensive cutting of the cask's steel shell (which takes time and energy at a point when other alarms are almost certainly active).

Having selected the sensor types and locations, it is now necessary to configure each type of sensor for adequate coverage and reliability. This can be done best if the specifications are known for each sensor type. The next section therefore summarizes the specifications of the selected sensors.

TABLE 8-1

TYPES OF SENSORS CONSIDERED FOR TRANSEAVER

1. Motion detectors:
   - a. Ultrasonic
   - b. Microwave
   - c. Passive IR (infrared)

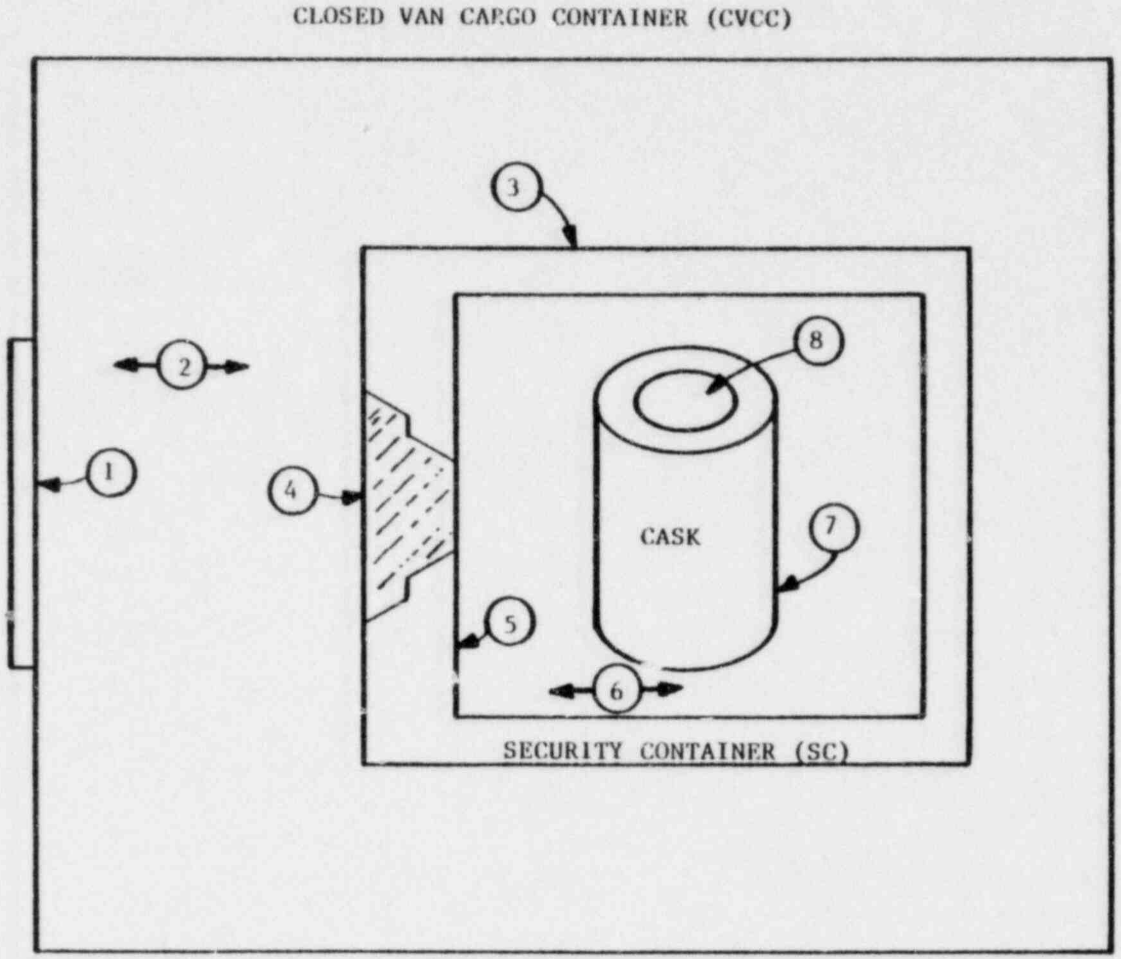
2. Penetration detectors:
   - a. Electronic remote-monitorable seal (ERMS)
   - b. Magnetic switch
   - c. Infrared beam
   - d. Proximity (capacitive)
   - e. E-field
   - f. Breakwire
   - g. Vibration
   - h. Temperature
   - i. Pressure
   - j. Strain

TABLE 8-2

MATRIX OF SENSOR TYPES/LOCATION

	Sensor Type						
Location	1. Passive IR (motion)	2. ERMS (seal)	3. Proximity (capacitive)	4. Vibration	5. Temperature	6. Pressure	7. Breakwire
1. Door of CVCC*		X					
2. Space between CVCC and SC*	X						
3. Outer surface of SC			X				
4. Door of SC		X					
5. Inner surface of SC				X	X		
6. Space between SC and Cask						X	
7. Outer surface of Cask							X
8. Port of Cask		X					

*CVCC = Closed van cargo container; SC = Security Container.



LOCATION

1. Door of CVCC
2. Space between CVCC and SC
3. Outer surface of SC
4. Door of SC
5. Inner surface of SC
6. Space between SC and CASK
7. Outer surface of CASK
8. Port of CASK

Figure 8.2 Possible locations for monitorat!e sensors.

8.3 Sensor Specifications

The selection of specific manufacturers' models for each sensor type should be done competitively on the basis of criteria 1, 2, 4, 5, 6, and 7 of Section 8.1. However, because of the brevity of the Phase I effort, the results include only the identification of one acceptable model for each sensor type. The detection specifications for each of these models are listed in Table 8-3, where each model is also identified by sensor type and manufacturer.

8.4 Sensor Configurations

This section discusses each selected sensor type in terms of the number of units to be used and the positioning of each unit. The basic criterion for a decision is the optimization of the cost/benefit considerations. Subcriteria are (1) adequate coverage of the region to be protected, (2) acceptable reliability through redundancy and voting, and (3) dollar cost for purchase and installation of multiple units.

Redundancy will be used where cost and space allow if the reliability of individual units is not high, either in responding to valid stimuli or in avoiding false alarms. When redundancy is used, the preferred arrangement will be three units replacing one, with two-out-of-three voting required for an alarm.

All sensor units are to be mounted in or on the security container (or its attached pallet) so that the security container, pallet, and sensors are transported as a single unit. This arrangement also enhances security by allowing all wiring associated with the sensors to be routed inside of the security container.

8.4.1 Passive IR Motion Detectors

These detectors monitor motion in the space around the security containers inside the closed van. As seen in Table 8-3, each detector covers the volume within a 70° cone, up to 35 ft from the detector on the circumference of the cone, and up to 50 ft on the centerline of the cone. The space around each security container can be adequately covered by mounting three IR motion detectors at each corner of the security container, aiming the axis of the sensing cone for each unit along the diagonal of one of the three adjacent container faces, and positioning each axis 35° from its respective face.

As there are eight corners on a security container, this approach requires 24 detectors for each container. This number would be reduced if the detectors were mounted on the inside of the closed van, but this alternative is not sufficiently secure: the back of each detection unit could then be accessed from outside the van and the detector wiring manipulated.

TABLE 8-3

DETECTION SPECIFICATIONS FOR SENSOR MODELS

	Sensor Type	Manufacturer	Model No.	Detection Specifications
1.	Passive IR motion detector	The Mosler Safe Co.	IR-50S	Range: 50 ft on center axis, 35 ft on edge of 70° cone.
2.	ERMS (seal)	The Fiber-Lock Corp.	Mark II, with monitor	On order. (Alarms on change of intensity or timing of light pulses.)
3.	Proximity detector	The Mosler Safe Co.	AL-26	Handles 6000 pF load.
4.	Vibration detector	Endevco	2260A-250 & 7741	Adjustable trip level.
5.	Thermal switch	Sundstrand Data Control	M556T 180B200	Close at 200°F (temp. rise). Open at 180°F (temp. fall).
6.	Vacuum switch	Pressure Controls, Inc.	V-10	1 atm. differential pressure, nominal. Adjustable.

The suggested arrangement of 24 detectors per security container involves enough units and enough overlap of coverage that the reliability of the motion sensor configuration is acceptable. This unit also has a low enough false alarm rate that voting is not required.

8.4.2 ERMS (seal)

The electronic remote-monitorable seals are quite expensive and are also acceptably reliable, being made of all solid-state electronics with quality control. Therefore, one seal for each normal access is sufficient. Normal access requires three seals: one each for the closed van, the security container, and the SNM cask.

8.4.3 Proximity Detector

The capacitive proximity detector is essentially a single sensor system since the security box itself is one plate of the sensing capacitor and the closed van is the other plate. However, redundancy can be provided in the associated electronics. Three signal processing units will be used, with two-out-of-three voting required for an alarm.

8.4.4 Vibration Sensor

One unit attached to the inside of the security container will perform the desired function. However, for acceptable reliability, three units will be mounted, and two-out-of-three voting will be required for an alarm.

8.4.5 Temperature Sensor

To detect a local temperature increase in any part of the security container, enough thermal switches must be used so less than two feet exists between switches or about 15 switches per container. For reliability, two independent sets of 15 switches will be mounted inside each security container, and at least two switches from at least one set must operate to generate an alarm.

8.4.6 Pressure Sensor

The vacuum switch will operate when the gas-tight seal on the security container is violated either by opening the container or penetrating it. One switch will perform the function, but three will be used for reliability, with two-out-of-three voting for protection against false alarms.

8.5 Related Considerations

Several matters not discussed separately deserve special consideration and are treated here.

8.5.1 Security of the Sensors

Sensors are protected from tampering by their locations and by the security of the communications and power links.

Considering a closed van cargo container with its cargo as a unit, the only component of the associated TRANSEAVER security equipment accessible from outside the closed van is the electric cable which carries power and data between the van and the communications processor. This cable is monitored by the communications processor so that tampering with the cable will generate an alarm in the processor. In this way, the inputs to and outputs from the sensors associated with the security container are secured against undetected tampering. In addition, steps will be taken to protect the cable from tampering, insofar as this is possible in the shipboard environment.

The monitored sensors themselves are both tamper-resistant and protected from undetected tampering by the manner in which they are used in the cargo configuration. None of the sensors, nor any of their associated wiring (inside the closed van), can be accessed without penetrating the protected regions, i.e., the interior of the van and the security container shell. So the sensors are self-protecting in the same way that they protect the cargo.

The electronic remote-monitorable seals are, of course, inherently tamper-resistant and tamper-indicating.

8.5.2 Flexibility of the Design

An important question is how readily the configuration of sensors developed can be adapted to variations in all of the important variables, e.g., protection level, cargo material.

8.5.2.1 Flexibility vs Protection Level

The level of protection has not been discussed in general terms. One conclusion is that the total system should be made as secure and reliable as possible, consistent with the applicable constraints. In addition, the sensor selection and configuration processes maximized the protection that could be achieved without producing an unwieldy design.

For these reasons, the original barrier/sensor configuration can be called a maximum protection design. Therefore, consideration here will be limited to a reduction of the protection level and, for simplicity, to what might be called a minimum protection design.

The minimum protection design that is recommended uses the same security container but eliminates certain of the sensors. The recommended minimum protection design is defined by Table 8-4: Matrix of Sensor Types/ Locatiors for the Minimum Protection Design. The sensor configuration for each type of sensor in the minimum protection design is the same as for the maximum protection design.

8.5.2.2 Flexibility vs Cargo Material

The cargo specified for Phase I TRANSEAVER is special nuclear material. The most likely alternative cargo that might use the seagoing TRANSEAVER system is nuclear spent fuel. The question therefore arises as to whether or not the sensor design already discussed is readily adaptable to use with spent-fuel cargo.

This question appears difficult and has not been pursued far enough to allow a definitive answer. However, the more significant considerations can be stated. First, a decision must be made whether to enclose a large, heavy, thick cask, such as is used with spent fuel, in an external security container or to work with the cask itself as the security container.

When that issue has been decided, an adequate sensor subsystem design can be conceived. Finally, a comparison of such a design with the Phase I TRANSEAVER design can be made and the adaptability of the Phase I design for use with the spent-fuel cargo evaluated.

The decision whether to use an external security container justifies a rather thorough examination of the two alternatives, since either approach will be expensive and would probably set an economically significant precedent.

A similar, but not identical, sensor design is anticipated for the external security container. If a spent-fuel cask is used as a security container, the sensor design is less predictable because of the inherent characteristics of such casks and because of the likelihood that different cask designs may require modifications to any basic sensor subsystem design.

8.6 Impact on Cask Certification

Any packages manufactured for the purpose of transporting radioactive materials must meet the requirements of applicable federal regulations. Packages (or casks) intended for commercial transportation of special nuclear material (SNM) are licensed (or certified) by the U.S. Nuclear Regulatory Commission (NRC).

TABLE 8-4

MATRIX OF SENSOR TYPES/LOCATIONS FOR THE MINIMUM PROTECTION DESIGN

	Sensor Type			
	1. ERMS (seal)	2. Proximity (capacitive)	3. Vibration	4. Temperature
Location				
1. Door of CVCC*	X			
2. Outer surface of SC*		X		
3. Door of SC	X			
4. Inner surface of SC			X	X

*CVCC = Closed van cargo container; SC = Security Container.

The NRC certifies casks based on a Safety Analysis Report that delineates the characteristics of the cask, the cask's cargo, and the conditions under which the cask will be used. Departure during use from any of the conditions under which a cask is originally certified can only be done by obtaining NRC review and approval of the special conditions.

To avoid the scheduling uncertainties and cost increments associated with NRC review of the SNM casks used with the Phase I TRANSEAVER cargo, the sensor selections and installations will not violate any conditions in the existing cask certifications. Therefore, the intended attachment of the TRANSEAVER power/data cable to the licensed SNM casks must conform to this requirement.

Also, if a spent-fuel cask should be used as a security container, rather extensive modifications to the cask would have to be performed, and recertification would probably be necessary.

8.7 Impact on Transportation Operations

Use of the TRANSEAVER system as an overlay on existing transportation methods will surely have a significant impact on transportation operations. However, the issue is restricted to the impact of the sensor subsystem on transportation operations.

This impact will be minimal in the Phase I Cargo Configuration because of the requirement to use a closed van cargo container for shipments of strategic special nuclear material. This requirement exists irrespective of whether the security container and associated sensor subsystem are in the van.

In addition, the closed van will be sealed whether or not the TRANSEAVER equipment is inside. The only difference between closed vans used with and without the TRANSEAVER system will be that each van with a TRANSEAVER-protected cargo will have a power/data cable between itself and the communications processor for the ship. The routing and connecting of these cables during loading and their disconnection and proper storage during unloading are the only additional tasks that will be required.

9.0 SELECTION OF SHIPPING CASKS

Using the NUREG 0383, Revision 2, Volumes 1 and 2, (October 79) Cask Survey, protective containers which are amenable to use with the TRANSEAVER System were reviewed. Selection criteria for casks included, but were not limited to, the following: access denial features, availability; cost; effect of required sensors on licensability; and applicability to a wide range of cargos.

Review of the package description in NUREG 0383 indicated that the casks most likely to find use in TRANSEAVER applications fall into two categories: (1) large, heavy, lead-shielded casks designed for nuclear fuel or radwaste, and (2) small, light, unshielded casks designed for highly enriched uranium (HEU) or plutonium (Pu), i.e., for special nuclear material (SNM).

When the shipment of strategic SNM (SSNM) is being considered, 10 CFR 73.26(1)91 requires that "shipments shall be made only on container ships," and that the SNM containers "shall be loaded into exclusive use cargo containers conforming to American National Standards Institute (ANSI) MH5.1 or International Standards Organization (ISO) 1496." These ANSI MH5.1 (now ANSI MH5.1M-1979) containers are "closed van cargo containers" of the modular type which can be handled by truck, rail, or ship, and which can be stacked in the holds of a container ship.

The cargo payload to be considered during Phase 1 of the TRANSEAVER contract is strategic quantities of special nuclear material (i.e., HEU/Pu). Table 9-1 below lists the NRC Certificate Numbers for the 14 casks that were identified from the NUREG 0383 Rev. 2 as licensed for SSNM.

Table 9-2 gives further information on the seven casks that are candidates for the TRANSEAVER Phase 2 cargo. The casks eliminated were unnecessarily large, heavy, or specialized; or insufficient information existed to draw a meaningful conclusion.

Two casks (Certificate Numbers 5332 and 9009) were investigated and found to have a high expectation of availability during the next few years. Table 9-3 shows procurement information for these two casks. Others of the seven casks described in Table 9-2 may also be available and can be investigated if desirable.

TABLE 9-1

LIST OF NRC CERTIFICATE NUMBERS FOR CASKS LICENSED TO CARRY
HEU AND PU (FROM NUREG 0383, REV. 2, OCT. 79)

5059
5236*
5331*
5332*
5468*
5492*
5908*
6142
6387
6581
9009*
9020
9069
9901

*See Table 9-2

TABLE 9-2

DESCRIPTION OF CASKS IDENTIFIED AS CANDIDATES FOR THE PHASE 1 TRANSEAVER CARGO

Certificate Number	Model Number	Expiration Date	Gross Weight[b]	Dimensions (Outside)[c]	Responsible Organization
5236	PR-1	Mar. 92		12x12x82.5	G.E.
	PR-2			12x12x58.5	
5331	BP-2	Aug. 83		22x22x33	G.E.
5332[a]	2030-1	Jan. 83	145	20Dx30	DOE
5468	NFS-IX-A	Mar. 82	<400	48x62x13.5	Nuclear Fuel Services
5492	RNG-181-I	Mar. 82	<150	20Dx30	Nuclear Fuel Services
5908	DOT-6M(B)	Feb. 81		(Not given)	Babcock/Wilcox
9009[a]	FL10-1	Aug. 83	500	22.5Dx68	G.E.

[a] Investigated and available

[b] lbs

[c] inches

TABLE 9-3

PROCUREMENT INFORMATION FOR TWO LICENSED SSNM CASKS

NRC Certificate No.	5332	9009
NFR's Model No.	2030-1	FL 10-1
Approx. Cost (ea)	$350	$**
* Item 3(a) Prepared by	U.S. Dept. of Energy Albq. Operations Office P.O. Box 5400 Albuquerque, NM 87115	General Electric Co. P.O. Box 780 Wilmington, NC 28401 919/343-5000
Contact	Edmond L. Barraclaugh 505/844-7276	A. L. Kaplan, x-5647 Doug Burns, x-5219
* Item 3(b) Title and identification of...application	Dow Chemical U.S.A. Rocky Flats Div. RFP-1857, Rev. 1 303/497-	General Electric Co. application, 12Mar73 as supplemented
Contact	Don Getman, x-2950 Ken Golligher, x-4117	
* Item 3(c) Docket No.	71-5332	71-9009
PROCUREMENT:		
Organization	U.S. Dept. of Energy Rocky Flats Area Office P.O. Box 928 Golden, CO 80401 Manager: Donald Ofte	General Electric Co. P.O. Box 780 Wilmington, NC 28401 919/343-5000
Reference	Ken Golligher of Dow Chemical, Rocky Flats [See Item 3(b)]	John Miss, Manager Traffic & Material Distribution, x-5625
AVAILABILITY:		
Data	By mid-1981	Immediately
Number	6 to 12	(Adequate)
Comments	Can be manufactured	** May be purchased, leased, or rented

* From Item 3 of the NRC Certificate of Compliance in NUREG 0383, Rev. 2 (Oct. 1979).

10.0 SCHEDULE AND COST ESTIMATES

TRANSEAVER, based on RECOVER components and commercially available equipment, can be quickly brought to viable operation through a four-phase program as follows:

Phase 1: Concept Definition, System Design
Phase 2: System Fabrication
Phase 3: System Test and Demonstration
Phase 4: Routine System Operation

This report represents the culmination of Phase 1. A bar chart showing the projected times for each phase of the program is Figure 10-1. Phase 4, Routine System Operation, can be accomplished within the third calendar quarter of 1982.

10.1 Estimated Program Costs

Estimates in costs to complete TRANSEAVER for Phases 2 and 3 are as follows:

Phase 2: $217,000 + $201,500 GFE
Phase 3: $120,000

The government-furnished equipment (GFE) required for Phase 2 already exists within the RECOVER program supplies which are available. Therefore, the GFE represents no new expenditures but use of equipment already on hand. The other costs are manpower and materials: Phase 2 will result in an operational prototype being assembled and tested in laboratory-type conditions; Phase 3 comprises the installation and monitoring of an actual operational test of the system as applied to a shipment of SNM. The quoted costs apply to the engineering manpower utilized to install the prototype on-board ship and to technician support during a 60-day shipment/ demonstration.

10.2 Estimated Operation Costs

Under the assumption that the only costs of interest for the operation of TRANSEAVER are those associated with the system itself, the following cost data is provided:

Hardware spare parts	$5,000/year
Communications Costs	
MARISAT at 2400 baud	$30 for initial three minutes
For one call per six hours	$120/day
Land line costs	Location dependent

If the remote verification unit were in Washington, D.C., the land line costs would be minimal to the MARISAT station just to the north of the

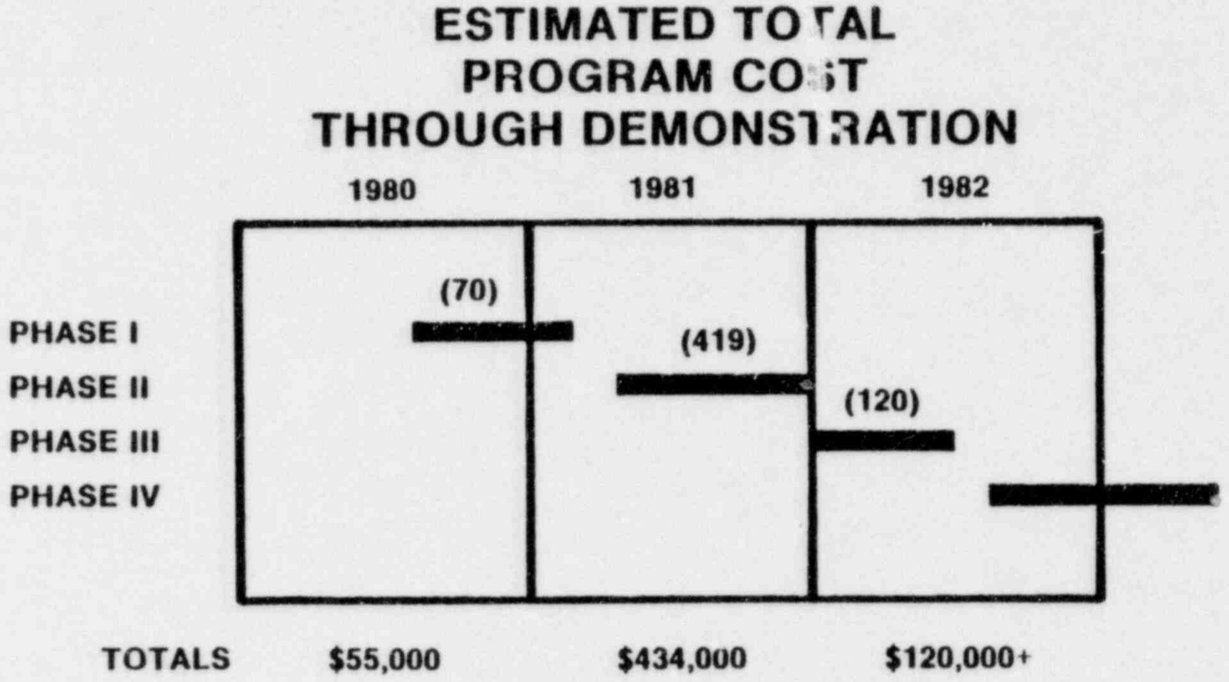


Figure 10-1 Bar Chart Showing Estimated Total Program Cost Through Demonstration

city. A three-minute call would cost less than $5.00; therefore, a daily expense of less than $20.00 would not be unreasonable.

10.3 Amortized System Cost Per Shipment

Beginning with a few relatively straightforward assumptions and the already established costs of equipment, a projected cost per shipment can be developed. The assumptions are as follows:

(1) The TRANSEAVER equipment will have a three-year useful life.

(2) A system can be used on five shipments per year if an average voyage lasts 60 days.

(3) The sensors are replaced after every shipment.

(4) The ship has no on-board MARISAT communications equipment, i.e., a complete shipboard installation is required.

A complete TRANSEAVER system comprises three separate subsystems. The first is a land-based installation unit which can be used to monitor multiple shipboard installations. The second is the shipboard installation which can monitor multiple shipboard containers. The third is the installation within each shipping container. The costs per subsystem are as follows:

1. Land-based installation

Portable Verification Unit (PVU) 2 units at $2,936.00	$ 5,872
Remote Verification Unit (RVU)	23,674
Subtotal	$ 29,546

2. Shipboard Installation

Communications Terminal (CT)	$ 75,000
Universal Teleprinter Interface (UT)	4,700
Navigation Terminal (NT)	10,500
Communications Interface Unit (CIU)	2,209
Uninterruptible Power Supply	4,750
Battery Pack	2,720
Subtotal	$ 99,879

3. Shipping Container Installation

Monitor Unit (MU) 30 @ $95 each	$ 2,850
On-Site Multiplexor (OSM)	1,847
Sensors	6,000
Subtotal	$ 10,697
System Total	$140,122

The hardware plus operational costs are now broken down to a per shipment basis, and the actual unit cost is determined. The sensors will be replaced every shipment.

Hardware (5 shipments/yr x 3 yrs)	$ 9,075
Sensors	6,000
Spare parts	1,000
Communications, 60-day mission MARISAT @ 1 call/6 hours	7,200
Land lines	1,200
	$24,475

Thus, for a cost-per-shipment basis of less than $25,000, TRANSEAVER can be functional on one ship.

10.4 Additional Cost Considerations

A few permutations regarding assumptions should be considered to put the cost per shipment calculated in Section 10.3 into perspective.

The first of these would involve using a ship with an already available MARISAT terminal on board. Since there are over 500 ships now operating with the equipment, the availability of one should be quite high. Therefore, removing the cost of only the Communications Terminal (CT) reduces the cost per shipment to $19,075.

The second permutation would involve multiple ships carrying multiple cargoes. This would spread the cost of the land-based installation and shipboard installation. Assume five ships with existing MARISAT terminals and each ship carries three cargo containers for a total of 225 shipments over the three years.

Under the second assumption, the capital equipment costs per shipment amortize to a remarkable $997. At less than a thousand dollars per shipment, the total costs therefore become controlled by the operational costs. Since the Communications Interface Unit (CIU) can handle the three shipping containers simultaneously and the data transmission rates are high, the communications costs per ship do not change. Thus, the cost per shipment is $10,800. If the sensor replacement cost is halved, the cost per shipment drops remarkably to $7,800.

11.0 OTHER DEDICATED COMMUNICATIONS SYSTEMS

A preliminary analysis of the feasibility of using other dedicated communications systems, analogous to MARISAT, to provide continual verification for truck, train, and air transport of special nuclear material (SNM) was performed. In general, no substitute for MARISAT was found; and, it is technically possible to create a system to use other available satellite systems for truck, train, and aircraft monitoring.

11.1 Ship to Shore Communications

From 1978 until the present time, only two satellite systems have been maintained to provide ship to shore telecon capabilities; FLTSATCOM (Fleet Satellite Communications) and MARISAT (Maritime Communications Satellite). Other satellites have been orbited but only for short durations or specific durations. In 1976, the U.S. Congresss directed that the FLTSATCOM dedicated Navy satellite program would be discontinued, with the Navy instead obtaining the necessary services through leasing arrangements with commercial carriers. Therefore, beginning in 1976, the Navy signed a five year lease with COMSAT General for UHF Channels on the three MARISAT satellites. By the end of 1981, additional commercial satellites are expected to be orbited under the LEASAT (Leased Satellite) Program for leasing of channels to the Navy through commercial carriers. In the mid-1980s a new system, GPSCS (General Purpose Satellite Communication System), is planned for deployment for U.S. industry and will provide leased services to U.S. commercial and military customers for ship to shore as well as ground run communications.

Meanwhile, the INMARSAT System (International Maritime Satellite System) of a 28 member multi-national consortium is expected to be operational by 1983. That is the follow-on to the present completely U.S. owned MARISAT system.

Therefore, at present time, MARISAT provides the only commercially available ship to shore telephone communication capability for either voyage or data transmission.

11.2 Truck, Train, and Aircraft Communications

The U.S. military has spent on the order of $700 million per year on satellite communication for the past ten years. Of this total, more than $220 million per year is directed toward developing terminals for communicating with the variety of satellites already in orbit or planned for the future. Specifically, the Navy has designed shipboard terminals utilizing the FLTSATCOM or MARISAT ship to shore communications satellite. The Air Force has designed aircraft mounted antennas and onboard terminals utilizing the current AFSATCOM and future AEROSATCOM system. The Navy has designed man portable terminals for the DSCS (Defense Satellite Communications System) and TACSATCOM/GMS (Tactical Satellite Communication System for Ground Mobile Forces).

Current programmatic approach to satellite communications by each of the military services is to meet satellite channels from commercial satellite communications carriers. Therefore, military developed terminals are technically usable by commercial users who would also reach channels on the same satellites.

The current technical approach to satellite communications by each of the military services is to move into the SHF (Super High Frequency) ban, which provides the same antenna gain characteristic with much smaller antenna, compared to the UHF (Ultra High Frequency) ban more widely used at present. Therefore, the newer terminals are to be much smaller and lighter.

Therefore, it is technically possible today to place a completely mobile satellite communication terminal onboard a truck, train, or aircraft, to perform automatic satellite tracking, and to provide direct satellite telephone communication capability to a fixed land-based location.

12.0 CONCLUSIONS

(1) Review of applicable federal regulations and international guidelines has shown that TRANSEAVER could enhance safeguards on shipments of nuclear and other sensitive material while maintaining compliance with current federal regulations and guidelines for such shipments.

(2) TRANSEAVER is designed to aid in providing the physical protection measures which include the provision of continuous two-way radio communication and frequent telephone communication.

(3) The system can be assembled from existing RECOVER components and other commercially available equipment.

(4) No new equipment need be developed to bring a system to the prototype stage for demonstration.

(5) Some software development would be required for the Communications Interface Unit (CIU).

(6) Commercially available sensors could be used as an effective system for detecting attempted diversions of materials provided that a sufficient number, appropriately integrated into an overlapping system, are used.

(7) Estimated operational costs and amortized capital expenses yield a cost per shipment that is not unreasonable even in the prototype demonstration stage.

(8) The estimated cost per shipment for a network of ships having multiple shipments per mission becomes very reasonable. If this estimate is correct, a commercially attractive system has been designed.

(9) No technology problems that would inhibit the rapid and successful assembly of a prototype system for demonstration have been identified during the system conceptual design stage.

REFERENCES

1. Report to The Congress by The Comptroller General of the United States: Federal Actions are Needed to Improve Safety and Security of Nuclear Materials Transportation, EMD-79-18, May 7, 1979. This document is available from the Government Printing Office.

2. Study of Physical Security of Special Nuclear Materials in Transit Between Nations, SAND 77-0518. This document is confidential and not available to the public.

3. U.S. Nuclear Regulatory Commission, Final Environmental Impact Statement on the Transportation of Radioactive Material By Air and Other Modes, NUREG-0170, Vol. 1, Washington D.C., December 1977. This document is available from the National Technical Information Service, order number PB-275529 (Vol. 1) and PB-275530 (Vol. 2).

4. "NRC/DOT Memorandum of Understanding," March 22, 1973, published in the Federal Register, Vol. 44, July 2, 1979 (44FR38690).

5. Saltzman, Jerome, "Effects on Transportation Coverage of Recent Modifications in the Price-Anderson Insurance and Indemnity System," Proceedings of the Fifth International Symposium on Packaging and Transportation of Radioactive Material, Vol. II, Las Vegas, May 1978. This document is available from the National Technical Information Service, order number CONF-780506.

6. Byrne, J. et al., TRW Systems Group, "RECOVER System Design Requirements Status Report," Contract No. AC8NC120, prepared for U.S. Arms Control and Disarmament Agency, February 2, 1979. This document is available at TRW.

7. Sandia Laboratories, Information Systems Department 1730, Intrusion Detection Systems Handbook, SAND 76-0554, November 1976, Revised October 1977. This is a controlled document and is available for inspection at Sandia Laboratories.

BIBLIOGRAPHY

1. ARC 54-5699, "Final Report, RECOVER Remote Continual Verification," June 1978.

2. ACDA Contract AC8NC120, "Initial Implementation and Demonstration of the Remote Continual Verification (RECOVER) System," September 28, 1978.

3. ACDA RFP 78-4, "Initial Implementation and Demonstration of the Remote Continual Verification (RECOVER) System," June 13, 1978.

4. Prell, J. A., "Interior Intrusion Alarm Systems," U.S. Nuclear Regulatory Commission, Office of Standards Development, NUREG-0320, February 1978.*

5. Sandia Laboratories, Facility Protection Department, Safeguards Control and Communications Systems Handbook, prepared for the United States Government, SAND 78-1785, May 1979.

6. TRW 34222.000, "Initial Implementation and Demonstration of the Remote Continual Verification (RECOVER) System Proposal," Technical and Management Volume, July 13, 1978.

7. Underwriter Laboratory Standard 478, "Data-Processing Units and Systems, Electrical," October 10, 1977.

8. Underwriter Laboratory Standard 609, "Burglar Alarm Units and Systems, Local," March 31, 1978.

9. Underwriter Laboratory Standard 611, "Burglar Alarm Units and Systems, Central Station," August 19, 1978.

10. Underwriter Laboratory Standard 634, "Connectors and Switches for Use with Burglar Alarm Systems," June 29, 1973.

11. Underwriter Laboratory Standard 796, "Printed Wiring Board, Electrical," August 10, 1973.

*Available for purchase from the National Technical Information Service, Springfield, VA 22161.

APPENDIX A

NRC REGULATIONS

The regulations that specify guidelines for ensuring adequate containment are l'sted in Part 71 -- "Packaging of Radioactive Material for Transport and Tra..ɔportation of Radioactive Material Under Certain Conditions."

The terms applicable to the TRANSEAVER project as defined in 10 CFR 71.4, "Definitions," are as follows:

"(d) 'Fissile classification' means classification of a package or shipment of fissile materials according to the controls needed to provide nuclear criticality safety during transportation as follows:

(2) Fissile Class II: Packages which may be transported together in any arrangement but in numbers which do not exceed an aggregate transport of 50. For purposes of nuclear criticality safety control, individual packages may have a transport index of not less than 0.1 and not more than 10. However, the external radiation levels may require a higher transport index number but not to exceed 10. Such shipments require no nuclear criticality safety control by the shipper during transportation.

(3) Fissile Class III: Shipments of packages which do not meet the requirements of Fissile Classes I or II and which are controlled in transportation by special arrangements between the shipper and the carrier to provide nuclear criticality safety.

(e) 'Fissile materials' means uranium-233, uranium-235, plutonium-238, plutonium-239, and plutonium-241.

(k) 'Package' means packaging and its radioactive contents;

(1) 'Packaging' means one or more receptacles and wrappers and their contents excluding fissile material and other radioactive material, but including absorbent material, spacing structures, thermal insulation, radiation shielding devices for cooling and for absorbing mechanical shock, external fittings, neutron moderators, nonfissile neutron absorbers, and other supplementary equipment."

The general standards for all packaging can be found in Subpart C, Section 71.31 of 10 CFR. The basic requirements are as follows:

"(a) Packaging shall be of such materials and construction that there will be no significant chemical, galvanic, or other reaction among the packaging components, or between the packaging components and the package contents.

(b) Packaging shall be equipped with a positive closure which will prevent inadvertent opening.

(c) Lifting devices: . . .

(d) Tie-down devices: . . ."

Structural standards for Type B and large quantity packaging specify requirements for load resistance and external pressure (10 CFR §71.32).

Criticality standards for fissile material packages specify the design and construction and content limitation so that the package would be subcritical if water were to leak into the containment vessel. Specific reference to the design factors can be found in Section 71.33.

The NRC has specified standards for normal conditions of transport and hypothetical accident conditions in Sections 71.35 and 71.36. Under normal conditions, a package having more than type A quantity of radioactive material shall be so designed that:

"(1) There will be no release of radioactive material from the containment vessel,

(2) The effectiveness of the packaging will not be substantially reduced;

(3) There will be no mixture of gases or vapors in the package which could, through any credible increase of pressure or an explosion, significantly reduce the effectiveness of the package;

(4) Radioactive contamination of the liquid or gaseous primary coolant will not exceed 10^{-7} curies of activity of Group I radionuclides per milliliter, 5×10^{-6} curies of activity of Group II radionuclides per milliliter, 3×10^{-4} curies of activity of Group III and Group IV radionuclides per milliliter; and

(5) There will he no loss of coolant."

(§71.35)

Furthermore, under normal conditions, a package shall be designed so that:

"(1) The package will be subcritical;

(2) The geometric form of the package contents would not be substantially altered,

(3) There will be no leakage of water into the containment vessel. This requirement need not be met if, in the evaluation of undamaged packages under §71.38(a), §71.39(a)(1), or

§71.40(a), it is assumed that moderation is present to such an extent as to cause maximum reactivity consistent with the chemical and physical form of the material; and

(4) There will be no substantial reduction in the effectiveness of the packaging, including:

(i) Reduction by more than five percent in the total effective volume of the packaging on which nuclear safety is assessed;

(ii) Reduction by more than five percent in the effecti:e spacing on which nuclear safety is assessed between the center of the containment vessel and the outer surface of the packaging;

(iii) Occurrence of any aperture in the outer surface of the packaging large enough to permit the entry of a four-inch cube.

(c) A package used for the shipment of more than a tyre A quantity of radioactive material, as defined in §71.4(q), shall be so designed and constructed and its contents so limited that under the normal conditions of transport . . . the containment vessel would not be vented directly to the atmosphere."

(§7:.35)

Under hypothetical accident conditions, the following standards apply:

"(a) A package used for shipment of more than a type A quantity . . . shall be so designed . . . that if subjected tc . . . the Free Drop, Puncture, Thermal, and Water Immersion conditions . . . it will meet the following conditions:

(1) The reductior of shielding would not be sufficient to increase the external radiation dose rate to more than 1,000 millirems per hour at three feet from the external surface of the package.

(2) No radioactive material would be released from the package except for gases and contaminated coolant containing total radioactivity exceeding neither:

(i) 0.1% of the total radioactivity of the package contents; nor

(ii) 0.01 curie of Group I radionuclides, 0.5 curie of Group II radionuclides, 10 curies of Group III radionuclides, 10 curies of Group IV radionuclides, and 1,000 curies of inert gases irrespective of transport group.

(§71.36)

(b) A package used for the shipment of fissile material shall be so designed . . . that if subjected to . . . the Free Drop, Puncture, Thermal, and Water Immersion conditions . . ., the package would be subcritical. In determining whether this standard is satisfied, it shall be assumed that:

(1) The fissile material is in the most reactive credible configuration consistent with the damaged condition of the package and the chemical and physical form of the contents;

(2) Water moderation occurs to the most reactive credible extent consistent with the damaged condition of the package and the chemical and physical form of the contents; and

(3) There is reflection by water on all sides and as close as is consistent with the damaged condition of the package."

(§71.36)

The NRC regulations describe three package classes: Fissile I, II, and III. Because Fissile Class I materials do not pertain to the TRANSEAVER project, the specifications for this class (§71.38) will not be discussed. A summary table follows below.

If a number of packages would be subcritical in any arrangement and in any foreseeable transport circumstances, NRC assigns them a Fissile Class II rating.

> "A Fissile Class II package shall be so designed and constructed and its contents so limited and the number of such packages which may be transported together so limited that:

(2) Twice that number of such packages would be subcritical in any arrangement if each package were subjected to the hypothetical accident conditions . . . as the Free Drop, Thermal, and Water Immersion conditions . . ., with close reflection by water on all sides of the array and with optimum interspersed hydrogenous moderation unless there is a greater amount of interspersed moderation in the packaging, in which case that greater amount may be considered.

(b) The transport index for each Fissile Class II package is calculated by dividing the number 50 by the number of such Fissile Class II packages which may be transported together as determined under the limitations of paragraph (a) . . . ."

(§71.39)

The Fissile Class III rating includes all packages of nonlimited fissile material that do not comply with the requirements of Class I or Class II pac<ages. Specific standards specify that the design, construction, and nur ber of packages for Fissile Class III be such that:

"(a) The undamaged shipment would be subcritical with an identical shipment in contact with it and with two shipments closely reflected on all sides by water; and

(b) The shipment would be subcritical if each package were subjected to the hypothetical accident conditions . . . as the Free Drop, Thermal, and Water Immersion conditions, with close reflections by water on all sides of the array and with the packages in the most reactive arrangement and with the most reactive degree of interspersed hydrogenous moderation which would be credible considering the controls to be exercised over the shipment . . . ."

(§71.40)

Special requirements for the shipment of plutonium include:

"(a) . . . plutonium in excess of twenty curies per package shall be shipped as a solid.

(b) Plutonium in excess of twenty curies per package shall be packaged in a separate inner container placed within outer packaging . . ." Solid plutonium . . . exempt from the requirements of this paragraph:

(1) Reactor fuel elements;
(2) Metal or metal alloy; or
(3) Other plutonium-bearing solids that the Commission determines should be exempt from the requirements of this section.

(§71.42)

Definitions for "special nuclear material" in transit are in Section 73.2 of 10 CFR. Relevant definitions are cited as follows:

"(x) 'Special nuclear material of moderate strategic significance' means:

(1) Less than a formula quantity of strategic special nuclear material but more than 1000 grams of uranium-235 (contained in uranium enriched to 20% or more in the U-235 isotope) or more than 500 grams of uranium-233 or plutonium or in a combined quantity of more than 1000 grams when computed by the equation, grams = (grams contained U-235) + 2 (grams U-233 + grams plutonium), or

REQUIRED NUMBER OF PACKAGES TO BE DEMONSTRATED AS SUBCRITICAL UNDER SPECIFIC MODERATION AND REFLECTION CONDITIONS AS PER SECTIONS 71.38, 71.39, AND 71.40 OF 10 CFR PART 71

<table>
<tr><th></th><th colspan="2">CONDITIONS OF SHIPMENT</th></tr>
<tr><th>FISSILE CLASS</th><th>NORMAL CONDITIONS</th><th>ACCIDENT CONDITIONS</th></tr>
<tr><td></td><td>(No more than 5% reduction in the total effective volume of the packaging on which nuclear safety is assessed.)</td><td>(All packages damaged as per hypothetical accident (HA) specifications.)</td></tr>
<tr><td>I</td><td>Unlimited number of packages are to remain subcritical with optimum interspersed hydrogenous moderation. No water reflection necessary.</td><td>250 packages are to remain subcritical in any arrangement under HA conditions with optimum interspersed hydrogenous moderation and close reflection by water on all sides of array.</td></tr>
<tr><td>II</td><td>Five times the number of packages to be shipped are to remain subcritical in any arrangement when this array is closely reflected by water.</td><td>Two times the number of packages to be shipped are to remain subcritical in any arrangement under HA conditions with optimum interspersed hydrogenous moderation and closer reflection by water on all sides of array.</td></tr>
<tr><td></td><td colspan="2">Since the maximum value of the Transport Index (TI) for an individual package of Fissile Class II is 10 and the TI equals 50 divided by the allowable number of packages, 5 is the smallest value for the maximum allowable number of packages in a shipment. Therefore, the minimum number of packages in the array that must be considered in the criticality analysis is:</td></tr>
<tr><td></td><td>5 x 5 or 25 packages for normal transport</td><td>2 x 5 or 10 packages for accident conditions</td></tr>
<tr><td>III</td><td>One shipment of packages is to remain subcritical when it is in contact with an identical shipment and the two-shipment array is reflected on all sides by water.</td><td>One shipment of packages is to remain subcritical under HA conditions with optimum hydrogenous moderation and close reflection by water.</td></tr>
</table>

From: USNRC Regulatory Guide 7.9, standard Format and Content of Part 71 Applications for Approval of Packaging of Type B, Large Quantity, and Fissile Radioactive Material, March 1979.

(2) 10,000 grams or more of uranium-235 (contained in uranium enriched to 10% or more but less than 20% in the U-235 isotope).

(y) 'Special nuclear material of low strategic significance' means:

(1) Less than an amount of strategic special nuclear material of moderate strategic significance, as defined in §73.2(x)(1), but more than 15 grams of uranium-235 (contained in uranium enriched to 20% or more in the U-235 isotope) or 15 grams of uranium-233 or 15 grams of plutonium or the combination of 15 grams of plutonium when computed by the equation, grams = grams contained U-235 + grams plutonium + grams U-233, or

(2) Less than 10,000 grams but more than 1000 grams of uranium-235 (contained in uranium enriched to 10% or more but less than 20% in the U-235 isotope),

(3) 10,000 grams or more of uranium-235 contained in uranium enriched above natural but less than 10% in the U-235 isotope.

(aa) 'Strategic special nuclear material' means uranium-235 (contained in uranium enriched to 20% or more in the U-235 isotope), uranium-233, or plutonium.

(bb) 'Formula quantity' means strategic special nuclear material in any combination in a quantity of 5,000 grams or more computed by the formula, grams = (grams contained U-235) + 2.5 (grams U-233 + grams plutonium).

APPENDIX B

DOT REGULATIOnS

The regulations as prescribed in Sections 173.391 through 173.396 of 49 CFR ꞁertain to the packaging design, size, and reꞇuired specific features. For example, there should be a seɐl on the outside of each package. The packaging design must maintain shielding efficiency and leak tightness (§173.393(b)(c)). Under normal transportation conditions, internal tracing or cushioning ". . . must be adequate to assure that . . . the distance from the inner container or radioactive material to the outside wall of the package remains within the limits for which the package design was based, and the radiation dose rate external to the package does not exceed the transport index number . . . ." (§173.393(1)).

During transport, any heat generated by the radioactive mate ials must not affect the efficiency of the package.

Specifically, the temperature of the external package surfaces will not exceed 122 degrees F in the shade (§173.393(2)). Suitable packaging must ensure that radiation dose rates do not exceed specific levels as prescribed in Section 173.393 (i)(j)(1-4).

Section 173.394 specifies the package requirements for a Type A quantity of special form radioactive material. Reference is made to specifications such as 7A (§178.350) and 55 (§178.250). For Type B quantities of special form radioactive materials, the following specifications apply:

"(1) Specification 55 metal encased shielded container . . .

(2) Specification 6M (§178.104) . . . metal packaging.

(5) Specification 20WC (§178.194) . . . wooden outer protective jacket, with a single, snug-fitting inner Type A packaging which has a metal outer wall and conforms to §178.350 . . . ."

(6) Specification 21WC (§178.195) wooden-steel protective overpack, with a single inner specification 55 inner packaging."

For large quantities of radioactive materials in special form, the following specifications apply:

(2) 6M (§178.104) . . . metal packaging . . .

(4) 20WC (§178.194) . . . wooden outer protective jacket, with a single, snug-fitting specification 55 inner packaging . . .

For Type A quantity of normal form radioactive material, a package must meet the following specifications:

(1) Specification 7A (§178.350)

(2) Specification 55 metal encased shielded container . .

For Type B quantity of normal form radioactive material, a package must meet the following specifications:

(1) Specification 6M (§178.104)

(2) Specification 20WC (§178.194) . . . wooden outer protective jacket, when used with a single, snug-fitting inner specification 2R (§178.34) . . . or specification 55 inner packaging.

For large quantities of radioactive materials in normal form, the following specifications apply:

(1) Specification 6M (§178.104) metal packaging. Authorized only for solid or gaseous radioactive materials which will not decompose at temperatures up to 250 degrees F. Radioactive thermal decay energy must not exceed 10 watts.

Fissile radioactive materials containing not more than Type A quantities of radionuclides, in either normal or special form, must be packaged in compliance with the following specifications:

(1) Specification 6L (§178.103) . . . metal packaging.

(2) Specification 6M (§178.104) . . . metal packaging.

(6) Specification 20PF-1, 20F-2, or 20PF-3 (§178.120).

(7) Specification 6J (§178.100) or 17H (§178.118) 55 gallon steel drum for transport of not more than 350 grams of uranium-235 in any non-pyrophoric form, enriched to any degree in the U-235 isotope. Each drum must have a minimum 18-gauge body and bottom head and 16-gauge removable top head, with one or more corrugations in the cover near the periphery. Closure must conform to §178.103-5(a) . . . At least four 1.2-centimeter (0.5-inch)-diameter vent holes must be provided, equally spaced on the sides of the drum near the top, each covered with weatherproof tape or equivalent device. Appropriate primary inner containment of the cor[illegible] and any necessary packing material must be provided, . . . such that Specification 7A (§178.350) . . . is satisfied. Each inner containment vessel must be capable of venting in the event the package was exposed to the thermal test described in §173.398(c)(2)(iii).

(8) Any metal cylinder which meets the performance requirements for a specification 7A Type A packaging §173.395(a)(1) and §178.350 for the transport of residual "heels" of enriched solid uranium hexafluoride without a protective overpack, or authorized as Fissile Class I packages . . .

(c) Fissile radioactive materials containing Type B quantities or radionuclides, in either normal form or special form, must be packaged as follows:

(1) Specification 6L (§178.103) metal packaging. Authorized only for uranium-235, plutonium-239 or 241, as metal, oxide, or compounds which will not decompose at temperatures up to 149 degrees C (300 degrees F). Radioactive thermal decay energy output shall not exceed 5 watts. Large quantity radioactive materials in normal form must be packaged in one or more sealed and leak-tight metal cans or polyethylene bottles within the Specification 2R containment vessel.

APPENDIX C

TRANSEAVER FUNCTIONAL REQUIREMENTS

This appendix defines the minimum, mandatory design requirements for the TRANSEAVER system. These requirements are described in three subsections--the functions to be performed (Section 1), the data to be maintained (Section 2), and the interfaces to be supported (Section 3).

1. Functional Description

The TRANSEAVER system has four subsystems that are the same as those of RECOVER: the Monitor Unit (MU), the On-Site Multiplexor (OSM), the Remote Verification Unit (RVU), and the Portable Verification Unit (PVU). Each of these subsystems is described briefly below.

(1) MU - The MU shall periodically read and record status data from a safeguards sensor and securely communicate this data and MU status data to an OSM on demand. Primary power for the MU shall be supplied by wireline from its OSM. In addition, the MU shall have an internal battery which shall provide for degraded MU operation if primary power is lost.

(2) OSM - The OSM shall periodically interrogate its MUs and record the status of each. The interrogation schedule for a particular MU shall be variable, shall be established by an inspector, and shall be based on the criticality of the data from the sensor to which a particular MU is interfaced (defined during MU installation). The data stored in the OSM shall be securely communicated to the CIU when the CIU interrogates the OSM. Primary power for the OSM shall be supplied by the TRANSEAVER battery supply. In case of interruption of this supply, the OSM shall contain a battery power supply to power the OSM for short periods.

(3) RVU - The RVU shall periodically interrogate each CIU, update its copy of the OSM status data, and generate an archive record describing the transaction. The RVU shall recognize predefined alert conditions and, when they occur, notify inspectors of the alert. Notification will include, as appropriate, initiating telephone calls to key personnel. The RVU shall also provide appropriate reports of current and past CIU, OSM, MU, and sensor status. The interrogation rate of a particular CIU shall be variable and can be overridden by inspector request at any time.

(4) PVU - The PVU shall be carried by inspectors to a ship for installation and checkout of MUs, OSMs, and CIUs. The PVU shall be capable of initializing and interrogating OSMs, CIUs, and MUs, and shall allow the inspector to determine their status. Power for operation of the PVU shall be obtained from external AC power.

In addition to the above four subsystems common to RECOVER, TRANSEAVER has several subsystems to meet the requirements of shipment at sea:

(1) CIU - The Communications Interface Unit shall periodically interrogate its OSMs and record the status of each. The interrogation schedule shall be consistent with the schedule that the OSMs use to interrogate the MUs. The data stored in the CIU shall be securely communicated to the RVU when the RVU interrogates the CIU. Also, if an alarm is detected by the CIU, it shall automatically forward that data immediately to the RVU in a secure fashion. The CIU shall be able to compare navigational data with a preprogrammed route and send an alarm to the RVU if the ship deviates significantly from the planned course. The TRANSEAVER battery supplies the primary power for the CIU. The CIU shall contain a battery to power the CIU for short periods.

(2) UTI - The Universal Teleprinter Interface shall automatically send navigational data upon request or poll from the RVU. It shall provide ship latitude, longitude, speed, heading, date, precise GMT, and any other available and pertinent information from the Navigational Terminal. The TRANSEAVER battery supply shall be the source of power.

(3) CT - The Communications Terminal shall be the onboard link to the MARISAT satellite. It shall have all necessary equipment for making that communication and interfacing to the UTI. Its power shall come from the TRANSEAVER battery supply.

(4) NT - The Navigational Terminal shall communicate with a navigational satellite system such as TRANSIT to obtain all data as called for by the UTI. It shall make maximum use of the existing satellite data to minimize the length of time between position fixes. Power for the NT shall be from the TRANSEAVER battery supply.

(5) TRANSIT - An existing navigational satellite system such as TRANSIT shall be used to obtain tracking information.

(6) MARISAT - The existing MARISAT satellite system shall be used for communications between ship and shore. Communication shall be between the Tracking, Telemetry, and Command Center through the System Control Center to the RVU using standard methods.

(7) TRANSEAVER Battery Supply - This battery system shall be capable of supplying all on-board TRANSEAVER components with their rated voltage and wattage for up to 1500 hours. The recharge time shall be less than 72 hours.

1.1 Monitoring Unit Functional Description

The MU shall perform the following functions:

(1) The MU shall accept eight (8) independent parallel bits of status from a sensor. (These bits will represent normal/abnormal status.)

(2) The MU shall maintain a historical record of the identity of any sensor status bits that have had abnormal status between OSM-MU polls, even if that bit reverts to normal status before the next OSM-MU poll.

(3) The MU shall determine its own physical status (normal or abnormal), to include at least external power status and battery status.

(4) The MU shall determine the status (normal or abnormal) of its interfaces, to include at least MU-sensor cable connection.

(5) The MU shall maintain a historical record of any physical or interface status items that have had abnormal status between OSM-MU polls, even if that status reverts to normal before the next OSM-MU poll.

(6) The MU shall maintain sufficient OSM-MU polling status data (such as a poll counter) so as to enable its OSM to recognize that illicit polls of the MU by some entity other than its OSM have been made.

(7) The MU shall provide an encoded MU status report [including at least current (sensor, MU physical, and MU interface status) data; historical (sensor, MU physical, and MU interface status) data; and OSM-MU polling status data] to its OSM upon receipt of an OSM-MU poll request.

(8) The MU shall immediately execute any of its functions upon receipt of an appropriate command from its OSM and provide the results of that execution to the OSM.

(9) The MU shall receive external power through its communications interface with its OSM.

(10) Normal MU operations shall be supportable by internal battery for at least one hour under maximum OSM-MU polling rates.

(11) The MU shall provide +11 to +15 volts DC at 5mA continuous to sensors being monitored.

In addition to the above-mentioned functions, the MU shall be designed in accordance with the following goals:

(12) The MU shall incorporate provisions to minimize power consumption.

(13) The MU shall incorporate provisions to minimize loss of information in its communications.

(14) The MU shall incorporate provisions to assume degraded modes of operation to minimize the problem of MU re-initialization.

1.2 On-Site Multiplexor Functional Description

The OSM shall perform the following functions:

(1) The OSM shall poll its MUs and receive status reports from the MUs.

(2) The OSM shall maintain a historical record of any MU status report items that have had abnormal status between CIU-OSM polls, even if that status report item reverts to normal before the next CIU-OSM poll.

(3) The OSM shall provide a single, bit-serial interface to the MUs. Communication by both the OSM and the MUs on this shared circuit will require addressing data to be transmitted as an integral part of every message.

(4) The OSM shall be capable of polling up to 30 MUs.

(5) The OSM shall be able to initiate an OSM-MU poll based on either of two initiation procedures: a random procedure with a specified mean polling rate per MU (defined at MU installation), or a demand procedure to poll a specified MU at a particular time.

(6) The OSM shall recognize that illicit polls of one of its MUs by some entity other than itself have been made.

(7) The OSM shall determine its own physical status (normal or abnormal), to include at least external power status, battery status, and intrusion status.

(8) The OSM shall determine the status (normal or abnormal) of its interfaces, to include at least individual MU responsiveness, and individual MU illicit polling recognition.

(9) The OSM shall maintain a historical record of any physical or interface status items that have had abnormal status between CIU-OSM polls, even if that status item reverts to normal status before the next CIU-OSM poll.

(10) The OSM shall maintain sufficient CIU-OSM polling status data (such as poll counters) so the CIU can recognize that polls of the OSM by some entity other than the CIU have been made.

(11) The OSM shall maintain historical activity counts of at least the establishment of CIU-OSM communications, the establishment of PVU-OSM communications, and unsuccessful attempts to establish communications with the OSM.

(12) The OSM shall provide an encoded OSM status report (including at least current MU, OSM physical, and OSM interface status data) to either the CIU or to a PVU upon receipt of a CIU (PVU)-OSM poll request.

(13) The OSM shall respond to interrogation commands (including at least a request for an OSM status report, a request for an OSM historical activity report, a request to poll all MUs, and a request to poll a specific MU) received from either an RVU through the CIU or a PVU.

(14) The OSM shall alter its operating parameters (to include at least specific MU polling parameters and predefined alert status conditions) upon commands received from either the RVU through the CIU or PVU.

(15) The OSM shall immediately execute any of its functions upon receipt of an appropriate command from either the RVU through the CIU or a PVU and provide the results of that execution to the RVU or PVU (as appropriate).

(16) The OSM shall detect specified, predefined alert status conditions within the MU status reports and shall record the occurrence of the alert condition.

(17) The OSM shall be able to command the MU to execute any of its functions and to receive any results of the execution from the MU.

(18) Normal OSM operations shall be supportable by internal battery for at least one hour under maximum OSM-MU and CIU-OSM polling rates.

In addition to the above-mentioned functions, the OSM shall be designed in accordance with the following goals:

(19) The OSM shall incorporate provisions to minimize power consumption.

(20) The OSM shall incorporate provisions to minimize loss of information in its communications.

(21) The OSM shall incorporate provisions to assume degraded modes of operation to minimize the problem of OSM re-initialization.

(22) The OSM design shall provide maximum assurance that any attempt to override the TRANSEAVER system's control, to compromise the accuracy of the data being transmitted, or to provide access to that data by unauthorized persons shall be detected and reported to the RVU.

1.3 Remote Verification Unit Functional Description

The RVU shall perform the following functions:

(1) The RVU shall poll the CIUs and receive status reports from the CIUs.

(2) The RVU shall support 5 CIUs initially, and shall, with additional memory, be capable of expanding to support up to 500 CIUs.

(3) The RVU shall be able to initiate an OSM-MU poll based on two initiation procedures--a random procedure with a mean polling rate per OSM defined at OSM installation, or a demand procedure to poll a specified OSM at a particular time.

(4) The RVU shall be able to automatically dial CIUs through the MARISAT system.

(5) In the event of unavailable, unsatisfactory, or deteriorating communication between the RVU and a CIU, the RVU shall hang up and either automatically redial the call or notify an inspector of the communication failure. This choice will depend on how the call originated (automatically dialed by the RVU or manually dialed by the inspector), the specific CIU being called, and the recent calling history to that CIU (such as previous uncompleted calls).

(6) The RVU shall update its data base from the data received in a CIU status report.

(7) The RVU shall detect specified, predefined alert status conditions within a CIU status report.

(8) The RVU shall initiate alert processes (to include at least generating special displays or reports, activating audio-visual alarm signals, dialing local telephones to contact personnel, or any combination of these) in response to the detection of an alert status condition. The actual alert process shall be predefined and shall vary based on the specific alert status condition detected.

(9) The RVU shall be able to automatically dial any of five telephone numbers as a possible response to detecting an alert status condition.

(10) The RVU shall have audio-visual alarm signals which may be activated as a response to detecting an alert status condition.

(11) The RVU shall maintain historical archive records of CIU status reports for 90 days.

(12) The RVU shall recognize that polls of a CIU by some entity other than itself have been made. Polls that are not accounted for within the RVU data base shall be an alert status condition.

(13) The RVU shall prepare reports including at least current alert situations, latest individual shipment status, latest individual CIU status, latest individual MU status, CIU and OSM operating parameters, RVU communication usage history, operations log, and summary shipment status.

(14) The RVU shall automatically display or print predefined reports.

(15) The RVU shall maintain historical archive records to include at least RVU communication usage (both attempted and completed), inspector requests of the RVU, and RVU activities (both automatic and in response to an inspector request).

(16) All historical archive records shall include a record time.

(17) The RVU shall display or print any report upon inspector command.

(18) The RVU shall alter its operating parameters (to include at least RVU-CIU polling parameters, predefined alert status conditions, alert status condition responses, and designation of automatic reports) upon inspector command.

(19) When in communication with a CIU, the RVU shall be able to command the CIU to alter any of its operating parameters, either in accordance with a direct inspector command or with stored inspector commands.

(20) When in communication with a CIU and in response to either a direct or stored inspector command, the RVU shall command the CIU to execute any of its functions (including, in turn, commanding a MU to execute any of its functions) and provide the results of the function execution to an inspector.

(21) The RVU shall execute any of its functions upon receipt of an appropriate command from an inspector and provide the results of that execution to the inspector.

(22) The RVU shall receive AC line power from its host facility.

(23) The RVU shall utilize manual restart procedure following power failures.

(24) The RVU shall not lose any information because of power failure.

In addition to the above-mentioned functions, the RVU shall be designed in accordance with the following goals:

(25) The RVU shall incorporate provisions to minimize lost information in its communications.

(26) The RVU design shall provide maximum assurance that any attempt to override the TRANSEAVER system's control, to compromise the accuracy of the data being transmitted, or to provide access to that data by unauthorized persons, shall be detected and reported.

1.4 Portable Verification Unit Functional Description

The PVU shall perform the following functions:

(1) The PVU shall initialize an MU for operation with a specific OSM.

(2) The PVU shall initialize an OSM for operation with the CIU.

(3) The PVU shall initialize a CIU for operation with the RVU.

(4) The PVU shall poll an OSM or a CIU and receive status reports from the OSM or CIU.

(5) The PVU shall detect specified, predefined alert status conditions within an OSM or CIU status report.

(6) The PVU shall initiate an alert process (consisting of presenting a special display and an audio-visual alarm and may include suspending other operations until an inspector acknowledgement is received) in response to detection of an alert status condition. The actual response shall be predefined and shall vary based on the specific alert status condition detected.

(7) The PVU shall prepare displays (including at least CIU status, OSM status, MU status, CIU or OSM operating parameters, CIU or OSM historical activity counts, and PVU operating parameters) and display them to an inspector on request.

(8) The PVU shall alter its operating parameters (including at least definition of alert status condition and CIU or OSM cryptographic parameters) upon inspector command.

(9) The PVU shall command the CIU or OSM to alter any of its operating parameters in accordance with inspector commands.

(10) The PVU, in response to inspector commands, shall command the CIU or OSM to execute any of its functions (including, in turn, commanding the MU to execute any of its functions) and display the results of the function execution to an inspector.

(11) The PVU shall execute any of its functions upon receipt of an appropriate command from an inspector and provide the results of that execution to the inspector.

(12) The PVU shall, upon inspector command, permanently disable all of its functions except display of CIU, OSM, and MU status data.

(13) Normal PVU operations shall be supportable by external power. An internal battery shall be used to retain the PVU's RAM.

In addition to the above-mentioned functions, the PVU shall be designed in accordance with the following goals:

(14) The PVU shall incorporate provisions to minimize power consumption.

(15) The PVU design shall provide maximum assurance that any attempt to override the TRANSEAVER system's control, to compromise the accuracy of data being transmitted, or to provide access to that data by unauthorized persons shall be detected and reported to an inspector.

1.5 Communications Interface Unit Functional Description

The CIU shall perform the following functions:

(1) The CIU shall poll its OSMs and receive status reports from the OSMs.

(2) The CIU shall maintain a historical record of any OSM status report items that have had abnormal status between RVU-CIU polls, even if that status report item reverts to normal before the next RVU-CIU poll.

(3) The CIU shall interface with the Navigational Terminal (NT) and obtain navigational information from it.

(4) The CIU shall retain a historical record of the navigational information.

(5) The CIU shall accept a preprogrammed navigational course from the PVU.

(6) The CIU shall compare the preprogrammed course with the actual course and record any significant deviation as an alarm.

(7) Upon receipt of any alarm, the CIU will automatically initiate a call to the RVU and report the alarm.

(8) The CIU shall be able to initiate a CIU-OSM poll based on either of two initiation procedures: a random procedure with a specified mean polling rate per OSM (defined at OSM installation) or a demand procedure to poll a specified OSM at a particular time.

(9) The CIU shall recognize that illicit polls of one of its OSMs by some entity other than itself have been made.

(10) The CIU shall determine its own physical status (normal or abnormal), to include at least external power status, battery status, and intrusion status.

(11) The CIU shall determine the status (normal or abnormal) of its interfaces, to include at least individual OSM responsiveness and individual OSM illicit polling recognition.

(12) The CIU shall maintain a historical record of any physical or interface status items that have had abnormal status between RVU-CIU polls, even if that status item reverts to normal status before the next RVU-CIU poll.

(13) The CIU shall maintain sufficient RVU-CIU polling status data (such as poll counters) so the RVU can recognize that polls of the CIU by some entity other than the RVU have been made.

(14) The CIU shall maintain historical activity counts of at least the establishment of RVU-CIU communications, the establishment of PVU-CIU communications, and unsuccessful attempts to establish communications with the CIU.

(15) The CIU shall provide an encoded CIU status report (including at least current MU, OSM, and CIU physical, and OSM and CIU interface status data) to either the RVU or to a PVU upon receipt of a RVU (PVU)-CIU poll request.

(16) The CIU shall respond to interrogation commands (including at least a request for a CIU status report, a request for a CIU historical activity report, a request to poll all MUs, and a request to poll a specific MU) received from either an RVU or a PVU.

(17) The CIU shall alter its operating parameters (to include at least specific MU polling parameters and predefined alert status conditions) upon commands received from either the RVU or PVU.

(18) The CIU shall immediately execute any of its functions upon receipt of an appropriate command from either the RVU or a PVU and provide the results of that execution to the RVU or PVU (as appropriate).

(19) The CIU shall detect specified, predefined alert status conditions within the MU status reports and shall record the occurrence of the alert condition.

(20) The CIU shall be able to command the OSM to execute any of its functions and to receive any results of the execution from the OSM.

(21) Normal CIU operations shall be supportable by internal battery for at least one hour under maximum CIU-OSM and RVU-CIU polling rates.

In addition to the above-mentioned functions, the CIU shall be designed in accordance with the following goals:

(22) The CJU shall incorporate provisions to minimize power consumption.

(23) The CIU shall incorporate provisions to minimize loss of information in its communications.

(24) The CIU shall incorporate provisions to assume degraded modes of operation to minimize the problem of CIU re-initialization.

(25) The CIU design shall provide maximum assurance that any attempt to override the TRANSEAVER system's control, to compromise the accuracy of the data being transmitted, or to provide access to that data by unauthorized persons shall be detected and reported to the RVU.

1.6 Universal Teleprinter Interface Functional Description

The UTI shall perform the following functions:

(1) The UTI shall obtain navigational data from a navigational satellite system through the NT.

(2) Ship speed, heading, longitude, latitude, date, and GMT shall compose the minimum set of data in the UTI. Additional data, if available, may also be used.

(3) The UTI shall communicate through the Communications Terminal to provide the navigational data to the RVU by responding to polls from the RVU.

(4) The UTI shall provide an interface link between the CIU and the CT without altering the encryption.

(5) The UTI shall provide navigational data to the RVU upon demand from the CIU.

1.7 Communications Terminal Functional Description

The Communications Terminal (CT) shall perform the following functions:

(1) The CT shall continuously receive a fixed-frequency carrier and continuously demultiplex from it the Assignment Channel and, when instructed, a telegraph channel.

(2) The CT shall automatically recognize messages addressed to the terminal on the Assignment Channel and automatically respond on the assigned ship-to-shore channel.

(3) The CT shall enable international telegraph messages to be semiautomatically sent to and automatically received from the domestic telegraph and telex networks via the shore station.

(4) The CT shall enable broadcast telegraph messages to be automatically received.

(5) The CT shall enable distress messages to be transmitted to the shore.

(6) The CT shall enable simplex telegraph messages to be sent.

(7) The CT shall enable the receiver and transmitter to be automatically tuned to any of 339 different frequency pairs within the operating frequency bands upon command via an Assignment Channel.

(8) The CT shall permit the automatic reception of a shore-to-ship simplex voice channel.

(9) The CT shall be capable of interfacing and providing power for the Universal Teleprinter Interface Unit.

(10) The CT antenna shall automatically lock in on a MARISAT at all times that the satellite is in view.

(11) The CT antenna shall be stabilized for ship motion.

(12) The CT interface to the UTI shall provide a data link to send encrypted data.

(13) The CT shall be compatible with the future INMARSAT system.

1.8 Navigational Terminal Functional Description

The Navigational Terminal (NT) shall perform the following functions:

(1) The NT shall automatically acquire satellite signals after initial operator settings have been entered.

(2) The NT shall derive position updates from satellite information obtained from each usable satellite pass.

(3) The NT shall continually track in an integrated complementary system that provides, automatically, between satellite passes, position updates at intervals of one minute or less.

(4) The NT shall acquire data consisting of, at least, speed, heading, longitude, latitude, date, and GMT.

(5) The NT shall acquire additional data, if practicable, of dead reckoning time, course and speed made good, set and drift, time and elevation of last satellite fix, and time and elevation of the next satellite pass.

(6) The NT shall provide interfacing for data transfer to the UTI and CIU.

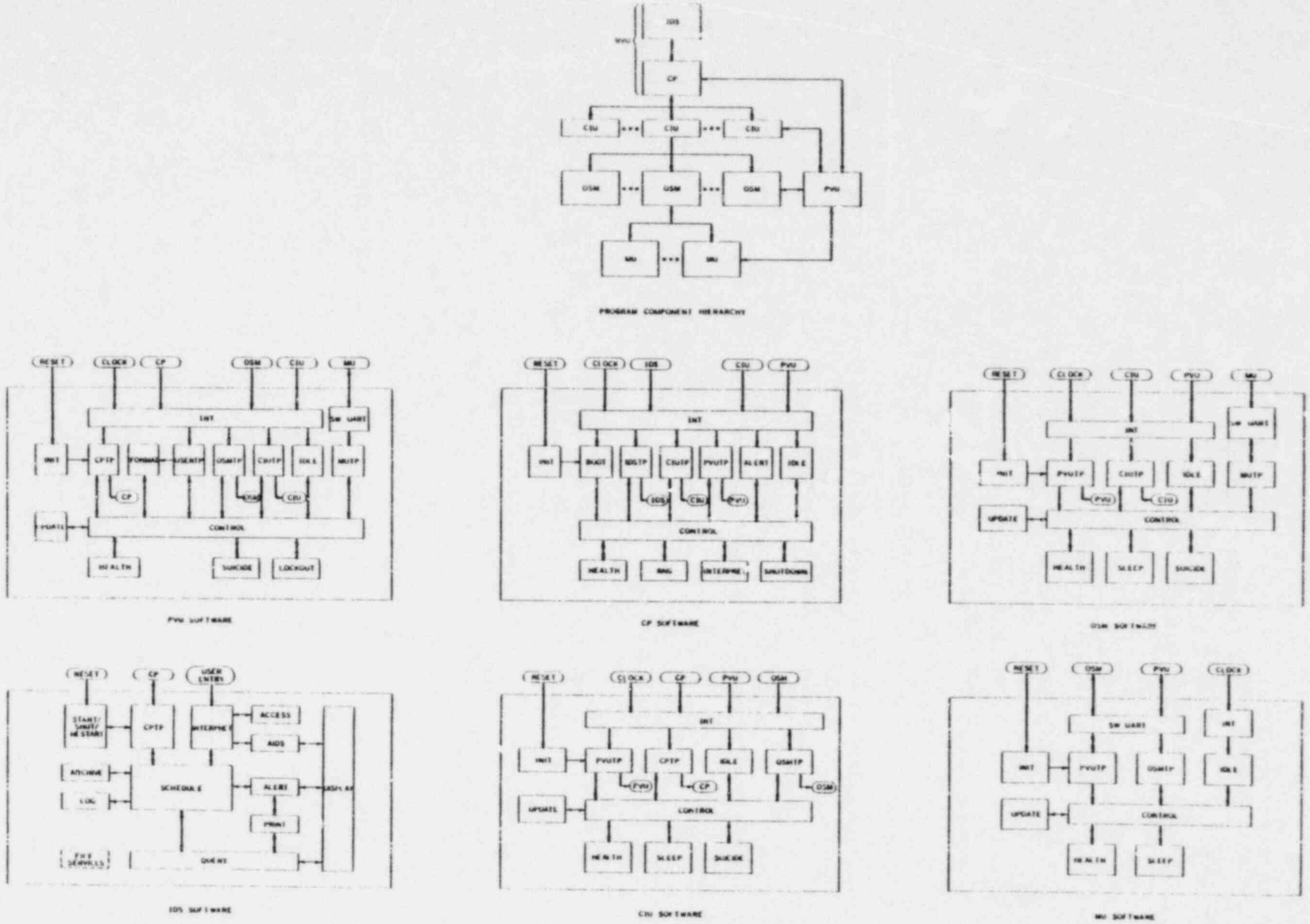
2. Data and Software Description

Each TRANSEAVER element shall have various data items within its own storage. Descriptions of the data items which shall be maintained by each TRANSEAVER element are presented in Table C-1. This table describes only the minimum data to be available and does not imply a required data base organization.

Presented in block diagram form in Figure C-1 is the software functional description. This layout follows the specifications in the functional descriptions of Section 1. A detailed description of the individual modules is contained in Table C-2.

3. Interface Description

The three categories of interface in TRANSEAVER are TRANSEAVER-sensor interfaces, intra-TRANSEAVER interfaces, and TRANSEAVER-inspector interfaces. The requirements for each of these interfaces are presented in the following sections.



PROGRAM COMPONENT HIERARCHY

PVU SOFTWARE

CP SOFTWARE

OSM SOFTWARE

IDS SOFTWARE

CIU SOFTWARE

MU SOFTWARE

Figure C-1 Software Block Diagram

TABLE C-1

REQUIRED TRANSEAVER DATA ITEMS

Data Item Name	Required at					Data Item Description
	MU	OSM	PVU	RVU	CIU	
MU Status (including)	X	X	X	X	X	
MU Identity						Uniquely determines one out of 30 MUs.
Current Sensor Status						Eight independent normal/abnormal conditions.
Historical Sensor Status						A record of abnormal sensor status occurrences.
Current MU Status (including)						
External Power						Normal/abnormal condition.
Internal Battery						Normal/abnormal condition.
MU-Sensor Cable Connection						Normal/abnormal condition.
Historical MU Status						A record of abnormal MU status occurrences.
MU-OSM Polling Status						Sufficient data to allow OSM to recognize that illicit polls of the MU have been made.
MU Cryptographic Parameters	X	X	X	X	X	Sufficient data to satisfy tamper resistance requirements.
OSM Status (including)		X	X	X	X	
OSM Identity						Uniquely determines one out of 500 OSMs.
MU Status						Data from up to 30 MUs.
Current OSM Status (including)						
External Power						Normal/abnormal condition.
Internal Battery						Normal/abnormal condition.
Intrusion						Normal/abnormal condition.
MU Responsiveness						30 independent normal/abnormal conditions.
MU Illicit Poll Recognition						30 independent normal/abnormal conditions.
Historical OSM Status						A record of abnormal OSM occurrences.
CIU-OSM Polling Status						Sufficient data to allow CIU to recognize that illicit polls of the OSM have been made.

TABLE C-1, Continued

	Required at					
Data Item Name	MU	OSM	PVU	RVU	CIU	Data Item Description
MU Function Commands		X	X	X	X	Sufficient data to command MU function execution.
OSM-MU Polling Parameters		X	X	X	X	Sufficient data to support a random process with a mean polling rate per MU.
OSM Historical Communications Activity Counts (including)		X	X	X	X	Sufficient data to tally establishment or communications at maximum possible OSM polling frequency for the maximum period expected between successive CIU polls of a particular OSM
RVU Communications Establishments						
PVU Communications Establishments						
Unsuccessful Communication Attempts						
Predefined MU Alert Status Conditions		X	X	X	X	Sufficient data to permit recognition of alert conditions in MU status data.
OSM Cryptographic Parameters		X	X	X	X	Sufficient data to satisfy tamper resistance requirements.
OSM Function Commands			X	X	X	Sufficient data to command OSM function execution.
Predefined OSM Alert Status Conditions			X	X	X	Sufficient data to recognize alerts in OSM status data.
CIU Status (including)			X	X	X	
CIU Identity						Uniquely determines one out of 500 CIUs.
OSM Status						Data from OSMs.
MU Status						Data from up to 30 MUs.
Current CIU Status (including)						
External Power						Normal/abnormal condition.
Internal Battery						Normal/abnormal condition.
Intrusion						Normal/abnormal condition.

TABLE C-1, Continued

	Required at					
Data Item Name	MU	OSM	PVU	RVU	CIU	Data Item Description
OSM Responsiveness						Normal/abnormal conditions.
OSM Illicit Poll Recognition						Normal/abnormal conditions.
Historical CIU Status						A record of abnormal CIU occurrences.
RVU-CIU Polling Status						Sufficient data to allow RVU to recognize that illicit polls of the CIU have been made.
MU Function Commands		X	X	X	X	Sufficient data to command MU function execution.
OSM-MU Polling Parameters and CIU-OSM Polling Parameters		X	X	X	X	Sufficient data to support a random process with a mean polling rate per MU.
CIU Historical Communications Activity Counts (including)			X	X	X	Sufficient data to tally establishment of communications at maximum possible CIU polling frequency for the maximum period expected between successive RVU polls of a particular CIU.
RVU Communications Establishments						
PVU Communications Establishments						
Unsuccessful Communication Attempts						
Predefined MU Alert Status Conditions		X	X	X	X	Sufficient data to permit recognition of alert conditions in MU status data.
RVU Communication Parameters					X	Sufficient data to allow the CIU to direct-dial the RVU.
CIU Cryptographic Parameters			X	X	X	Sufficient data to satisfy tamper resistance requirements.
CIU Function Commands			X	X	X	Sufficient data to command CIU function execution.

TABLE C-1, Continued

Data Item Name	Required at MU	OSM	PVU	RVU	CIU	Data Item Description
Predefined CIU Alert Status Conditions			X	X	X	Sufficient data to recognize alerts in CIU status data.
Site Configuration Parameters			X	X		Sufficient data tc initialize/change the MU/sensors combinations at a shipment.
Predefined PVU Alert Process			X			Sufficient data to allow a unique alert process for each alert status condition.
PVU Access Log			X			Self-explanatory.
RVU-CIU Polling Parameters (including)				X		
Polling Process Parameters						Sufficient data to support a random process with a mean polling rate per MU.
Recent CIU Communication History (including)						
Last Contact						Date and time of day.
Number of Unsuccessful Attempts Since Last Contact						Sufficient data to tally one attempt per hour for 30 days.
Predefined RVU Alert Process Response Parameters (including)				X		
Alert Process						Sufficient data to allow a unique alert process for each alert status conditions.
Local Telephone Parameters						Sufficient data to dial five different local telephone numbers.
Acknowledgements						Sufficient data to allow unique inspector acknowledgements for each alert status condition.

TABLE C-1, Continued

Data Item Name	Required at					Data Item Description
	MU	OSM	PVU	RVU	CIU	
Historical and Archive Records (including)				X		Self-explanatory.
CIU Status						
OSM Status						
Alert Status Conditions (including)						
Pending						
Acknowledged						
Communication Usage (including)						
Successful						
Attempted						
RVU Automatic Activities						
RVU Demand Activities						
RVU Accesses						
Narrative Data (including)				X		Self-explanatory.
Individual Sensors						
Individual Facilities						
Individual CIU Networks						
Individual OSM Networks						
Inspector Support (including)						
Prompts						
Assistance						

TABLE C-2

IDS MODULE DESCRIPTIONS

MODULE	DESCRIPTION
START/SHUT/RESTART	Start and Restart transmit microcode to the CP and initialize IDS memory from a checkpoint file. Shutdown saves IDS status on the checkpoint file and instructs the CP to shutdown.
CPTP	Provides a centralized interface to CP.
INTERPRET	Detects user inputs and performs preliminary interpretation of user keyins.
ACCESS	Validates user functions (primarily logon and function/data privileges).
AIDS	Provides user interaction assistance. It may be solicited (e.g., help) or unsolicited (e.g., error message).
ALERT	Detects alarm conditions, classifies them (type, severity), and initiates notification procedures (display, print, log, and local dialout).
QUERY	Performs parameter constrained file searches and generates hard and soft copy reports.
DISPLAY	Provides centralized control of the IDS CRT. This includes all soft copy output, data-to-window allocation and highlighting.
PRINT	Provides centralized control of the IDS printer.
ARCHIVE	Performs data base reorganization functions resulting in movement of certain data (e.g., old, obsolete) to an off-line storage medium.
LOG	Appends time and status tagged entries to the various TRANSEAVER logs.
SCHEDULE	Maintains a prioritized task queue and dispatches other IDS modules to perform task steps. The three primary sources of queue entries are the user, the automatic polling data file, and the alert detection module.

TABLE C-2, Continued

IDS MODULE DESCRIPTIONS

MODULE	DESCRIPTION
FILE SERVICES	Provides centralized file control services for all the above modules.

TABLE C-2, Continued

CP MODULE DESCRIPTIONS

MODULE	DESCRIPTION
INIT	Clear RAM, set up register allocations.
BOOT	Load RAM with all CP software except INIT, BOOT, INT, and certain utility routines.
IDSTP	Analyze IDS input buffer, determine function and post CONTROL indicating next step. Initiate transmission for complete IDS output buffer and post CONTROL when complete.
CIUTP	Initiate dialout to the CIU when needed. Manage the status of the communication line. When CIU input buffer is complete, decrypt, communication decode and post CONTROL. Initiate transmission for complete CIU output buffer, encrypt, communication code, and post CONTROL when complete.
PVUTP	Establish communication with the PVU. When PVU input buffer is complete, analyze and post CONTROL with PVU status. Initiate transmission for complete PVU output buffer and post CONTROL when complete.
ALERT	When alert condition exists, handle local dialout for alert process.
IDLE	Enable interrupts and wait for an interrupt.
INT	Determine whether a clock or I/O interrupt. If a clock interrupt, check I/O time-outs and post time-sequenced functions, e.g., dialout, random number collection. If an I/O interrupt, process next byte and post completion.
HEALTH	Perform self checks and post status. If a sufficiently severe condition exists, post CONTROL to call SHUTDOWN.
RNG	Maintain a buffer of random numbers.
INTERPRET	Analyze IDS user input buffer and translate into a function parameter list as appropriate.

TABLE C-2, Continued

CP MODULE DESCRIPTIONS

MODULE	DESCRIPTION
SHUTDOWN	Gracefully close out all active functions, e.g., complete buffers, disconnect phones. Maintain a tight loop responding to IDS queries with a shutdown message.
CONTROL	Maintain "next function" parameter. Perform an N-way branch to application.

TABLE C-2, Continued

CIU MODULE DESCRIPTIONS

MODULE	DESCRIPTION
INIT	Clear RAM, set up register allocations.
PVUTP	Receive, inspect, and change commands from PVU and update RAM. Echo back message when complete.
CPTP	Receive poll request from an RVU, after establishing telephone communication. Decrypt and perform command. Commands include status dumps, specific OSM polls and parameter modifications. Send status data as appropriate. Receive RVU acknowledgement. Receiving input is governed by a delay counter to prevent frequent CIU polls, thus delaying the discovery of an encryption key.
OSMTP	Initiate poll of the OSM. When OSM input buffer is complete, decrypt, communication decode and post CONTROL. Initiate transmission for complete OSM output buffer, encrypt, communication code, and post CONTROL when complete.
IDLE	Enable interrupts and wait for an interrupt.
INT	Determine whether a clock or I/O interrupt. If a clock interrupt, decrement delay counter for RVU input and SW UART timer. If an I/O interrupt, process next byte and post completion.
UPDATE	Gather self status, current and cumulative. Detect and post CIU/OSM/MU/sensor alert conditions.
HEALTH	Perform self checks and if a failure is encountered, wait for reinitialization.
SLEEP	Maintain parameter denoting the amount of time CIU will operate on battery. When time expires, suspend CIU activities until power is restored.
SUICIDE	Detect physical intrusion and clear memory.
CONTROL	Maintain "next function" parameter. Perform an N-way branch to application.

TABLE C-2, Continued

OSM MODULE DESCRIPTIONS

MODULE	DESCRIPTION
INIT	Clear RAM, set up register allocations.
PVUTP	Receive, inspect, and change commands from PVU and update RAM. Echo back message when complete.
CIUTP	Receive poll request from CIU, after establishing communication. Decrypt and perform command. Commands include status dumps, specific MU polls and parameter modifications. Send status data as appropriate. Receive CIU acknowledgement. Receiving input is governed by a delay counter to prevent frequent OSM polls, thus delaying the discovery of an encryption key.
MUTP	Scan MU polling parameters to determine time of next poll. If now, generate and send an MU poll request. Receive and store sensor and MU status. Send an acknowledgement. Generate time for next poll.
SW UART	Perform general I/O functions such as detecting input, receiving a byte, signaling output and transmitting a byte. Timing is consistent with SW UART in the MU.
IDLE	Enable interrupts and wait for an interrupt.
INT	Determine whether a clock or I/O interrupt. If a clock interrupt, decrement delay counter for RVU input and SW UART timer. If an I/O interrupt, process next byte and post completion.
UPDATE	Gather self status, current and cumulative. Detect and post OSM/MU/sensor alert conditions.
HEALTH	Perform self checks and if a failure is encountered, wait for reinitialization.
SLEEP	Maintain parameter denoting the amount of time OSM will operate on battery. When time expires, suspend OSM activities until power is restored.
SUICIDE	Detect physical intrusion and clear memory.

TABLE C-2, Continued)

OSM MODULE DESCRIPTIONS

MODULE	DESCRIPTION
CONTROL	Maintain "next function" parameter. Perform an N-way branch to application.

TABLE C-2, Continued

MU MODULE DESCRIPTIONS

MODULE	DESCRIPTION
INIT	Clear RAM, set up register allocations.
PVUTP	Receive, inspect, and change commands from PVU and update RAM. Echo back message when complete.
OSMTP	Receive poll request from an OSM, encrypt and respond with status information. Receive OSM acknowledgement. Receiving input is governed by a delay counter to prevent "communication collisions" because the OSM and all MUs communicate on the same data bus. Also it prevents an intruder from frequently polling an MU, thus delaying the discovery of the MU encryption key.
SW UART	Perform general I/O functions such as detecting input, receiving a byte, signaling output and transmitting a byte.
IDLE	Enable interrupts and wait for a clock interrupt.
INT	Decrement delay counter for OSM input and software UART timer.
UPDATE	Gather sensor and self status, current and cumulative.
HEALTH	Perform self checks and if a failure is encountered, wait for reinitialization under hardware control.
SLEEP	Maintain parameter denoting the amount of time MU will operate on battery. When time expires, suspend MU activities until power is restored.
CONTROL	Maintain "next function" parameter. Perform an N-way branch to applications.

TABLE C-2, Continued

PVU MODULE DESCRIPTIONS

MODULE	DESCRIPTION
INIT	Clear RAM, set up register allocations.
CPTP	Receive, echo back, and execute inspect and change command from CP and update RAM when requested.
FORMAT	Format buffer and output to CRT.
USERTP	Receive user input, interpret, and perform command. Commands include modify/display memory, enable "TPs" and control user access to PVU.
OSMTP	Issue inspect and change command and verify when initializing an OSM. Generate and send poll request, receive and store data and send acknowledgement when inspecting on OSM.
CIUTP	Issue inspect and change command and verify when initializing a CIU. Generate and send poll request, receive and store data, and send acknowledgement when inspecting a CIU.
MUTP	Issue inspect and change command and verify memory modifications when initializing an MU.
SW UART	Perform general I/O functions such as detecting input, receiving a byte, signaling output and transmitting a byte. Timing is consistent with SW UART in the MU.
IDLE	Enable interrupts and wait for an interrupt.
INT	Determine whether a clock or I/O interrupt. If a clock interrupt, decrement SW UART timer. If an I/O interrupt, process next byte and post completion.
UPDATE	Collect self status.
HEALTH	Perform self checks and if a failure is encountered, wait for reinitialization under hardware control.

TABLE C-2, Continued

PVU MODULE DESCRIPTIONS

MODULE	DESCRIPTION
SUICIDE	Detect physical intrusion. If condition is beyond a severity threshhold, clear memory.
LOCKOUT	Inspect parameter denoting number of unsuccessful login attempts. If too many, ignore login attempts for a certain time period.
CONTROL	Maintain "next function" parameter. Perform an N-way branch to application.

3.1 TRANSEAVER-Sensor Interface

TRANSEAVER shall interface to all sensors through an MU. Up to eight independent, normal/abnormal signals shall be provided by the sensor to the MU.

To simplify MU-sensor interface design, the MU shall provide the following to the sensor:

(1) +5V DC reference voltage

(2) Ground reference

(3) +11 to +15V DC at 5mA continuous power

(4) Logical "1" acknowledgement signal upon completion of obtaining sensor status.

Where possible, existing sensors that interface to this standard will be used. Otherwise, interfaces shall be designed as needed.

3.2 Intra-TRANSEAVER Interfaces

Table C-3 describes the required characteristics of the intra-TRANSEAVER interfaces. The data items that shall be transmitted across these interfaces are identified in Table C-4. This table only identifies the minimum information to be transmitted and does not imply a required message organization or transmission procedure. Note that all interfaces except PVU-MU are used in sensor status flow. The PVU interfaces are used for TRANSEAVER installation/maintenance and facility inspection. The PVU-MU interface is used only during MU installation. Subsequent use of the PVU will be at the OSM.

3.3 TRANSEAVER-Inspector Interfaces

TRANSEAVER shall interface to inspectors through the RVU or the PVU. These interfaces shall be used to:

(1) Alert inspectors to special situations.

(2) Provide control of TRANSEAVER automatic operations and present automatically generated outputs.

(3) Direct TRANSEAVER demand operations and present demand-generated outputs.

(4) Install TRANSEAVER elements.

TABLE C-3

INTRA-TRANSEAVER INTERFACE CHARACTERISTICS

	Interfaces					
	MU-OSM	MU-PVU	OSM-PVU	OSM-CIU	CIU-RVU	PVU-RVU
Purpose of Interface	Sensor/MU Status Update	Install MU Sensor, Trouble Shoot	Install TRANSEAVER on the Shipment, Trouble Shoot, Status Dump	Status Update	Status Update	Transfer Shipment OSM Parameters
Type of Interface	Wire Line Fiber Optics Option	Wire Line	Wire Line	Wire Line	MARISAT	Wire Line
Maximum Transaction** Rate (number/time)	1 per second	1 per 10 seconds	1 per 10 seconds	1 per 10 seconds	1 per 6 hours	2 per day
Maximum Transaction Time	1/30 second	1/3 second	1 second	1 second	3 minutes*	3 minutes
Initiator of Interface Communications	OSM	PVU	PVU	CIU	RVU	PVU

* Depending on communication quality.

**A transaction is a poll for the MU-OSM and OSM-RVU interfaces, and a command for the PVU interfaces.

TABLE C-4

INTRA-TRANSEAVER INTERFACE DATA ITEM TRANSMISSION REQUIREMENTS

Interface	Transmitted Data Items	Comments
Sensor to MU	Current Sensor Status	Each MU need receive data from only one sensor. A sensor need transmit a given data byte to only one MU. Sensors needing to transmit more than eight conditions will use multiple MUs.
MU to OSM	MU Status	Each OSM shall receive data from up to 30 MUs. Each MU need transmit data to only one OSM.
OSM to MU	MU Identity MU Function Command	Each MU need receive data from only one OSM. Each OSM shall transmit data to up to 30 MUs.
MU to PVU	MU Status	Each PVU shall receive data from up to 30 MUs. Each MU need transmit data to only one PVU.
PVU to MU	MU Identity MU Cryptographic Parameters MU Function Commands	Each MU need receive data from only one PVU. Each PVU shall transmit data to up to 30 MUs.
OSM to PVU	OSM Status OSM-MU Polling Parameters OSM Historical Activity Counts Predefined MU Alert Status Conditions RVU Telephone Parameters	Each PVU shall receive data from one OSM. Each OSM need transmit data to only one PVU.
PVU to OSM	OSM Identity MU Identity OSM Cryptographic Parameters MU Cryptographic Parameters OSM Function Commands OSM-MU Polling Parameters Predefined MU Alert Status Conditions RVU Telephone Parameters	Each OSM need receive data from only one PVU. Each PVU need transmit data to only one OSM.
OSM to CIU	OSM Status OSM-MU Polling Parameters OSM Historical Activity Counts Predefined MU Alert Status Conditions	The CIU shall receive data from several OSMs. Each OSM need transmit data to only one CIU.
CIU to OSM	OSM Identity MU Identity OSM Function Commands OSM-MU Polling Parameters Predefined MU Alert Status Conditions	The OSM need receive data from only one CIU. The CIU shall transmit data to many OSMs.
PVU to RVU	CIU-OSM Identity CIU-OSM Cryptographic Parameters CIU-OSM Status MU Status CIU-OSM-MU Polling Parameters Predefined MU Alert Status Conditions RVU Telephone Parameters	The RVU shall receive data from one PVU. Each PVU need transmit data to one RVU.

TABLE C-4, Continued

INTRA-TRANSEAVER INTERFACE DATA ITEM TRANSMISSION REQUIREMENTS

Interface	Transmitted Data Items	Comments
RVU to PVU	CIU-OSM Identity CIU-OSM Cryptographic Parameters Site Configuration Parameters	Each PVU need receive data from one RVU. The RVU shall transmit data to one PVU.
CIU to RVU	CIU-OSM Status CIU-OSM-MU Polling Parameters CIU-OSM Historical Activity Counts Predefined MU Alert Status Conditions Navigational Data and Alerts	The RVU shall receive data from up to 500 CIUs. Each CIU need transmit data to only one RVU.
RVU to CIU	CIU-OSM Identity MU Identity CIU-OSM Function Commands CIU-OSM-MU Polling Parameters Predefined MU Alert Status Conditions	The CIU need receive data from only one RVU. The RVU shall transmit data to up to 500 CIUs.

(5) Limit access to the TRANSEAVER system to authorized personnel and protect the TRANSEAVER system data from accidental or unauthorized actions.

Outputs from TRANSEAVER shall consist primarily of displays and printed reports.* Other outputs, consisting of audio-visual alarms and telephone calls, shall be used in alert notifications. All TRANSEAVER outputs shall be designed to include human factors considerations. Inputs to TRANSEAVER shall consist of function designation and parameter specification (when needed).** The RVU shall provide simple, easy-to-use interface features, including at least positive system response to inputs, clear error messages (to permit correction of entries), minimization of keystrokes, and a simple form of on-line assistance. The PVU shall provide at least the first three of the above features.

The following paragraphs describe the TRANSEAVER-inspector interface.

3.3.1 Alert Notification

The RVU, PVU, OSM, and CIU each have the capability to detect specified, predefined alert status conditions. The inspectors shall be notified about the detection of these conditions as follows:

(1) The RVU and PVU shall be able to generate special, preformated and/or predefined displays.

(2) The RVU shall be able to print special preformated and/or predefined reports.

(3) The RVU and PVU shall be able to activate special audio-visual alarm signals.

(4) The RVU shall be able to dial local telephone numbers to contact inspectors.

(5) The RVU shall be able to transmit a recognizable audio signal to a previously dialed and answered local telephone.

(6) The RVU shall be able to repeat a predefined alert process until input acknowledging the alert notification is received.

(7) The PVU shall be able to suspend further operations until an input acknowledging the alert notificaiton is received.

(8) Inspectors shall be able to predefine an RVU alert process to include any combination, in any order, of items (1) - (6).

* See Tables C-5 and C-6.

** See Tables C-7 and C-8.

TABLE C-5

PARTIAL LISTING OF RVU DISPLAYS AND REPORTS

RVU Display
- Power on display
- Login display
- Logoff display
- Poweroff display
- Prompts to manually establish communication link to CIU
- Successful establishment of communications with CIU display
- Unsuccessful attempt to establish communications with CIU display
- Establish communications with PVU display
- Terminate communications with CIU display
- Terminate communications with PVU display
- PVU initialization display
- Specific MU-sensor detailed status report display
- MU-sensor status summary display
- CIU status report display
- CIU communication status report display
- PVU status report display
- RVU status report display
- Specific sensor parameters display
- Summary sensor parameters display
- Specific MU parameters display
- Summary MU parameters display
- Specific CIU parameters display
- Specific CIU communication parameters display
- Specific PVU parameters display
- Summary PVU parameters display
- RVU parameters display
- Activity summary display
- Alert display
- Alert summary display
- Newly acquired status reports display
- Communication usage display
- RVU automatic activities display
- Inspector activities display
- Command CIU to transmit CIU status display
- Command CIU to transmit CIU parameters display
- Command CIU to transmit specified MU status display
- Command CIU to transmit specified MU parameters display
- Command CIU to transmit all MU status display
- Command CIU to transmit all MU parameters display
- Command CIU to poll a specified MU display
- Command CIU to poll all MUs display
- Command CIU to change CIU parameters display
- Command CIU to change specified MU parameters display
- Command RVU to poll a specified OSM display
- "Trip Planning" display

TABLE C-5, Continued

"Help" displays
Change criticality parameters display
Change sensor parameters display
Change MU parameters display
Change CIU parameters display
Change PVU parameters display
Change RVU parameters display
Alert notification display
Alert acknowledgement display

TABLE C-6

PARTIAL LISTING OF PVU DISPLAYS

PVU Displays

- Power on display
- Login display
- Access permanently set to status interrogation only display
- Logoff display
- Poweroff display
- Successful establishment of communications with CIU-OSM display
- Unsuccessful attempt to establish communications with CIU-OSM display
- Establish communications with RVU display
- Terminate communications with RVU display
- Terminate communications with CIU-OSM display
- Successful MU initialization display
- Unsuccessful MU initialization display
- Initialize CIU-OSM display (page 1)
- Initialize CIU-OSM display (page 2)
- PVU initialization from RVU display (page 1)
- PVU initialization from RVU display (page 2)
- Successful MU checkout display
- Defective MU display
- Successful CIU-OSM checkout display
- Defective CIU-OSM checkout display
- Successful PVU self check display
- Defective PVU display
- Specific MU detailed status report display
- MU status summary display (up to 6 pages)
- CIU-OSM status report display (page 1)
- CIU-OSM status report display (page 2)
- PVU status report display
- MU polling parameters display
- MU alert condition parameters display
- RVU telephone parameters display
- CIU-OSM initialization default values display
- Sensor (MU initialization) default parameters display
- Command OSM poll of all MUs display
- Command OSM poll of a specified MU display
- Command CIU poll of all OSM displays
- Command CIU poll of a specified OSM display
- Add an MU display
- Delete an MU display
- Change MU polling parameters display
- Change MU alert condition parameters display
- Change MU sensor type display
- Change sensor status mask display
- Change sensor default OSM-MU polling parameters display
- Change sensor default alert condition display
- Change RVU telephone number display

TABLE C-6, Continued

Change CIU-OSM default alert condition display
Change default RVU telephone number display
Change MU cryptographic parameters display
Change CIU-OSM cryptographic parameters display
Update CIU-OSM memory display
Update RVU data base display
Alert notification display
Alert acknowledgement display

TABLE C-7

PARTIAL LIST OF INSPECTOR COMMANDS TO RVU

- Inspector commands
  - Access commands
    - Power on
    - Logon
    - Logoff
    - Power off
  - Communications commands
    - Establish communications
      - Auto dial CIU
      - Manual dial CIU
      - With PVU
    - Terminate communications
      - With CIU
      - With PVU
  - Initialization commands
    - Initialize PVU
  - Interrogation commands
    - Status reports
      - Sensor
      - MU
      - CIU
      - CIU communication
      - PVU
      - RVU
    - Parameter reports
      - Sensor
      - MU
      - OSM
      - CIU
      - CIU communication
      - PVU
      - RVU
    - Activity reports
      - Time period summaries
      - Alerts
      - Newly acquired status reports
      - Communication usage
      - RVU automatic activites
      - Inspector directed activities
    - Display next page
    - Print hard copy
  - Action commands
    - Command CIU to
      - Transmit CIU status
      - Transmit CIU Parameters
      - Transmit OSM status

TABLE C-7, Continued

```
          Transmit OSM parameters
          Transmit specified MU status
          Transmit specified MU parameters
          Transmit all MU status
          Transmit all MU parameters
          Poll a specified MU
          Poll all MUs
          Change CIU parameters
          Change OSM parameters
          Change specified MU parameters
     RVU
          Poll a specified CIU
     "Trip Planning"
     "Help"
Update commands
     Change criticality parameters
     Change sensor parameters
     Change MU parameters
     Change OSM parameters
     Change CIU parameters
     Change PVU parameters
     Change RVU parameters
     Update sensor, MU, OSM, and CIU status based upon PVU inputs
Alert acknowledgement
```

TABLE C-8

PARTIAL LISTING OF INSPECTOR COMMANDS TO PVU

- Inspector commands
    - Access commands
        - Power on
        - Logon
        - Permanently set access to status interrogation only
        - Logoff
        - Power off
    - Communcations commands
        - Establish communications
            - With OSM
            - With CIU
            - With RVU
        - Terminate communications
            - With OSM
            - With CIU
            - With RVU
    - Initialization commands
        - Initialize MU
        - Initialize OSM
        - Initialize CIU
        - Accept PVU initialization from RVU
    - Diagnostic commands
        - Check out MU
        - Check out OSM
        - Check out CIU
        - Self check PVU
    - Interrogation commands
        - Status reports
            - MU
            - OSM
            - CIU
            - PVU
        - CIU operating parameter reports
            - OSM polling parameters
            - Alert status condition parameters
            - RVU communication initiation parameters
        - OSM operating parameter reports
            - MU polling parameters
            - Alert status condition parameters
        - PVU operating parameter reports
            - Sensor parameter default values
            - OSM initialization default values
            - CIU initialization default values
            - Sensor parameters
        - Display next page

TABLE C-8, Continued

- Action commands
  - OSM poll all MUs
  - OSM poll a specified MU
  - CIU poll all OSMs
  - CIU poll a specified OSM
- Update commands
  - Change onboard configuration
    - Add MU
    - Delete MU
  - Change OSM operating parameters
    - MU polling parameters
    - Alert status condition parameters
  - Change CIU operating parameters
    - OSM polling parameters
    - Alert status condition parameters
    - RVU communication initiation parameters
  - Change PVU operating parameters
    - Sensor parameter default values
    - CIU-OSM initialization default values
    - Sensor parameters
    - MU cryptographic parameters
    - CIU-OSM cryptographic parameters
  - Update CIU-OSM memory
  - Update RVU data base
- Alert acknowledgement

(9) Inspectors shall be able to predefine a PVU alert process to be item (1); items (1) and (3), or items (1), (3), and (7).

(10) Inspectors shall be able to define a unique alert process for any given alert status condition.

(11) Inspectors shall be able to define a common alert process for two or more alert status conditions.

(12) Inspectors shall be able to acknowledge all alerts with special inputs and messages entered at the RVU or PVU as appropriate.

(13) Inspectors shall be able to acknowledge locally telephoned alert notifications by a predefined telephone touch-tone sequence.

3.3.2 Automatic Operation Interface

The RVU provides the primary automatic operation interface of the TRANSEAVER system. The PVU provides supplementary automatic operation interface capability at CIU-OSM sites. This automatic operation interface shall consist of the following:

(1) Upon inspector command, the RVU (having established a link with a specified CIU-OSM) and PVU shall command the CIU-OSM to alter OSM-MU polling parameters, predefined MU alert status conditions, or the RVU telephone parameters.

(2) Upon inspector command, the RVU shall alter its predefined MU alert status conditions, predefined CIU-OSM alert status conditions, predefined RVU alert process parameters, RVU-CIU polling parameters, and any narrative data.

(3) Upon inspector input, the PVU shall alter its predefined CIU alert status conditions and predefined alert process parameters.

(4) The inspector shall be able to designate any display or printed report for automatic generation after passing of a specified time interval.

(5) The RVU shall present automatically generated displays at the RVU console.

(6) The RVU shall print automatically generated reports on the RVU line printer.

(7) The PVU shall present automatically generated displays on its self-contained display.

3.3.3 Demand Operation Interface

The RVU provides the primary demand operation interface of the TRANSEAVER system. The PVU provides supplementary demand operation interface at CIU-OSM sites. This demand operation interface shall consist of the following:

(1) Upon inspector input, the RVU or PVU shall immediately execute any of its ʻunctions and display tʼe results of the execution.

(2) The RVU shall present demand-generated displays at the RVU console.

(3) Upon inspector command, any predetermined display on the RVU console shall be printed on the RVU line printer.

(4) The RVU shall print demand-generated reports on the RVU line printer.

(5) The PVU shall present demand-generated displays on its self-contained output device.

(6) All PVU displays shall be completed within three seconds after inspector command, except for those reports that require CIU-OSM interrogation. The latter reports shall be displayed within three.seconds of receipt of the necessary data by the PVU. An intervening "wait" display shall be presented to assure the operator that the PVU is still operating.

(7) Upon inspector command, the RVU shall move portions of the historical and archive records to an off-line medium.

(8) Upon inspector command, the RVU shall load portions of the historical archive records from an off-line medium.

(9) Historical and archive record movement shall be selectable based on record type (including, at least, CIU-OSM status, alert status conditions, telephone usage, RVU automatic activities, RVU access log, and operator activities), record time (within a specified time period), or record geographic location.

(10) historical and archive record movement shall not interfere with other RVU functions.

3.3.4 TRANSEAVER Subsystem Installation

The PVU is the on-site CIU, OSM, and MU installation and fault isolation tool. The RVU provides remote fault isolation data at a central facility. The PVU and RVU shall provide the following capabilities:

(1) Upon inspector input, the PVU shall initialize an MU by providing to the MU at least the MU identity and MU cryptographic parameters.

(2) Upon inspector input, the PVU shall initialize an OSM by providing to the OSM at least the OSM identity, OSM cryptographic parameters, OSM-MU polling parameters, OSM historical activity counts, predefined MU alert status conditions, RVU communication parameters, attached MU identities, and attached MU cryptographic parameters.

(3) Upon inspector input, the PVU shall attach one or more additional MUs to an OSM by providing to the OSM at least the additional MU identities and additional MU cryptographic parameters.

(4) Upon inspector input, the PVU shall delete one or more MUs from the OSM.

(5) Upon inspector input, the PVU shall initialize a CIU by providing to the CIU at least the CIU identity, CIU cryptographic parameters, CIU-OSM polling parameters, CIU historical activity counts, predefined OSM alert status conditions, RVU communication parameters, attached MU identities, and attached MU cryptographic parameters.

(6) Upon inspector input, the PVU shall attach one or more additional OSMs to a CIU by providing to the CIU at least the additional OSM identites, and additional OSM cryptographic parameters.

(7) Upon inspector input, the PVU shall delete one or more OSMs from the CIU.

(8) The PVU shall be able to provide default values for any initialization parameters.

(9) The inspector shall be able to input values for any initialization parameter.

(10) Upon inspector input, the PVU and RVU (having established a link with a specified CIU) shall display the values of any CIU, OSM, or MU data element.

(11) Upon inspector input, the PVU and RVU (having established a link with a specified CIU) shall alter the values of any CIU, OSM, or MU data element.

(12) Upon inspector input, the PVU and RVU (having established a link with a specified CIU) shall command the CIU or its attached CIUs and MUs to execute any of its functions and shall display the results of the execution.

3.3.5 Access Control

Both the RVU and PVU shall minimize unauthorized access to their respective data and functions. Hardware and software provisions will be included to address the following goals within the constraints of cost, size, and power and within the imposed state of available technology.

(1) The RVU and PVU access procedures shall be designed to prevent unauthorized users.

(2) The RVU and PVU shall log all access attempts.

(3) Three repeated unsuccessful PVU access attempts shall cause the PVU to selectively clear its memory and become inoperative.

(4) Three repeated unsuccessful RVU access attempts shall be an alert status condition.

(5) PVU users shall not be able to alter the PVU access log.

(6) RVU users shall not be able to alter the RVU historical and archive records.

(7) A TRANSEAVER access connection shall be severed after five minutes of user inactivity.

APPENDIX D

TRANSEAVER GENERA' SERVICE REQUIREMENTS

In addition to satisfying the specific functional requirements delineated in Appendix C, the TRANSEAVER system must also satisfy several general service requirements including operation under adverse environmental conditions and operation despite attempts by unknown parties to deceive or subvert system elements. Further, TRANSEAVER elements must satisfy overall system reliability, maintainability, safety, and packaging requirements. These general service requirements are specified in the following sections.

1. Environmental Requirements

As a minimum, the MU, OSM, CIU, PVU, and RVU shall withstand the environmental conditions delineated in Table D-1. In addition, for protection against electro-magnetic interference (EMI), the MU, OSM CIU, and PVU shall conform to the applicable portions of IEEE Standar, 472-1974 and shall be able to pass the UL Dust Test. Further, both t e MU and PVU shall be able to pass the UL Shock Test; and the MU shall be able to pass the UL Rain Test.

2. Tamper Indication and Resistance Requirements

TRANSEAVER must be able to function despite possible attempts by unknown parties to disrupt or deceive TRANSEAVER elements. To this end, the TRANSEAVER system must incorporate both physical and operational measures to detect and/or resist tamper attempts. As a minimum, TRANSEAVER elements and interfaces shall include the tamper indication/resistance measures listed in Tables D-2 and D-3.

3. Maintainability Requirements

TRANSEAVER elements, other than the RVU, shall be designed for maintenance by replacement. The RVU shall be maintained by preventative maintenance and standard data processing repair procedures.

The MU and inexpensive components in the MU-OSM link shall be designed to be "throw away" units. Other communication components, OSMs, CIUs, and PVUs shall be returned to a central maintenance facility to be repaired.

4. Safety Requirements

TRANSEAVER elements must incorporate fail-safe provisions and human factor considerations (such as rounded corners, appropriate markings, and one-way connectors) to assure that no electrical or other hazard exists to maintenance or other personnel. Since it is not feasible to demonstrate conformance to all potential standards, TRANSEAVER elements, as a minimum,

TABLE D-1

ENVIRONMENTAL REQUIREMENTS

	System Element					
Environmental Condition	Monitoring Unit	On-Site Multiplexor	Communication Interface Unit	Portable Verification Unit	Remote Verification Unit	Communication Equipment
Temperature (Celsius)	0 to +50*	+10 to +50	+10 to +50	0 to +50	+10 to +50	+10 to +50
Altitude (Meters)						
Operating	0 - 3,000	0 - 3,000	0 - 3,000	0 - 3,000	0 - 3,000	0 - 3,000
Storage	0 - 10,000	0 - 10,000	0 - 10,000	0 - 10,000	0 - 3,000	0 - 10,000
Relative Humidity (%)	20 - 100 (with condensation)	20 - 95	20 - 95	20 - 95	20 - 95	20 - 95
Radiation (Rads/3 years)	10^4	10^4	10^4	10^4	10^2	10^2

*Specific facility installation may require operation over a broader temperature range. In this event, additional provisions will be made for the basic MU and for the PVU during installation, if necessary.

TABLE D-2

REQUIRED TAMPER INDICATION/RESISTANCE MEASURES - SYSTEM ELEMENT

	System Element						
Requirement	Monitoring Unit	On-Site Multiplexor	Communication Interface Unit	Portable Verification Unit	Remote Verification Unit	Communications Equipment	Remarks
PHYSICAL MEASURES							
Power Status Sensing/ Reporting	Yes	Yes	Yes	No	Yes	Yes	Detect disconnect
Memory Protection Upon Power Off	Yes	Yes	Yes	Yes	N/A	Yes	Survive power loss
Protective Potting	Total**	Selected Modules	Selected Modules	Selected Modules	No	No	Encryption keys protected
Physical Penetration Detection	N/A**	Yes	Yes	Yes	No	Yes	Detect intrusion
Critical Memory Erasure Upon Penetration	N/A**	Yes	Yes	Yes	No	Yes	Protect encryption keys
Detect and Record Abnormal Opening of Housing	N/A**	Yes	Yes	Yes	No	Yes	Detect intrusion
Detect and Record Normal Opening of Housing	N/A**	Yes	Yes	Yes	No	Yes	Record rate of inspection
OPERATIONAL MEASURES							
Record Unsuccessful Transaction* Attempt	Yes	Yes	Yes	Yes	Yes	No	Detect possible intruder

TABLE D-2, Continued

Requirement	System Element						Remarks
	Monitoring Unit	On-Site Multiplexor	Communication Interface Unit	Portable Verification Unit	Remote Verification Unit	Communications Equipment	
Record Successful Transaction* Activity	Yes	Yes	Yes	Yes	Yes	No	Record rate of use
Limit Transaction* Rate	Yes (1 per sec)	Yes (1 per 10 sec)	Yes (1 per 5 min)	Yes (after 3 unsuccessful attempts)	Yes (after 3 unsuccessful attempts)	N/A	Protect from forced cycling or tie-up
Record Invalid Transaction* Responses	N/A	Yes	Yes	Yes	Yes	N/A	Detect possible intruder
Log Transaction* and Activities	N/A	N/A	N/A	Yes	Yes	N/A	Record rate of transactions
Prohibit Changing of Logs and Historical Data	N/A	N/A	N/A	Yes	Yes	N/A	Protect records

* A transaction is a poll for the CIU, OSM, and MU or a logon for the RVU/PVU.

** MU will be potted thereby requiring physical destruction to penetrate.

TABLE D-3

REQUIRED TAMPER INDICATION/RESISTANCE MEASURES - SYSTEM INTERFACES

Requirement	MU-Sensor	MU-OSM	MU-PVU	OSM-PVU	OSM-CIU	CIU-RVU	PVU-RVU	PVU-Inspector	RVU-Inspector
PHYSICAL MEASURES									
Detect Physical Disconnect	Yes	Yes	No	No	No	Disconnect Part of Normal Operations	No	N/A	N/A
OPERATIONAL MEASURES									
Encrypt Communications	No	Yes	Yes	Yes	Yes	Yes	No	No	No
Password Access Protection	No	Optional	Optional	Optional	Optional	Optional	Optional	Yes	Yes

shall conform to the appropriate portions of the UL standards listed in Table D-4.

5. Packaging Requirements

All TRANSEAVER elements shall satisfy the following general packaging requirements:

(1) The type and color of paint or other coating to be applied to the TRANSEAVER elements shall be specified by the ACDA.

(2) Different system elements shall be readily identifiable by their external appearance.

(3) Each element shall have an identification number visible on the outside for use in inventory control.

Individual TRANSEAVER elements (except for the RVU) shall satisfy the specific requirements presented in Table D-5. No specified packaging requirements apply to the RVU, with the possible exception of the operator console, since the RVU is expected to be a commercially available, general-purpose computer.

6. Reliability and Survivability Requirements

The TRANSEAVER system will be designed to support three modes of operation:

(1) Primary Mode:
Supports all TRANSEAVER system functions under site power (normal or emergency);

(2) Back-Up Mode (on-board devices):
Same as primary mode except under battery power (applies during power change-over operations); and

(3) Quiescent Mode (on-board devices):
Under the quiescent mode none of the primary system functions are supported, i.e., changes to sensor state are not recorded nor are these changes communicated.

The secondary functions supported by the quiescent mode are to retain:

(1) Memory of MU/sensor initialization data,

(2) Memory of encryption parameters, and

(3) Memory of sensor state prior to entering quiescent mode.

As such, the quiescent mode permits a site TRANSEAVER system to be automatically revived after extended power outages.

TABLE D-4

SAFETY REQUIREMENTS

UL Standards	System Element				
	Monitoring Unit	On Site Multiplexor	Communication Interface Unit	Portable Verification Unit	Remote Verification Unit
#796 Printed Wiring Board, Electrical	X	X	X	X	X
#478 Data-Processing Units and Systems, Electronic					X
#611 Burglar Alarm Units and Systems, Central Station		X	X		X
#609 Burglar Alarm Units and Systems, Local	X			X	

UL Standards	System Interfaces					
	MU-Sensor	MU-OSM	MU-PVU	OSM-PVU	OSM-CIU	CIU-RVU
#634 Connectors and Switches for Use with Burglar Alarm Systems	X	X	X	X	X	X

TABLE D-5

PACKAGING MAXIMUM SIZES (INCLUDING BATTERIES)

Element	Size (cm)	Weight (kg)	Field Assembly
MU	8 x 13 x 3	0.5	None
OSM	45 x 45 x 60	25	Minimal
CIU	45 x 45 x 60	25	Minimal
PVU*	15 x 30 x 45	15	None

*Must fit under airline seat

7. Reliability Goals

TRANSEAVER system hardware will be fabricated using the best available commercial components consistent with cost and other constraints on the hardware design (heat dissipation, fabrication procedures, workmanship). Table D-6 shows, by device, goals associated with system reliability. The mean-time-to-repair estimates assume that spare parts are available and that either devices (MU) or boards are replaced. At the completion of the hardware design effort, quantitative estimates will be made for the operating life (failure rate) and reliability of the system and its major subsystems.

TABLE D-6

TRANSEAVER RELIABILITY GOALS

Subsystem	Reliability*	MTTRR**
MU	.95	1 hour
OSM	.9	1 hour
CIU	.9	1 hour
PVU	.9	2 hours
RVU	.9	2 hours

*likelihood of no-fault operation for 3 years
**mean-time-to-repair-or-replace (after diagnosis)

APPENDIX E
PROJECT QUALITY ASSURANCE PLAN

ENERGY INCORPORATED
IDAHO FALLS, IDAHO

PROJECT QUALITY ASSURANCE PLAN

QAPP-ACDA-201

TRANSPORTATION BY SEA VERIFICATION
(TRANSEAVER)

FOR

ARMS CONTROL AND DISARMAMENT AGENCY
(ACDA)

APPROVED BY: ______________________________ ____________________
PROJECT MANAGER DATE

______________________________ ____________________
QUALITY ASSURANCE MANAGER DATE

TABLE OF CONTENTS

SECTION	TITLE	PAGE
--	INTRODUCTION	ii
1.0	ORGANIZATION	1
2.0	QUALITY ASSURANCE PROGRAM	1
3.0	DESIGN AND ANALYSIS CONTROL	1
4.0	PROCUREMENT DOCUMENT CONTROL	1
5.0	PROCEDURES, INSTRUCTIONS, AND DRAWINGS	1
6.0	DOCUMENT CONTROL	2
7.0	CONTROL OF PURCHASED MATERIAL, EQUIPMENT, AND SERVICES	2
8.0	IDENTIFICATION AND CONTROL OF MATERIALS, PARTS, AND COMPONENTS	2
9.0	CONTROL OF SPECIAL PROCESSES	2
10.0	INSPECTION	2
11.0	TEST CONTROL	3
12.0	CONTROL OF MEASURING AND TEST EQUIPMENT	3
13.0	HANDLING, STORAGE, AND SHIPPING	3
14.0	INSPECTION, TEST, AND OPERATING STATUS	3
15.0	NONCONFORMING MATERIALS, PARTS, AND COMPONENTS	3
16.0	CORRECTIVE ACTION	3
17.0	QUALITY ASSURANCE RECORDS	4
18.0	AUDITS	4

INTRODUCTION

This Project Quality Assurance Plan defines the program Energy Incorporated (EI) shall implement to comply with the quality assurance requirements during Phases II and III for the Transportation by Sea Verification System (TRANSEAVER). The plan will provide the monitoring necessary for verification that project criteria are met. Audits and surveillances will be performed during design, procurement, fabrication, and engineering activities to assure compliance with the plan.

1.0 ORGANIZATION

The organizational structure of Energy Incorporated and the duties and responsibilities of key individuals shall be as described in Section 1.0 of the EI Quality Assurance Manual and Section 1.0 of the EI Engineering Procedures Manual. This manual section (1.0) is applicable to this project in its entirety.

2.0 QUALITY ASSURANCE PROGRAM

Section 2.0 of the EI Qualit, Assurance Manual dealing with QA manuals, QA procedures, and training is applicable to this project in its entirety.

3.0 DESIGN AND ANALYSIS CONTROL

Section 3.0 of the EI Quality Assurance Manual and Section 4.0 of the EI Engineering Procedures Manual dealing with design and analysis control are applicable to this project in their entirety plus the following requirements.

3.1 After original approval by ACDA, proposed design changes shall be submitted to ACDA for review and comment prior to their implementation.

4.0 PROCUREMENT DOCUMENT CONTROL

All procurement documentation required will conform to Section 4.0 of the EI Quality Assurance Manual in its entirety and to the EI Procurement Procedures.

5.0 PROCEDURES, INSTRUCTIONS, AND DRAWINGS

Section 5.0 of the EI Quality Assurance Manual and Section 4.0 of the EI Engineering Procedures Manual will apply in their entirety to Phase II of this project.

6.0 DOCUMENT CONTROL

Section 6.0 of the EI Quality Assurance Manual and Section 5.0 of the EI Engineering Procedures Manual, will apply in their entirety to Phase II of this project.

7.0 CONTROL OF PURCHASED MATERIAL, EQUIPMENT, AND SERVICES

Section 7.0 of the EI Quality Assurance Manual is applicable to this project in its entirety and is supplemented as follows.

7.1 Source inspection plans shall be prepared, as required, concurrent with the preparation of the quality assurance requirements for the procurement package.

7.2 Source inspection plans shall be submitted to ACDA for review and concurrence prior to implementation.

8.0 IDENTIFICATION AND CONTROL OF MATERIALS, PARTS, AND COMPONENTS

Section 8.0 of the EI Quality Assurance Manual will apply in its entirety to Phase II of this project.

9.0 CONTROL OF SPECIAL PROCESSES

Section 9.0 of the EI Quality Assurance Manual and Section 4.0 of the EI Engineering Procedures Manual will apply in their entirety to Phase II of this project.

10.0 INSPECTION

Section 10.0 of the EI Quality Assurance Manual is applicable to Phase II in its entirety as it applies to source inspection plans prepared by EI and source inspections conducted by EI.

11.0 TEST CONTROL

Section 11.0 of the EI Quality Assurance Manual and Section 4.0 of EI Engineering Procedures Manual will apply in their entirety to Phase II of this project.

12.0 CONTROL OF MEASURING AND TEST EQUIPMENT

Section 12.0 of the EI Quality Assurance Manual will apply in its entirety to Phase II of this project.

13.0 HANDLING, STORAGE, AND SHIPPING

Section 13 of the EI Quality Assurance Manual will apply in its entirety to Phase II of this project.

14.0 INSPECTION, TEST, AND OPERATING STATUS

Section 14 of the EI Quality Assurance Manual will apply in its entirety to Phase II of this project.

15.0 NONCONFORMING MATERIALS, PARTS, AND COMPONENTS

Section 15 of the EI Quality Assurance Manual will apply in its entirety to Phase II of this project.

16.0 CORRECTIVE ACTION

Section 16.0 of the EI Quality Assurance Manual is applicable to this project in its entirety with the additional requirement that all corrective action and followup documentation shall be provided to ACDA.

17.0 QUALITY ASSURANCE RECORDS

Section 17.0 of the EI Quality Assurance Manual is applicable to this project in its entirety. These requirements shall extend to, as a minimum, the following documents.

17.1 System and Component Descriptions, Specifications, and Drawings

17.2 Design Calculations, Reports, and Computer Codes

17.3 Inspection, Examination, Audit, and Test Reports

17.4 Quality Assurance Program Policies and Procedures

17.5 Design Review Reports

18.0 AUDITS

Section 18.0 of the EI Quality Assurance Manual is applicable to this project in its entirety. An audit shall be scheduled for this project at a time appropriate to determine that the organization is performing the function as required by the quality assurance program.

NRC FORM 335
(7 77)

U.S. NUCLEAR REGULATORY COMMISSION
BIBLIOGRAPHIC DATA SHEET

1. REPORT NUMBER *(Assigned by DDC)*
NUREG/CR-2169

4. TITLE AND SUBTITLE *(Add Volume No., if appropriate)*
TRANSEAVER/TRANsport-by-SEA-VERification

2. *(Leave blank)*

3. RECIPIENT'S ACCESSION NO.

7. AUTHOR(S)
B.R. Peterson, D.L. Small, O.L. Green, R.W. Griebe

5. DATE REPORT COMPLETED
MONTH May
YEAR 1981

9. PERFORMING ORGANIZATION NAME AND MAILING ADDRESS *(Include Zip Code)*

Energy Incorporated
P.O. Box 736
Idaho Falls, ID 83401

Under Subcontract to
U.S. Arms Control and
Disarmament Agency
320 21st Street, NW
Washington, DC 20451

DATE REPORT ISSUED
MONTH June
YEAR 1981

6. *(Leave blank)*

8. *(Leave blank)*

12. SPONSORING ORGANIZATION NAME AND MAILING ADDRESS *(Include Zip Code)*

Division of Safeguards
Office of Nuclear Material Safety and Safeguards
U.S. Nuclear Regulatory Commission
Washington, DC 20555

10. PROJECT/TASK/WORK UNIT NO.

11. CONTRACT NO.
FIN B7302

13. TYPE OF REPORT
FINAL REPORT

PERIOD COVERED *(Inclusive dates)*
9/29/80 - 5/15/81

15. SUPPLEMENTARY NOTES

14. *(Leave blank)*

16. ABSTRACT *(200 words or less)*

A conceptual design for TRANSEAVER, Transport by Sea Verification, has been completed which shows the system could be a cost effective way to enhance safeguarding strategic and special nuclear materials during transport at sea. Applicable federal regulations and international guidelines have been considered with the expectation that TRANSEAVER will assist in meeting legal and regulatory considerations when used to monitor shipments. Utilizing existing RECOVER components and commercially available sensors, TRANSEAVER's link to a land-based command console is via MARISAT ship-to shore communications equipment. Licensed shipping casks are enclosed in a security contrainer and placed into a required closed van cargo container for a multiple boundary configuration which allows effective use of multiple sensor configurations. Any deviation from planned course or attempted tampering with the protected cargo automatically produces an Alerting Report at the command console.

17. KEY WORDS AND DOCUMENT ANALYSIS

17a. DESCRIPTORS

Safeguards
Physical Security
Special Nuclear Material
Satellite
MARISAT
Non-Proliferation
Maritime Communications

17b. IDENTIFIERS/OPEN-ENDED TERMS

18. AVAILABILITY STATEMENT
Unlimited

19. SECURITY CLASS *(This report)*
Unclassified

21. NO. OF PAGES

20. SECURITY CLASS *(This page)*
Unclassified

22. PRICE
$