Advanced Communications Project

Shipboard Communications Center Modernization Recommendations Report

Prepared for
The United States Coast Guard
Research & Development Center
1082 Shennecossett Rd.
Groton, CT 06340-6096

By
PRC Inc. and
VisiCom Laboratories Inc.
Via
Volpe NTSC

August 1995

CUTTER MODERNIZATION REPORT

FOR THE

UNITED STATES COAST GUARD

CUTTER COMMUNICATIONS CENTER

MODERNIZATION PROJECT

14 July 1995

Submitted to:

PRC, Inc.
1 Kendall Square
Building 200, Suite 2200
Cambridge, MA 02139

Submitted by:

VisiCom Laboratories, Inc.
41 N. Jefferson Street
Pensacola, FL 32561

EXECUTIVE SUMMARY

Background. This report presents the results of a communications system modernization study for the radio room of the U.S. Coast Guard (USCG) high endurance cutter (WHEC) and medium endurance cutter (WMEC). A four step sequential analysis approach was undertaken in the production of this report. Step 1 characterized the WHEC and WMEC operational environment. Based upon this environmental characterization, the mission and operational requirements were then determined in step 2. During step 3, technical requirements were derived from the operational requirements. Finally in step 4 and from the technical requirements, a recommended communications modernization approach and architecture was proposed.

Previous trade-off studies and analysis have focused on identifying and assessing requirements for functional modifications and additions to existing system components supporting USCG operations. This report presents options and recommendations to the USCG on how to improve USCG communications capabilities within a modular architectural framework that is independent of specific spectrum, radios, modems or processing equipment. This approach allows trade-off's concerning equipment types and transition mechanisms to be performed within the context of a well-defined and established architectural framework. This accommodates existing USCG high frequency (HF) and satellite communications (SATCOM) systems as well as near-term upgrades and/or enhanced capabilities such as International Maritime Satellite (INMARSAT), Iridium, and Naval Modular Automated Communication Subsystem (NAVMACS) Model II. In this manner, the individual components can be analyzed in greater depth with an understanding of their individual place in the overall system.

The approach and architecture of this modernization report is derived from comparable efforts to improve the US Navy's communications architecture. Like the Coast Guard, though at a much larger order of magnitude, existing Navy systems have been vertically integrated from user to antenna. Consequently, implementation of a new radio had dramatic impact upon implementation of the data processing equipment connected to the radio. Consequently, these communication systems and networks have been developed and deployed by individual user communities to provide specific communications capability (i.e., communication of perishable tactical data, record traffic, navigation data, etc.). This has resulted in a communications architecture characterized by a large number of separate, non-interoperable, vertically organized communications systems. This "stove pipe" approach has significant inherent limitations in terms of communication system performance and implementation. The communication systems are "fragile" under conditions of stress. If a particular communication resource is lost, it is difficult to reconfigure other communications resources to compensate for this loss. These systems are not interoperable. It is difficult to rapidly route data between individual systems and the overall composite system cannot respond to imbalances in the traffic load. One communications resource may be under-utilized while the capacity of another is being exceeded or backlogged. From the perspective of operational maintenance, the lack of an overall systems approach makes it impossible to perform system level diagnostics or to provide automated assistance to operational personnel. In terms of system development, development costs are high as each communication system development is done as an independent program. Furthermore, as each communication system has unique hardware and software, life cycle support costs are high.

Proposed Approach. This report proposes an overall USCG architecture based on the Navy's Copernicus Architecture that is interoperable with US Navy systems present and future. Specifically, this architecture is based on the Copernicus' Communication Support System (CSS) architectural framework which provides a mechanism allowing for both change and growth in requirements and technology. This concept relies upon the separation of the existing and planned users from direct access and control of the set of radio frequency assets ("resources") available on each platform. It "inserts" a software/hardware "framework" between the users and the

communications systems and provides multi-link communications services to the composite collection of communication users.

A cornerstone of this concept is that the communication users are not aware of the media employed to transfer data to or from other users. The users are also not aware of data rate, coding mechanisms, link protocols, or timing relationships. The users regard the CSS as only providing the communications services which they specified in terms of distribution, security, quality, timeliness, and throughput.

Study Architectural Recommendation. This study proposes an Integrated Communications Architecture (ICA) and the goal Integrated Communications System (ICS) implementation of the architecture for the WHEC and WMEC class Coast Guard vessels. The goal system is based upon an open and scaleable communications design utilizing commercial-off-the-shelf (COTS) and Non-Development Item (NDI) technologies. The architecture meets current and near-term cutter requirements, and provides a platform for future growth with minimum cost, technical risks, and "down time". It permits modular system development, reconfiguration, incremental expansion, and encourages system definition and development using standards available in the public domain.

(1) Integrated Communications Architecture. The ICA framework protects the Coast Guard from utilizing NDI components that are obsolete at the time of production and operation. Open system architectures permit simplified integration of systems and components not native to the developed system. This benefit is realized in integration, but is even more evident during the product life cycle as system upgrades are made to accept new technologies or to replace outdated equipment. The use of open system standards in NDI can result in reduced development engineering and transition-to-production costs.

(2) Integrated Communications System. The ICS makes the total radio frequency (RF) capacity onboard a cutter available to ALL RF users. Allocation of the cutter's RF resources are allocated on a priority basis in accordance with an ICS Communications Plan (COMMPLAN). Priorities are determined by each vessel based on user type and message characteristics (perishability, addressees, data precedence, etc.). The ICS provides automated network monitoring and management and assists operators in the assignment and control of communication equipment. The ICS will resolve the issues of communications efficiency, RF channel scarcity, and the proneness aboard WMEC and WHEC to "lose" RF channels. It provides users with a communication service independent of their message processing functions. Users will not be concerned with the specifics of the communications path taken by their messages. Rather, they concentrate on their communications' destinations.

Study Implementation Recommendation. This study recommends a physical partitioning baseline which allocates physical communication system elements in a logical manner. The allocation baseline which follows is called the SATCOM System Architecture and is partitioned into six (6) individual physical groups:

(1) Antenna Group. The Antenna Group contains components which interface with the RF equipment and primarily includes the antenna, control assembly, bandpass amplifier-filter, and RF distribution assembly (e.g., cable assemblies, multicouplers, patch panels).

(2) Link Access/Radio Group. The Link Access Radio Group (LARG) establishes the RF data link and physical layers of the Open System Interconnect (OSI) standard architecture. It processes antenna input signals

and transduces emitted radio frequency (RF) energy media or radio frequency interference (RFI) to electrical data or linear electrical signals.

(3) Communications Service Group. The Communications Service Group (CSG) provides the networking protocols and interfaces communication system users to the radio equipment (LARG). CSG functions include: (a) communication with user systems (b) performance of "intelligent gateway" processing - RF media selection for user data (c) execution of media protocols - OSI subnet layer functions.

(4) System Control Group. The System Control Group (SCG) provides the system wide control mechanisms necessary to tailor communications operations to the specific platform environment. SCG functions include: (a) system initialization, (b) system configuration, (c) performance monitoring, (d) fault detection and recovery, (e) inter-platform control information exchange, and (f) data base control and maintenance.

(5) User Group. The User Group provides the gateway between the users and the communications networks. User Group functions include: (a) data compression, (b) message filtering, (c) duplicate search, (d) character conversion, (e) data formatting, and (f) Communications Security (COMSEC). In addition, the User Group provides the functions of message generation, format verification, editing, local message distribution, and hardcopy generation. The User Group is representative of all users except that it has specific functions associated with formatted communications.

(6) System Distribution Group. The System Distribution Group (SDG) provides distribution of baseband data and control among groups throughout the ICA architecture. SDG functions include: (a) inter-group communications connectivity - Link Access/Radio, Communications Service, System Controller, user, (b) inter-group control connectivity, and (c) inter-group security control.

TABLE OF CONTENTS

SECTION **PAGE**

TABLE OF CONTENTS

(continued)

SECTION **PAGE**

TABLE OF CONTENTS

(continued)

SECTION **PAGE**

LIST OF ILLUSTRATIONS

FIGURE **PAGE**

LIST OF ILLUSTRATIONS
(continued)

FIGURE **PAGE**

LIST OF TABLES

TABLE **PAGE**

1.0 Introduction

1.1 Purpose

This document presents the results of a communications system modernization study for the radio room of selected U.S. Coast Guard cutters. This study has been performed under contract GS-22F-0053B of the Department of Transportation, Volpe National Transportation Systems Center. It was initiated under delivery order number DTRS-57-94-F-00102, for the U.S. Coast Guard Research and Development Center.

1.2 Document overview

This document has four sections which are listed below.

- Section 1.0 is the introduction. It includes the purpose, this document overview, the technical approach, and the requirements analysis for this study.
- Section 2.0 provides a conceptual overview of a communications architecture which integrates existing communications system equipment with new communications technologies and new integrated communications system concepts. It includes a rationale for the selection of an overall system architecture, a description of the ICA concept, and a description of the goal system (the Cutter ICS).
- Section 3.0 provides detailed discussions and descriptions of the communications technologies identified for the ICA and specific details of the ICS.
- Section 4.0 allocates the equipment currently in the USCG inventory as well as equipment representative of the newer technologies that would be part of ICS to the segments of the ICA.

1.3 Analysis Approach

The analysis approach utilized for this study is illustrated in Figure 1.3-1. The first step was characterization of the WHEC and WMEC operational environment. Next, the study determined the mission and operational requirements based on that environment. The technical requirements were derived from the operational requirements. Finally, the communications technology was proposed.

The cutter's operational environment was determined under Task 2 of this delivery order contract. The conclusions were documented in the "Current Capabilities and Work Flow Analysis Report."

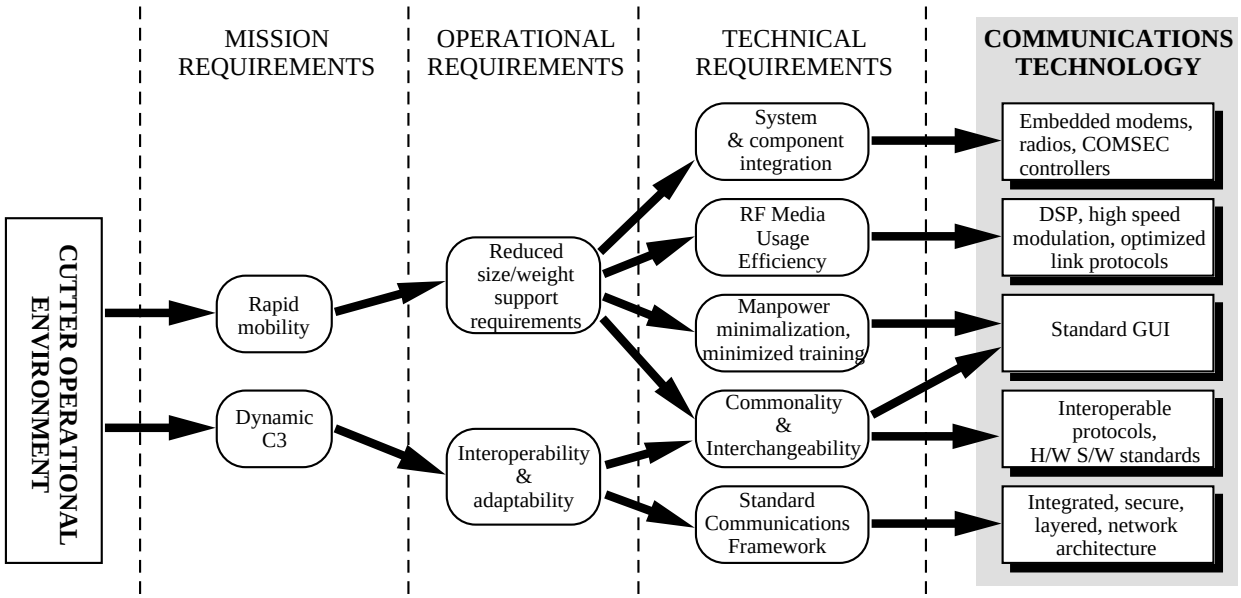


Figure 1.3-1 Study Analysis Approach

1.4 Technical Approach

Previous trade-off studies and analyses have focused on identifying and assessing requirements for functional modifications and additions to existing system components to support USCG operations. The focus of this task is to present options and recommendations to the USCG on how to improve USCG communications capabilities within a modular architectural framework that is independent of specific spectrum, radios, modems or processing equipment. Once this shipboard architecture is established, trade-off's concerning equipment types and transition mechanisms can be performed. This modular architecture will accommodate existing USCG HF and SATCOM systems as well as near-term upgrades and/or enhanced capabilities such as INMARSAT, Iridium, and NAVMACS Model II.

This approach is derived from comparable efforts to improve the US Navy's communications architecture. Because the existing systems were vertically integrated from user to antenna, implementation of a new radio had dramatic impact upon implementation of the data processing equipment connected to the radio. To provide the USCG a credible recommendation of how to improve USCG communications, or how to reduce or eliminate communications watchstander requirements, it is necessary to posture the communications system within an overall framework. In this manner the individual components can be analyzed in greater depth with an understanding of their individual place in the overall system.

In the past, USCG and Navy communication systems and networks have been developed and deployed by individual user communities to provide specific communications capability (i.e., communication of perishable tactical data, record traffic, navigation data, etc.). The result of this approach is a current communications architecture that is characterized by a large number of separate, non-interoperable, vertically organized communications systems. For example; the USCG accesses two US Navy communications “systems”: the Common User Digital Information Exchange Subsystem (CUDIXS)/NAVMACS network and the Officer in Tactical Command Information Exchange Subsystem (OTCIXS) network. The NAVMACS consists of specifically designed Navy equipment modified for use by the USCG. NAVMACS only operates on this specific equipment (processors, crypto's, modems, multiplexers, radios, antennas) and

only the specific ultra-high frequency (UHF) SATCOM 25 kHz channel allocated to the CUDIXS network. The network and equipment only process narrative record messages formatted in accordance with very strict standards. These messages can only be input via specific peripherals. A change in peripherals necessitates a change in the software controlling the network. A change in the network necessitates a change in the processing software and conceivably the interface to the peripherals. OTCIXS and NAVMACS are hosted on identical US Navy platforms. Wherever there is an OTCIXS, there is a NAVMACS. OTCIXS has its own set of equipment and another (different) specifically allocated 25 kHz SATCOM channel. If any of the equipment in the NAVMACS path to the CUDIXS fails, it is difficult, if not impossible, in most circumstances to use the OTCIXS network to exchange the same data. If the CUDIXS channel fails or the channel loading is excessive it is similarly impossible to use the OTCIXS network. The Navy and USCG experience have shown that there are significant limitations to this "stove pipe" approach (further discussed in Section 2.2). The most severe limitations include:

a. The communication system is "fragile" under conditions of stress. If a particular communication resource is lost, it is difficult to reconfigure other communications resources to compensate for this loss.

b. The communication systems are not interoperable. It is difficult to rapidly route data between the systems.

c. The architecture cannot respond to imbalances in the traffic load. One communications resource may be under-utilized while the capacity of another is being exceeded.

d. It is difficult to respond to the changing communication requirements of current users, or to the requirements of new users.

e. Since each communication system development is done as an independent program, total development costs are high.

f. Since each communication system has unique hardware and software, life cycle support costs are high.

g. The lack of an overall systems approach makes it impossible to perform system level diagnostics or to provide automated assistance to operational personnel.

The elimination of the "stovepipe" approach to communications is the target of the Navy's Copernicus Architecture. Within this architecture, Copernicus is comprised of four elements referred as "pillars": the Global Information Exchange System (GLOBIXS), the Commander in Chief (CINC) Command Complex (CCC), the Tactical Data Information Exchange System (TADIXS), and the Tactical Command Center (TCC). As a C^4I architecture, Copernicus is abstracted as an interactive framework that ties together the command and control process of the Navy tactical commander afloat, the Joint Task Force (JTF) commander, the numbered fleet commander and others with the CINCs ashore. The Copernicus design goals include:

a. Increase communication survivability via automated multimedia access by all users to all media, without sacrificing user throughput or communications efficiency.

b. Provide a means for incorporating new communications capabilities without requiring changes to the user equipment or operating procedures.

c. Maximize use of existing communications equipment.

d. Phased development efforts of planned programs to allow timely transition of Copernicus' CSS concepts.

This Modernization report focuses on providing an overall USCG architecture that is interoperable with the US Navy systems present and future and on ensuring that a mechanism exists for change and growth in requirements as well as technology. The features inherent in this approach are:

a. An "open" architecture that will allow "segments" of the architecture to be upgraded as new technology emerges, and will allow the architecture to be expanded to accommodate new users and radio equipment.

b. A locally interconnected system that will provide USCG users with multimedia access.

c. A distributed dynamic resource allocation capability that will provide load sharing across multiple media and survivability in cases of RFI, jamming, or equipment failure.

d. Reusable hardware and transportable software to provide lower development and life cycle costs.

e. Media specific link protocols to satisfy data exchange requirements over all media. The protocols employed will match the specific user requirements for data exchange, and the unique operating parameters of the particular radio frequency.

According to the Copernicus architecture, the CSS is part of the TADIXS pillar and includes all of the components of Navy communications. This boundary definition does not imply that all of the Navy's communications components will be redefined, redeveloped or replaced. The CSS concept provides a management protocol and procedural framework specifying techniques whereby most of these components need not change their operation at all. Within the CSS concept, communication users requiring communication services are external to the CSS. Equipment (existing and planned) which are used to implement the communication requirements of the user are within the CSS.

In order to achieve the goals described above within the cost constraints of the existing and planned systems, the CSS concept relies upon the separation of the existing and planned users from direct access and control of the set of resources available on each platform, and the insertion of “framework” software and hardware between the users and the communications systems which provides for the capability to provide communications services to the users. A cornerstone of the CSS concept is that the users are not aware of the media employed to transfer data to or from other users. The users are also not aware of data rate, coding mechanisms, link protocols, or timing relationships. The users regard the CSS as only providing the communications services which they specified in terms of distribution, security, quality, timeliness, and throughput.

The separation of users and communications functions within CSS is based upon two logical functional areas: communications resources and communications services. These are defined in CSS as follows:

a. **Resources** are the fixed collection of assets available to the user such as radios, modems, transmission media and the protocols available to the user to effect communications on these links. For descriptive purposes a resource is divided into two sections: the “link” section which consists of the RF equipment, security, and media components and the “protocol” section which controls the link. Within the CSS, communication systems are built to

incorporate the resources into a CSS-defined mechanism for performing an individual user communication service. CSS defined communication systems consisting of both hardware and software perform the protocols, interfacing and control functions for the communication needs of the user. In the existing non-CSS communications architecture, communication protocols are not differentiated from the user specific applications performed by User Systems. A single resource within CSS will consist of the media (channel, frequency, time slot, etc.), the communications equipment including radios, modems, encryption units and multiplexers employed to effect communications on that media, and the communications protocols which provide access, routing and control the exchange of information between each node operating on that resource. Examples of a resource in existing system terms are:

1. A single UHF channel operating a communications link protocol such as CUDIXS/NAVMACS and the Antenna, WSC-3, KG-36, ON-143(V)4, and communications protocol software operating within the AN/UYK-20 computers. The elements of CUDIXS/NAVMACS which perform record message processing, peripheral device control, operator interaction, and report generation are not associated with the resource.

2. If that same CUDIXS/NAVMACS application was operating on a single slot with Demand Assigned Multiple Access (DAMA) then the resource would be defined as above, except that the media portion of the resource would only consist of the slot and not the entire channel.

b. **Services** are the functions required of the communications systems by the user. For example; the Composite Warfare Commander (CWC) requires a service to connect all of his individual warfare commanders (AAW, ASUW etc.) in order to exchange data and voice in a near real time fashion. The service would specify the access time, delivery time, error control, priority, probability of intercept, accountability and security requirements. There is *significant differentiation* in the definition between the service required and the media employed to provide the service. In order to satisfactorily fulfill the requirements of users it is necessary to isolate the services required from the media and protocols which are used in today's communications environment to satisfy those requirements. In the example above, there is no specified path or data rate in the service parameter list.

The first phase of CSS as described herein will process two major types of information: VOICE and DATA. Processing of data includes the assignment of the data service to a resource or resources and the control of the exchange of the data via the resource. Voice processing will only include the assignment of a single voice service to a single resource. Voice information will not flow through the CSS Framework but around the framework and communications will be controlled directly by the voice terminal. All types of data will be handled by the CSS from teletypewriter (TTY) narrative to file and video information. For stream oriented data the subscriber interface may have to provide special processing in order to accommodate CSS protocols. The degree that CSS can process these data types in the manner required is directly proportional to the number and type of resources available at the instant the service is required.

The CSS concept does not provide new bandwidth via enhanced radios, modems or new satellites. The CSS concept only provides a new method of using the resources which are available. It consists of the following core segments:

a. The Subscriber Interface Controller (SIC) provides a common interface for all subscribers to the other CSS segments. The SIC permits the subscriber to define service requirements in a manner acceptable to the subscriber. The SIC

also determines which resource will be used for an individual packet of information. The SIC selects from the set of resources that have been assigned by the SSC. There is one SIC for each Subscriber at each CSS site.

b. The System Site Controller (SSC) provides the management functions associated with CSS including assigning and allocating services to the various resources.

c. The File Server Controller (FSC) provides for control and access of the on-line data base.

d. The Resource Access Controller (RAC) performs network and data link protocol functions which provide for network routing, site access, data exchange, and error detection and correction. There is one RAC for every Resource at each CSS site.

e. The Operator Interface Controller (OIC) permits the operator access to the CSS segments.

f. The Security Segment provides for COMSEC and the isolation of COMSEC information.

g. The RF Component is the antenna and media employed to effect communications. This includes conformance to the RF wave form associated with the use of the media with specific radio equipment.

h. A Link Access Controller (LAC) provides the interface to the antenna and may perform modem, coding, multiplexing, and radio functions. Many of these functions are currently distributed amongst various equipment. For example the TD-1271 has modem, coding and multiplexing functions. Mini DAMA provides all of those functions and the radio function. The USC-38 also provides all of those functions for MILSTAR access. The intent is not to define new requirements for new equipment but to characterize the existing equipment and to provide guidelines for new equipment that may be required for HF or UHF line of sight (LOS) or for future media purposes.

1.5 Background / Current Status

Navy efforts to evolve into the next generation communication system architecture under CSS have progressed significantly over the last two years. Functional requirements have been identified and investigated resulting in CSS Segment Specifications and Software Requirements Specifications (SRS) for CSS Framework elements. In recent months these identified requirements have been implemented into Naval Ocean System Center’s (NOSC) CSS Emulation Testbed to provide a high degree of confidence for many CSS concepts. In addition, NOSC's parallel CSS Simulation efforts have also provided a baseline tool to permit multi-site and multiple media simulation and analysis of CSS architectural alternatives. The combination of these activities and planned enhancements over the next year offer the capability to exhaustively research both single site and multi-site CSS networking issues.

To consider the accomplishments of the last two years, the diagram in Figure 1.5-1 identifies those areas of the SATCOM architecture that have been the focus of NOSC's CSS efforts. NOSC's engineering effort has been directed at functional definition and software development for Subscriber Interface Controller, Resource Access Controller, System/Site Controller, Operator Interface Controller, File Server Controller and the Inter-Process Control functions to tie together each of the other functions. These developments have been hosted in a multiple chassis, VME configuration with an interconnecting Local Area Network (LAN) and Sun scaleable processor architecture/desktop computer (SPARC/DTC-II) equivalent workstation

environment within the CSS Emulation Testbed. At this point, security provisions have been identified but not developed even in prototype form.

A supporting effort targeted at security was recently initiated with this same study team that will expediently evaluate implementation alternatives for the CSS Security Architecture and insertion of Naval Research Laboratory's (NRL) Modular Security Device (MSD) technology into NOSC's efforts over the next year. Efforts have also recently been initiated by NOSC to fully address the subscriber and user interface issues.

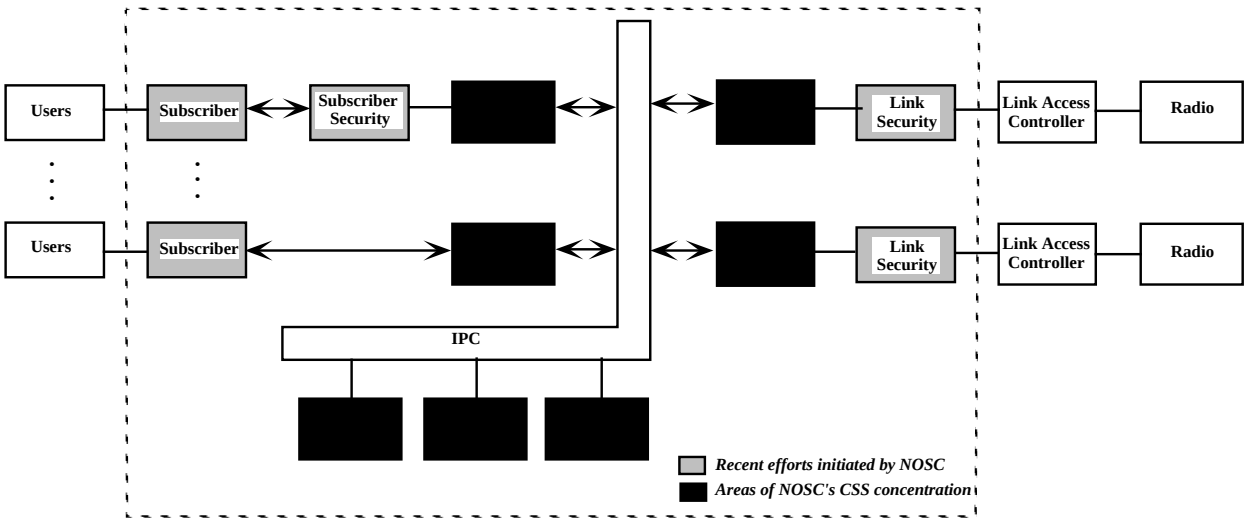


Figure 1.5-1 NOSC's Major CSS Focus

These major accomplishments have brought CSS one step closer to implementation and have now provided the confidence level necessary to broaden the focus to address other areas of the communication architecture such as User Functions, Subscriber Functions, Link Access Functions and the next generation Radio architecture.

A directed investigation of operational configurations and physical packaging implementations is also now in order. This investigation is necessary to move CSS from a demonstrated laboratory concept into a fielded system, procurable by currently planned programs. Issues such as installation, cabling modifications, physical connectivity to existing systems throughout transition and implementation on a wide variety of platforms (various ship classes, aircraft, submarines, shore stations and shelters) must be given immediate attention. This will help ensure procurement schedules for new and upgraded systems such as NAVMACS-II.

This is not to imply that operational configurations or physical packaging has not been considered throughout CSS efforts. In fact, the SPAWAR, NOSC and Support Contractor team that has evolved CSS have many years of experience in development, installation and support of Navy SATCOM systems. These important operational and physical implementation factors have been considered in each of their decisions along the way. It is no "coincidence" that current functional allocations will efficiently map to a physical implementation. What remains, however, is the task to further scrutinize these aspects of next generation SATCOM systems and formally document physical implementation approaches to serve as a baseline for revision or generation of system specifications.

1.6 Goals of Study

The primary objective of this effort is to initiate the transition from functional requirements to physical implementation. NOSC has already addressed implementation considerations for selected SATCOM areas that have been emphasized for near-term demonstration (e.g., NOSC's EHF/IXS demonstration proposal). The objective of this effort is to perform a more comprehensive review across multiple information exchange systems and corresponding component technology. To accomplish this objective, the following goals have been established:

a. Partition the end-to-end next generation communications architecture into manageable groups for implementation review and assessment.

b. Address issues not currently being emphasized by CSS.

   1. Link Access Control Processing
   2. Radio Architecture
   3. User functions (user functions that are the responsibility of communication systems)
   4. Unique user interfaces
   5. Antennas
   6. Operational Configurations and Physical Packaging (Ship/Shore and Aircraft/Submarine)
   7. Installation Issues

c. Provide physical implementation recommendations for next generation baseband systems and next generation SATCOM Radios (UHF concentration).

d. Recommend a specification tree for next generation SATCOM systems in the open system, standardized environment of CSS.

e. Recommend methods for the Coast Guard to produce system specifications for this new environment.

f. Recommend a set of specifications that would be required next generation UHF communication capabilities.

2.0 Top Level Architecture

This study proposes the ICA and the goal ICS implementation of the architecture for the WHEC and WMEC class Coast Guard vessels. The goal system is based upon an open and scaleable communications design utilizing COTS and Non-Development Item (NDI) technologies. The architecture meets current and near-term cutter requirements, and provides a platform for future growth with minimum cost and technical risks. It permits modular system development, reconfiguration, incremental expansion, and encourages system definition and development using standards available in the public domain.

2.1 Rationale

The ICA protects the Coast Guard from utilizing NDI components that are obsolete at the time of production and operation. This concern was considered up-front and can only be reliably addressed through a true open architecture. It is important to note that not all NDI solutions are open. The single key factor in open systems architecture is the definition, management, and communication of standards that specify interfaces, services and supporting formats for interoperability of software and hardware systems and the components of the systems. For example, older VAX architecture computers are NDI, but not open because they do not use open interfaces that allow for interoperability with non-VAX components. Likewise, the Navy's standard UYK computers (currently deployed aboard medium and high endurance cutters) are certainly NDI, but have very closed architectures.

The key benefit of employing an open system architecture is the simplified integration of systems and components not native to the developed system. This benefit is realized in integration, but is even more evident during the product life cycle as system upgrades are made to accept new technologies or to replace outdated equipment. The use of open system standards in NDI can result in reduced development engineering and transition-to-production costs.

Based on the selected architecture, the communications technologies shown in Figure 1.3-1 are appropriate to this approach. These technology topics listed below are discussed further in Section 3.0 of this report.

a. Embedded modems, radios, RF controllers, and COMSEC equipment

b. High speed modulation techniques

c. Optimized link protocols

d. Standard, consistent Graphical User Interface (GUI)

e. Standard interoperable communication protocols

f. Standard interoperable hardware and software standards

g. Integrated, secure, and layered communications network architecture

2.2 Integrated Communications System Concept

Today’s U.S. Coast Guard communications system for cutters deployed at sea is a collection of discrete special purpose networks (RF links). Each network has been developed and allocated for a specific communications capability for a specific community of users. Each network link is, in general, dedicated to the specific user community. Associated with these links are unique message formats and dedicated communications gear spanning the antenna hardware to standalone baseband equipment. The nature of these network links conforms to the traditional circuit switched approach. For example, General Service (GENSER) record message traffic

to/from high endurance cutters (WHEC) is transmitted and received via the Common User Digital Information Exchange Subsystem (CUDIXS)/Naval Modular Automated Communication Subsystem (NAVMACS) network. This network subsystem requires a dedicated satellite channel, baseband communications processor, operating procedures, and a shore-based network controller. No other type of traffic (voice or data) can be transmitted via this network or processed by the CUDIXS/NAVMACS subsystem. Loss of the satellite channel for any reason requires manual procedures to re-route the traffic. This is termed a "stove pipe" architecture.

Clearly, "stove pipe" architectures significantly limit the flexibility, survivability, and growth potential of their communications subsystems. A user whose RF access is denied, due to loss of channel or equipment failure, totally loses their communications capability. They are incapable of alternately routing their message traffic to other available networks.

Conceptually, the ICS proposed for the WMEC and WHEC provides a single, shared, composite communications resource. Sharing individual RF resources permits more efficient use of the relatively scarce communications assets onboard these vessels. Yet, transition considerations can overwhelm the implementation of new capabilities that do not inherently provide for a mechanism to transition. There will not be sufficient funding to supply all platforms simultaneously with a new architecture, nor will the interoperability issues with the US Navy suddenly go away. Thus, integrated shared communications resources are clearly the wave of the future and must be considered, yet the system architecture cannot ignore existing stove pipe systems. Though the existing equipment cannot handle the older architectures, the new equipment must operate in both worlds.

For the communication system user, this architecture provides a number of significant benefits. Backlogged users can share the idle capacity of other networks to help clear their traffic, thereby obtaining increased throughput from the communication system. The ICA based communications system provides a measure of survivability as traffic on failed links is alternately (and automatically) re-routed by the communication system. Flexibility is enhanced, as the system adapts to changes in traffic patterns and loading as the cutter's operational situation changes. Users of the ICA architecture access the communications system via a standard interface. No longer are specific discrete interfaces needed for every network, but rather all transmit and receive traffic over a single common interface. Finally, the ICA provides for scaleable growth. A new community of users (e.g., exchangers of video images) is integrated into the communications architecture without the need for additional dedicated network assets. New RF communications capabilities, once introduced into the communication system, are provided to ALL users via the ICA defined common interface.

2.2.1 Scaleability

The ICS is based on open and layered principals. The architecture is designed for growth, NDI integration, ease of maintenance, extendibility, and hardware independence. It is a scaleable system that can be adapted to changes and the evolution of WHEC/WMEC mission requirements.

Growth and flexibility directly relate to cost. It is beyond the scope of this document to discuss actual costs. However, there are two cost approaches to providing growth capability. One approach provides a low cost initial system outlay, though changes of any nature tend to incur substantial costs. A second approach is to pay a premium for the initial system. Changes can then be provided at a minimal cost.

PC based systems are an achievable goal for the cutter radio room. The PC system might provide a lower cost for the initial system, but the PC is inherently limited to single processor

technology. Adding I/O load or processing functions means that an additional processor is needed, which equates to a substantial cost.

A superior technical approach envisions a system that will permit independent changes at a minimal cost which provides a scaleable multiple processor bus system (e.g. VME) that provides for growth in the following ways:

a. Basic System Sizing: The basic system recommended in this report exceeds current and near-term cutter requirements. Therefore, near-term growth is achieved by the initial system.

b. Scaleable Hardware Component Architecture: Features such as memory size, processing power, I/O control, and radio control are onboard items that can be field upgradeable.

c. Scaleable Hardware Interconnectivity: The use of the VMEbus and the availability of additional board slots means that new capabilities not even envisioned can be added to the system without major system upgrades.

d. Scaleable Software Features: The ability to add the hardware is important, but if changes require substantial software rework, then any savings could be lost. Scaleable hardware requires scaleable software. Software designed and coded based on standard interfaces (UNIX) accommodates hardware change. Further, software can be designed such that the structure is organized to isolate areas of probable hardware incompatibility. Thus, new hardware can be incorporated with minimal software changes.

The approach recommended in this report is to provide a scaleable framework within which both scaleable and non-scaleable components may be utilized. For example, a VMEbus system consisting of multiple processors is a scaleable architecture that has proven itself in naval communications applications. But, procurement mechanisms may inhibit the use of a fully scaleable VME system for the USCG communications needs. Thus, the need will exist for the ICA to accommodate scaleable technologies such as VME but also accommodate low cost processor environments such as those represented by the lowly PC and the new desktop TAC-4 RISC processor environment.

2.2.2 Multiple Layers

The capability to provide growth or flexibility is not achieved by simply stating that interface standards will be used. There needs to be a conceptual plan for achieving growth and a plan for adapting to new requirements. Without this concept, the software may require significant change and the hardware may require expensive retrofit or modification. This report proposes multiple layers of growth based on the following scenario:

a. An increase in the data rate of the communication channels. The current cutters deal with very low data rates. However, this study shows that T1 (1.544 Mbps) rates are already employed on U.S. Navy shipboard platforms today. Current UHF SATCOM Demand Assigned Multiple Access (DAMA) burst rates are at 32 kbps.

b. An upgrade to the communication protocols. The current protocols used for the RF interfaces are very simple. Future growth in this direction would require the use of more sophisticated protocols such as X.25, or HDLC, ADCCP, etc. These bit-oriented protocols are accommodated by most commercial VMEbus boards without additional hardware. By using the onboard processing and memory of the VMEbus boards, this architecture

isolates the *data link level* impacts associated with growth in the target vessels' communication requirements. Changes in the communication processing capability do not impact the applications processing (system control, message processing, etc.).

c. An upgrade in the Cryptographic Subsystem. Within the next decade, there will be embedded encryption schemes. Such cards are already being developed for satellite surveillance systems. These embedded cryptos will reside on VME based boards. Although use of such a device would necessitate use of a chassis with red/black isolation, existing VMEbus cards would not need upgrading.

d. Increase in requirements for data presentation. The use of embedded interactive training using audio, graphics, and video is becoming a standard mechanism for reducing the costs associated with training computer system operators and maintainers. There are several COTS training development packages currently available for UNIX systems. These packages dramatically reduce the time and cost for providing embedded computer based training (CBT). CBT provides on-line tutorials, help and maintenance information to system users.

e. Increase in secure operating system requirements. Future data handling requirements may require higher COMPUSEC levels such as B1/B2. These operating systems require faster and more powerful processors, such as those used in today's RISC computers. Current PC technology will not perform the processing in a timely manner for an event driven real time system associated with the "labeling" requirements of B2. There are no PC based operating systems (O/S) that satisfy the security requirements envisioned by this study. To achieve the security goal, UNIX and RISC-level processors are needed.

f. Increase in platform connectivity. Laptop computers may be desired in the future cutters as part of the communication architecture. Using the proposed open system approach and inexpensive COTS software, laptops could be added in a manner which requires no expenses other than the cost of the laptop and its associated native operating software.

2.2.3 Flexibility

Flexibility is achieved in the proposed system by its inherent adaptability to the changing world. Flexibility is different from growth in that the changes may not be growth in capability but simply technological. Several examples of this type of change and the inherent flexibility gained from employing open system techniques are:

a. Vendors of NDI price their products in accordance with market volume demand. Therefore, if large volumes of a given item are purchased, the item generally costs less to produce. By purchasing in the commercial arena the Coast Guard procures within an already competitive atmosphere.

b. In the open system architecture, application software is based on UNIX, which isolates it from the hardware. Further, UNIX software is often designed so that it is layered over a standard interface to "hide" the hardware from application functions. This allows different, but compatible, hardware vendors to be substituted, without incurring extensive software redesign and rehost costs.

c. Eventually, the vendors stop production of a particular board and introduce a replacement that uses newer technology. In these cases, the Coast Guard

solution has been to buy out the production line. This often leads to even greater problems down the road because maintenance of older technology means maintenance of the test equipment and test tools, further spares become costly, or worse, unavailable. The open system architecture proposed in this study, base on the VMEbus and UNIX environment, provides a viable alternative. These recognized standards are adhered to by the new technology since so many customers have vested interests in maintaining them. Thus, it becomes cost effective to employ the new technology since most of the current software and interfaces remain unchanged.

2.3 Integrated Communications Architecture Concept

This section describes system partitioning which is oriented such that programmatic considerations such as annual funding line limitations and use of existing components is maximized. With this partitioning, the trade-offs concerning types of radios, processors and interconnection technologies can be addressed. The ICS concepts discussed above which require new equipment as well as existing USCG equipment can be overlaid on top of this physical architecture.

The end-to-end next generation USCG system architecture is partitioned into six (6) separate physical groups as discussed in the immediately following subsections. This architectural abstraction is based on the next generation communications system architecture. Shown within each group are the allocated physical components. It is important to note that groups shown do not necessarily indicate separate boxes. The components within each group are physical entities. In some applications (e.g., aircraft deployment) components may be integrated into one or two chassis. Each of these components could be an existing USCG component or a new component. For example; an existing NAVMACS system consists of user interface devices such as keyboard, displays and printers, UYK-44 processors, mass storage devices, encryption equipment, a DAMA multiplexer/modem, a WSC-3 radio, and an UHF SATCOM antenna. In the case of NAVMACS many of the communications functions are highly coupled and not well isolated from the perspective of the casual investigator. For example, using the model shown in Figure 2.3.1-1, the UYK-44 performs the functions associated with the User Group, the System Distribution Group, the Communications Services Group and the System Controller Group. The software in the UYK-44 performs user interfacing to displays, keyboards, and printers. It also provides message generation and processing functionality, and controls access to the communications link (operates within the CUDIXS link protocol). The AN/WSC-3 performs the Link Access/Radio Group functions in a single integrated package on a per channel basis.

But, that is the existing physical implementation today. The ICA also facilitates different implementations. For example, a new VME-based radio could provide multiple channels of UHF communications access within a single integrated chassis and include other functions such as the existing DAMA functionality within a single VME card. In addition, the implementation used for the Link Access/Radio Group need not be the same implementation used for the User Group or any other group. Trade-offs can be made which consider the schedule for replacing existing equipment and the fact that new technologies will be available in several years that are not even considered at this time. This architecture attempts to be technology independent.

The following subsections describe system partitioning. In addition, the partitioning is evaluated in terms of programmatic considerations.

2.3.1 Physical Architecture Groups

The end-to-end next generation Coast Guard communication system architecture is partitioned into the six (6) separate physical groups shown in Figure 2.3.1-1. Shown within each group are

the allocated physical components. It is important to note that groups shown do not necessarily indicate separate boxes. The components (shown in white) within each group are physical entities. In some applications (e.g., aircraft or submarine deployment) components may be integrated into one or two chassis.

A summary of the contents of each physical architecture group is provided below with a more in-depth discussion of each group in Section 3.0.

a. The Antenna Group includes all antennas, couplers, servo and control mechanisms and the RF Distribution between antennas and the Link Access/Radio Group.

b. The Link Access/Radio Group includes an interface to the Antenna Group and interfaces to the Communications Service and System Controller Groups via the System Distribution Group. A link processor is incorporated to perform link access control functions and link security is provided by either external and/or embedded COMSEC devices. Radios are also included in the group consisting of a modem/mux and a transceiver consisting of a receiver/exciter and power amplifier. The control processor provides automated control by the System Controller Group and/or Communication Service Group or semi-automated control can be provided through the front panel (display, keypad, switches, etc.). BIT functions and diagnostic capability is also provided by the control processor/front panel. Distribution for the Link Access/Radio Group consists of a variety of items. It includes backplane distribution of baseband and control/bit/status information, IF distribution between modem/mux and transceivers and RF distribution between receiver/exciter and power amplifier elements of the transceiver. This distribution also includes required point-to-point and patch panel connectivity for interconnecting with existing equipment contained within the group.

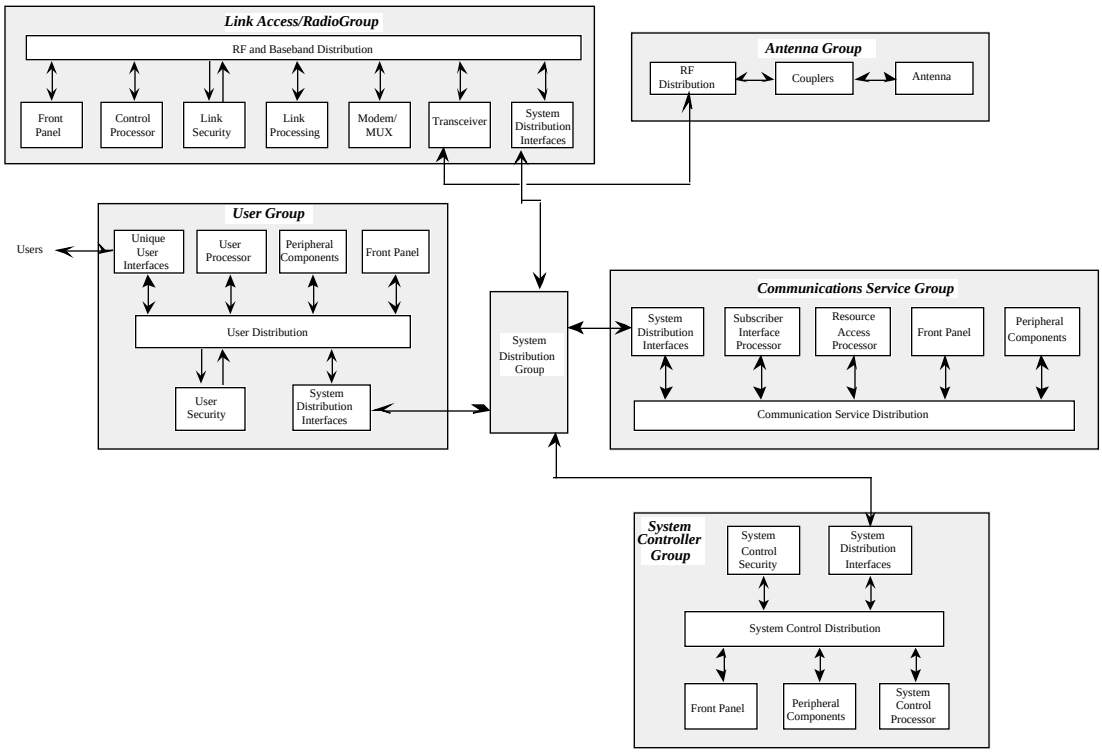


Figure 2.3.1-1 Communication Physical Architecture Groups

c. The Communications Service Group physically implements the Subscriber Interface Controller (SIC)user and Resource Access Control (RAC) functions of CSS using processors and software based upon developments by NOSC. It also contains a standard system distribution interface that is envisioned to be a LAN interface for shipboard applications. For aircraft or submarine applications where multiple groups may be implemented within one or two chassis, this interface may reduce down to a backplane. The front panel consists of displays, keypads, indicators, switches, etc. to permit manual local control of the group and facilitate local diagnostic capability for maintenance purposes. Peripheral components include hard disks, tape drives, etc., that are used for control, databases or archival storage. In many cases peripheral components in the System Controller Group can also be used by this group if security permits. The communications service distribution includes backplanes/bus and external interconnects. LAN or point-to-point serial interfaces may be required for those applications where the capacity within the Communications Service Group dictates the use of two or more chassis. A logical packaging concept for this situation might be to partition user processors and resource access processors into separate chassis with a LAN interconnect.

d. The System Controller Group physically implements the System/Site Controller (SSC), File Server Controller (FSC) and Operator Interface Controller (OIC) functions of CSS. This group also includes a standard system distribution interface anticipated to be a LAN interface in most applications. Two possible implementations have been evaluated for this group. The baseline is a workstation approach (e.g., DTC-II) to implement the system

control processor, display, system control distribution and provide peripheral components. However, in applications with limited physical space, the system control processor can be implemented by an embedded processor module. The operator or maintenance interface could be a front panel display and keypad on a chassis that includes not only the System Controller Group, but also physical elements from other groups. System control security includes the elements necessary to protect system control information in a multi-level security environment and at some point in the future provide automated key distribution to the communication system. System control security is implemented with a combination of COMSEC and COMPUSEC technology.

e. The User Group provides the interface between users (existing and new) and the Communications Service Group via the System Distribution Group. It also provides a physical architectural layer that facilitates security issues to be partitioned on a user basis (e.g., SI User, GENSER Secret User, Unclassified User, etc.). This group also includes a system distribution interface for system connectivity. It has a user processor that handles user-to-user message transfers and provides user level message flow control. It includes all the unique interfaces to accommodate connectivity of users into the system. For certain applications the User Group will contain peripheral components that are workstation based to provide operator interfaces and user level traffic analysis capability similar to that available in present day IXS. For security purposes, sensitive intelligence users require this stand-alone capability. The User Group also includes a user security subgroup. The two most viable security architecture alternatives for CSS both require a COMSEC device to be provided at the SI users interface and the current security baseline requires a COMSEC device at each user interface. The majority of user equipment are procured by other organizations and the only concern is to provide reliable communication service to these users. However, there are exceptions (e.g., sensitive intelligence) that represent user functions that remain the responsibility of an external agency (e.g., Drug Enforcement Agency). For this reason, further investigation is warranted into these Communication User Group implementations. The majority of these applications will be satisfied with a workstation approach to provide operator interface. This group also includes a system distribution interface subgroup that provides connectivity to the User Group through the System Distribution Group. For the most part this subgroup consists of a point-to-point serial interface.

f. The System Distribution Group. This physical group has been allocated to address connectivity between each of the other groups. It also, along with the system distribution interfaces within the other groups, performs the Inter-Process Control function of CSS. The long-term goal is to provide this connectivity between groups through fiber optic LANs to the maximum extent possible. The key to a near-term successful implementation of next generation communication architecture is an effective transition architecture for interconnectivity between new and existing equipment. During the transition period, the System Distribution Group will contain multiple variations of LANs, point-to-point cabling, multiplexers, patch panels, etc. This group will also vary greatly from one platform type to another. The importance of these issues dictated their allocation to a major group for consideration.

2.3.2 Assessment of Physical Partitioning

The physical partitioning baseline that has been selected appears to allocate physical elements in a logical manner. To ensure that this baseline can incorporate CSS accomplishments and provide

the necessary flexibility and robustness for effective implementation and deployment, several considerations must first be examined. Listed below are the areas examined to evaluate the baseline. The following subsections address each of these considerations.

a. Existing equipment/subsystems must map into physical architecture groups.

b. CSS functional allocations (i.e., SIC, RAC, SSC, OIC, etc.) must cleanly map into physical architecture groups.

c. Security architecture restrictions must be accommodated.

d. Major programs (e.g., the Navy's next generation UHF SATCOM Radio) must map into physical architecture groups.

2.3.2.1 Mapping of Existing Equipment/Subsystems into Physical Groups

One of the first considerations examined was the mapping of existing communication equipment into baseline physical architecture groups. A primary concern in implementing the next generation communication systems is the transition period where a combination of existing and new equipment is to be accommodated. Therefore, it becomes extremely critical to examine how existing equipment and subsystems map into the physical group partitioning. If interfaces are to be defined around the defined groups and subgroups, then the impact on interconnectivity to existing equipment and subsystems becomes obvious. To examine this consideration a generic, end-to-end, present day communication architecture was mapped into baseline physical groups. This mapping can be reviewed in Figure 2.3.2.1-1. As can be seen, there is a clean one-to-one mapping with the exception of current communication processing provided by the AN/UYK series of processors.

In current systems these processors perform user and network functions. In the CSS concept, the network functions will be integral to the Communications Service Group and shared by multiple users. For current IXS to interface and gain the multiple media resource sharing advantages offered by CSS, either software modifications will be required to current systems to remove or bypass network functions and interface user functions direct to the Communication Service Group or IXS need to be upgraded to the new architectural approach. It is anticipated that existing IXS will continue to be provided fixed access to communication links during transition. As each IXS is upgraded within the CSS architectural concept, it is recommended that current processing structures be partitioned into User and Communications Service Groups. In this transition approach, the fact that the current IXS processors are spread across several of the physical architecture groups becomes insignificant. As IXS upgrades take place, their current network functions will be moved to the Communications Services Group and the remaining functions will reside primarily in the User Group. A minimal amount of functionality will be moved to the User Group in some applications (e.g. sensitive intelligence operator message generation).

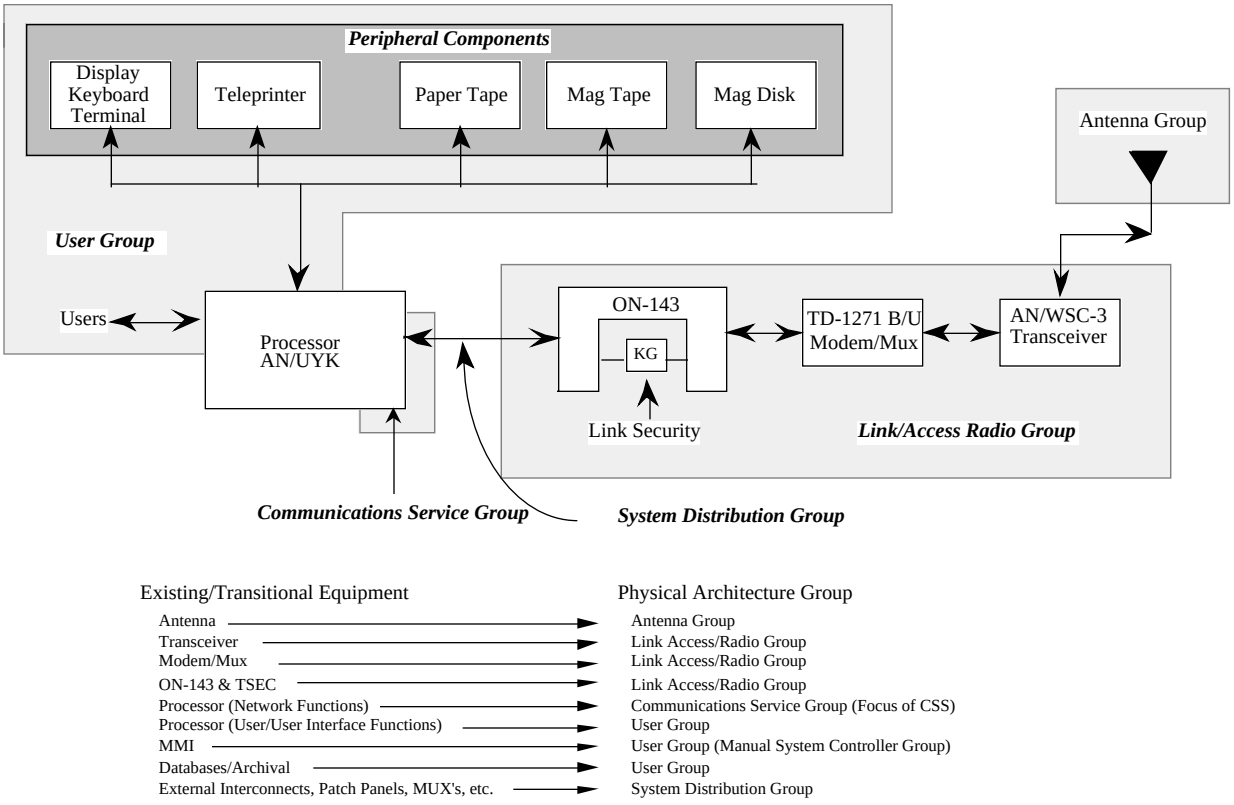


Figure 2.3.2.1-1 Mapping of Existing Equipment/Subsystems into Physical Architecture Groups

2.3.2.2 Mapping of CSS onto Physical Architecture Groups

The Standard Operating Environment (SOE) for CSS has been the result of many man-years of effort by the Navy to define and analyze the optimum functional layered architecture. To ensure benefits of CSS are realized in implementation of the next generation SATCOM system architecture we must examine the mapping between CSS functional Segment Specifications and the recommended physical architecture groups. Figure 2.3.2.2-1 contains a diagram of this mapping. As can be seen, CSS Segment Specifications (SIC, RAC, S/SC, etc.) map direct to given physical groups and the Inter-Process Control (IPC) function ties together each of these groups. This direct mapping is an ideal situation. A concentrated effort is being directed throughout this review to make recommendations that maintain this layered separation.

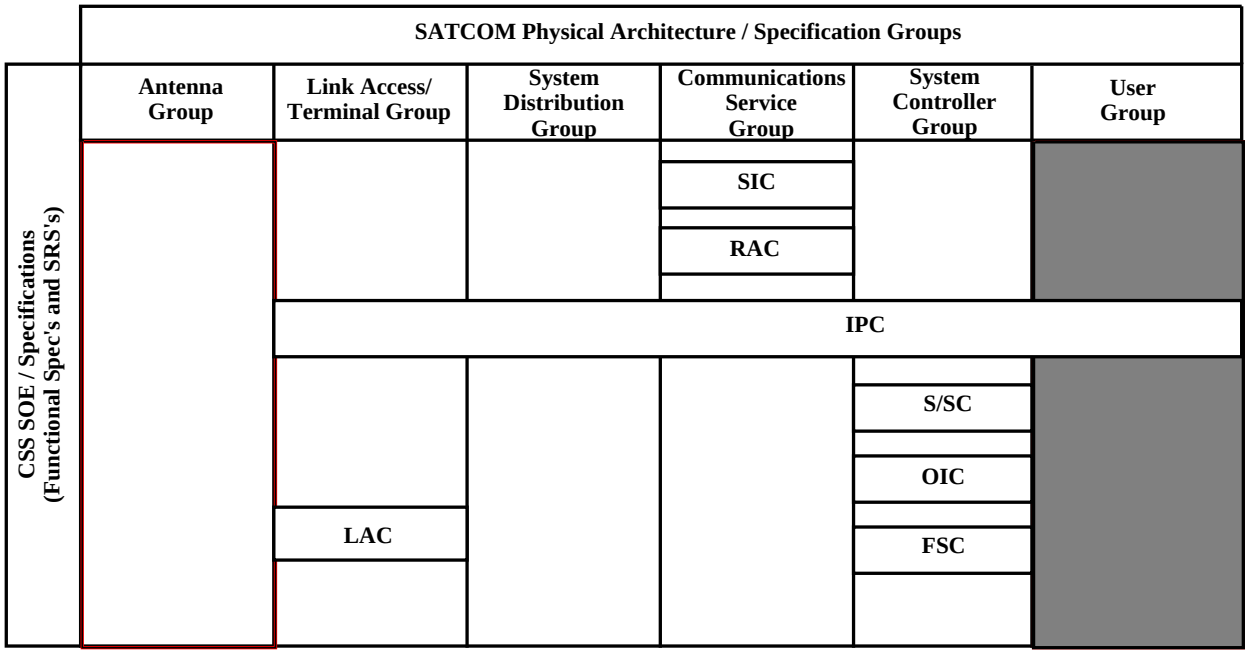


Figure 2.3.2.2-1 Mapping of CSS SOE/Specifications to SATCOM Physical Architecture/Specification Groups

2.3.2.3 Security Architecture Constraints on Physical Partitioning

Several CSS Security Architectures have been considered and two viable alternatives continually emerge.

a. User-level COMSEC for all users (this is the current NRL baseline).

b. User-level COMSEC for SI users only, with COMPUSEC (at the *Orange Book's* B2 or B3 level) for the Communications Service Group and System Controller Group.

SPAWAR, NOSC and NRL continue to explore the relative merits and risks for each of these approaches and have recently increased their efforts directed at this critical implementation consideration. This subsection addresses whether both of these approaches can be accommodated by the baseline physical partitioning. Both alternatives are addressed in terms of physical packaging and operational configurations within the applicable group discussions in Section 3.0. NOSC has contracted a study team to perform an in-depth implementation assessment for the CSS Security Architecture. The results of that effort that address physical sizing, performance, cost and risk will not be available to support this effort. Therefore, only physical implementations for each alternative will be presented in this report.

Figure 2.3.2.3-1 is a top level diagram showing security architecture alternatives. Both architectures require link encryption/decryption of signals transferred over the selected communications link/media, and both require encryption/decryption of compartmented SI user data for transfer within the system. Each architecture also requires distributed, trusted computing for distribution of COMMPLAN and planning/support control data from the System Controller Group to other groups to effect the communications service. For COMSEC-intense alternatives (architecture 1) this function includes full system key management for selection and distribution of crypto-keys. In a simpler alternative (architecture 2), key management will still be required, but can be implemented on a lesser scale for SI COMSEC and link COMSEC. Considerations for

trade-offs include application (shore, air, sea platforms), development schedule risks, cost of implementation, and transition to future embodiments.

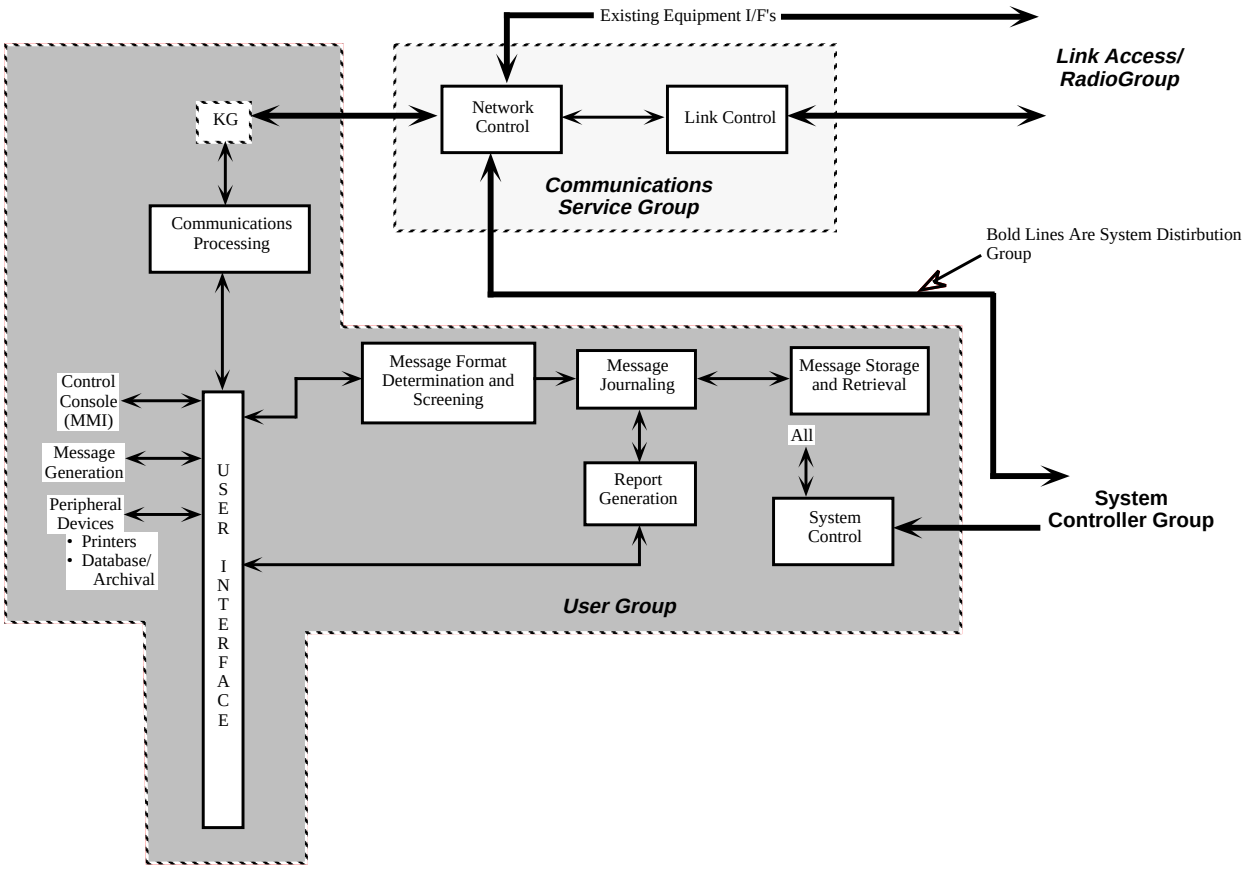


Figure 2.3.2.3-1 Security Architecture Considerations

In both security architectures there is a need for some degree of COMSEC separation for SI users and for link level COMSEC. There is also a desire by some users to incorporate user level security for further compartmentation. These alternatives are supportive of the separate user, User and Link Access/Radio Physical Groups selected for the baseline physical architecture. Similarly, either architectural alternative will require COMSEC or COMPUSEC for protection of unique System Controller Group functions. This supports a separate System Controller Group. Although the two architectures described in this section or other candidate architectures are the subject of in-depth analysis, the following security drivers will always hold true.

a. Security separation of some form must be provided for the user level

b. Link level security will always be required

c. Users in the future may require or desire a user level compartmentation

d. System control functions will always require special security consideration

In summary, the defined baseline physical partitioning into groups is highly supportive of this security environment.

2.3.2.4 Mapping of Program Requirements into Physical Groups

Another consideration in evaluating the physical partitioning for the Coast Guard is to assess how well planned functional and physical requirements for next generation Navy programs such as TACINTEL II, NECC and the next generation SATCOM Radio map to baseline groups. These planned program requirements provide an excellent evaluation tool to test the reasonableness of the baseline.

a. TACINTEL II is a good example of an upgrade to an existing Navy IXS to provide enhanced performance and message delivery reliability under CSS. To consider TACINTEL II, the functional requirements were extracted from the current TACINTEL II Draft System Specification. Although the terminology and architectural approaches are pre-CSS the functional and operational requirements remain unchanged. Figure 2.3.2.4-1 contains a mapping of TACINTEL II functional requirements into recommended physical architecture groups. Provided in Table 2.3.2.4-1 are brief definitions of each TACINTEL II function to assist the reader in evaluating the mapping. The mapping of functions into the recommended physical groups in this manner is somewhat crude, but does indicate a general compatibility of mapping existing and planned upgrade IXS functions into the recommended architecture. It also indicates that TACINTEL II has a substantial User Group function and that some user functions are currently embedded in IXS such as TACINTEL. Both of these areas are outside the mainstream CSS efforts and dictate increased attention.

b. NECC**.** Figure 2.3.2.4-2 provides a similar map of NECC functions from the February 1990 Draft Specification into physical architecture groups. It is anticipated that this functional diagram will continue to evolve, but is a good snap-shot for comparison against the recommended partitioning. As can be seen the functional diagram easily maps to our physical architecture groups. It is important to note that NECC is a good example of a new generation of IXS under CSS where the majority of functions will be implemented by the Communications Service Group.

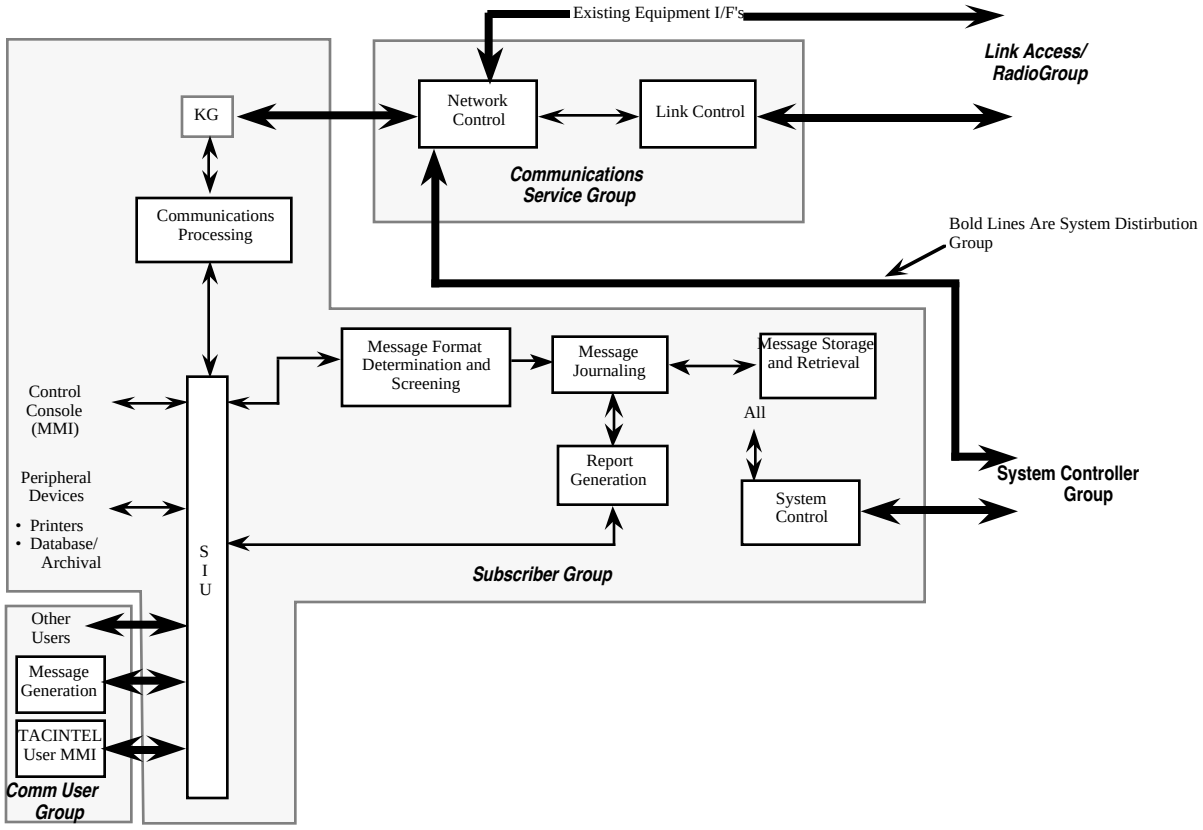


Figure 2.3.2.4-1 Mapping of TACINTEL II Functional Block Diagram into Recommended Physical Architecture Groups

c. Next Generation SATCOM Radio**.** There is an inherent direct mapping of the next generation SATCOM Radio to the Link Access/Radio Group. Interest in this area is consequently at the component level. Figure 2.3.2.4-3 contains the Link Access/Radio Group diagram annotated with numbers and a corresponding top-level block diagram for the next generation SATCOM Radio. Each block in the diagram has been assigned a number to indicate which component the block maps into in the Link Access/Radio Group. As can be seen, there are sufficient component-level categories to handle each of the required physical elements.

Table 2.3.2.4-1 TACINTEL II Functional Requirements Definition

TACINTEL II Functions	Description	User Group	Comm Service Group
Message Generation	• Message Composition and Edit • Message Formatting assistance • Message Analysis and Validation	X	
Message Journaling	• Message and Control Long and Short- Term Storage • File Management • File System Operator Control	X	
Message Storage and Retrieval	• Short and Long-Term Storage • System Parameter and Statistics Storage	X	
Message Format Determination and Screening	• Determine Format of each message • Screen Message for Proper Address	X	
Report Generation	• System Analysis Function • Automatically or Manually Generate Reports on Message Activity, System Status, etc.	X	
Interface Unit	• Peripheral and User Interfaces • Delimiting • Security Checking • User Routing	X	
Network Control	• Network Selection • Routing and Relaying • Map Global Addresses to Network Addresses • Maintenance of Network Connectivity Tables • Link Status Monitoring • Flow Control • Precedence Control		X
Link Control	• Link Protocol for each Media • Link Quality Monitor • Crypto Interfaces		X
System Control	• Initialization and Control • BIT/BITE • Error Detection and Recovery • System Status	X	
Human-Machine Interface	• TACINTEL Operator Interface	X	
Comm Processing	• Map message address to global address • Segment data for efficient transmission • Reassemble received data • Format data for delivery to network control	X	

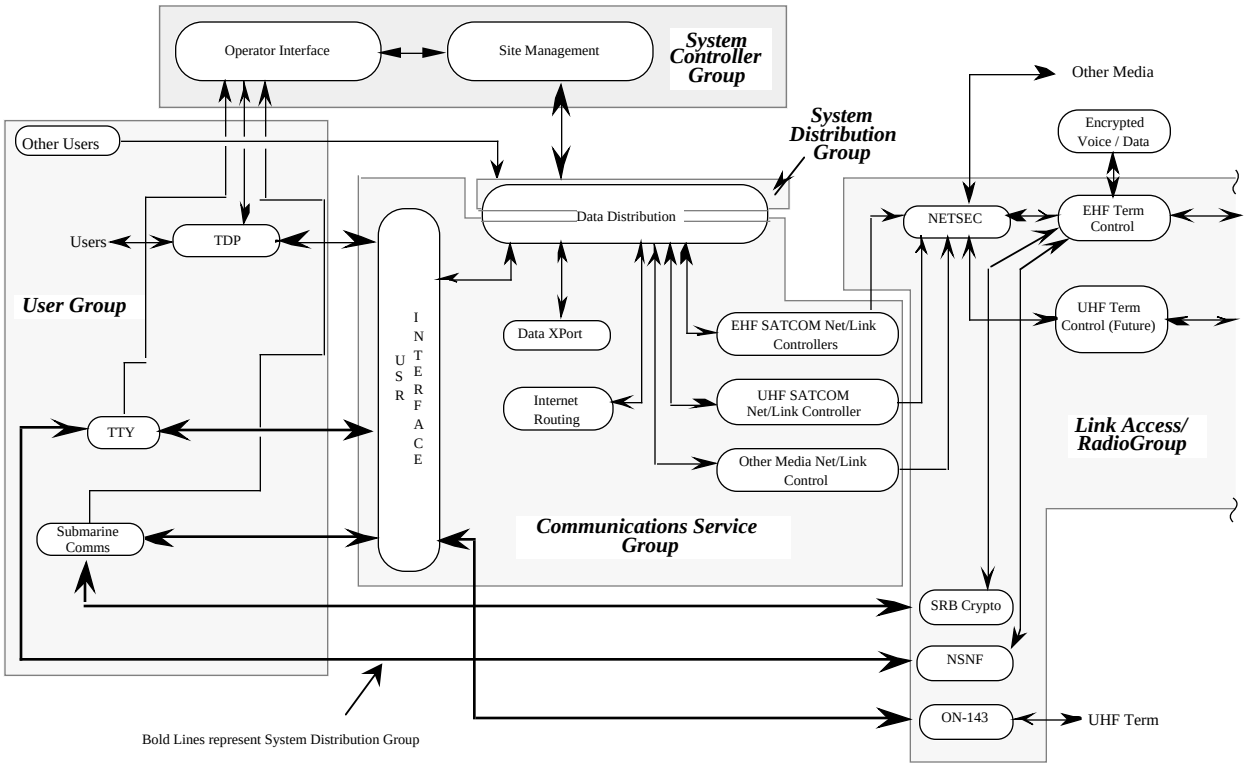


Figure 2.3.2.4-2 Mapping of NECC Functional Block Diagram into Recommended Physical Architecture Groups

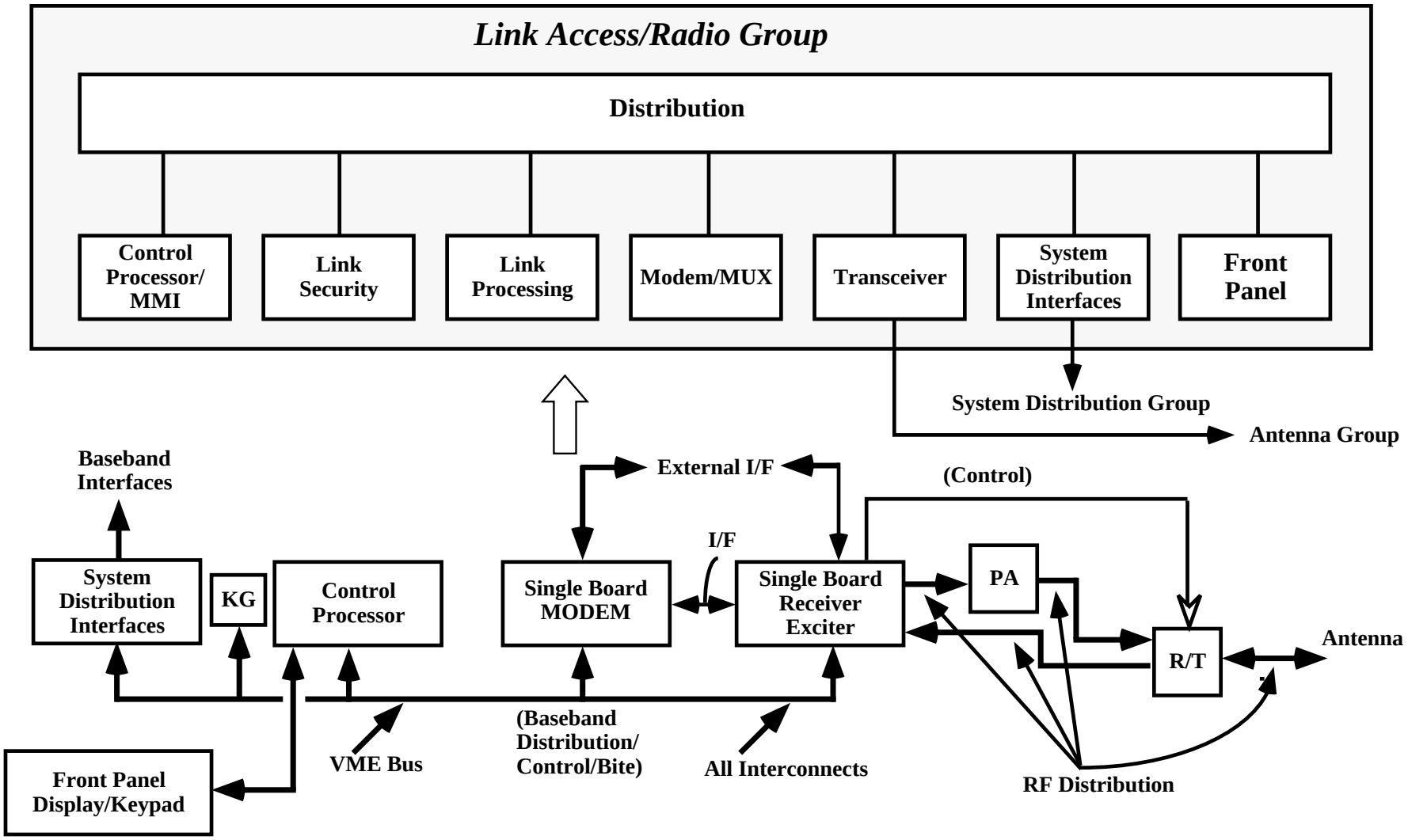


Figure 2.3.2.4-3 Mapping of Next Generation SATCOM Radio into Physical Architecture Groups

2.3.3 Implementation Methodology

The system development/implementation methodology for the ICS needs to fit isomorphically with the ICS abstraction. The generation of system and subsystem specifications within the open architecture and standardized environment defined by the ICS require careful consideration. The concept of a "specification tree" is recommended for developing specifications for the communication elements of the ICS. This section recommends a top-level specification tree and addresses how Coast Guard engineers and Program Managers might approach specification generation in this new environment. Recommended detailed levels of the specification tree for each group are presented in Section 3.0.

2.3.3.1 Top-Level Specification Tree

Figure 2.3.3.1-1 contains a diagram of the Top-Level next generation SATCOM specification tree. The top of the tree is a SATCOM Requirements Specification. This specification serves as the Program Manager's guideline for configuring system requirements and generating specifications. It details how to step through each of the SATCOM groups and select equipment from entire groups, subgroups, or elements within subgroups for inclusion in system/subsystem specifications. Also provided is guidance and requirements on how to incorporate CSS requirements and common standardized hardware and/or software for use across multiple programs. Below is a description of the intended contents for each specification level.

a. System/Subsystem Specifications. These are the specifications by which the Coast Guard would procure systems and subsystems. They combine operational and performance requirements with tailoring of referenced group, subgroup and element requirements specifications. CSS requirements are incorporated by reference in group-level specifications.

b. SATCOM Group Requirements and Interface Specification. These specifications define the partitioning of end-to-end SATCOM requirements into groups and defines interface requirements between these groups. It provides a defined division of requirements so that each group can be managed by the organization that is best suited to address technical issues associated with a particular group.

c. Group-Level Specifications. Each group specification defines the interfaces between components and the functional requirements allocated to each component. It also defines requirements for use of CSS common hardware and software by referencing CSS specifications. A group specification also maintains a table of all component equipment that is available for use.

d. Component and Element Specifications. These levels are not shown in Figure 2.3.1-1, but require a description for completeness. Component specifications reside under group specifications and define the interfaces between elements in the component. They also provide a listing of acceptable elements for use and the constraints for development of new elements. Standard CSS hardware elements or software that is recommended for use are listed component specifications. Element specifications reside under component specifications and define physical hardware elements such as a processor. In many cases element specifications may be pulled directly from standard CSS hardware element specifications that are incorporated by reference in the subgroup specification.

e. CSS Requirements Specification. This specification defines the CSS Standard Operating Environment (SOE) and the requirements for CSS software segment requirements and common CSS hardware.

f. CSS Software Segment Specifications. Provides allocation of CSS SOE into functional segments (e.g., SIC, RAC, S/SC, etc.) for software development.

g. Common Software Specifications. Software Requirements Specifications, Interface Requirements Specifications, etc. for segments per DoD-STD-2167B.

h. Common Hardware Specification. Provides requirements and guidelines for hardware elements (e.g., processors, standard interfaces, etc.) that are common across multiple groups and programs. Common hardware element specifications reside under this specification.

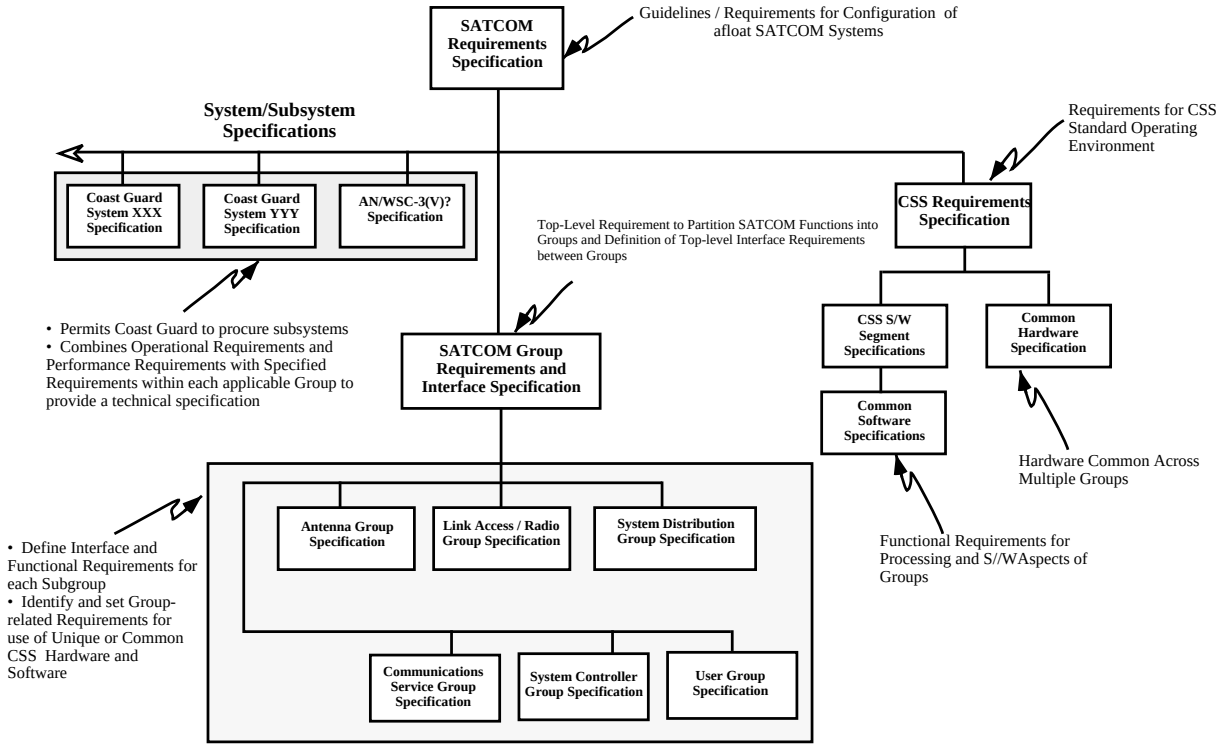


Figure 2.3.3.1-1 Next Generation SATCOM Specification Tree (Top Level

2.3.3.2 How to Apply the Specification Tree

The basic specification tree approach is shown in Figure 2.3.3.2-1. The Program Manager uses the SATCOM Requirements Specification as the guidelines and requirements for configuring systems and generating specifications. System/Subsystem group-level requirements are obtained by tailoring standard group-level specifications and component or element-level specifications. This is accomplished by incorporating these standard specifications in their entirety and specifying required modifications or by referencing only the applicable sections of these standard specifications. CSS specifications are incorporated by reference in standard group, component and element-level specifications.

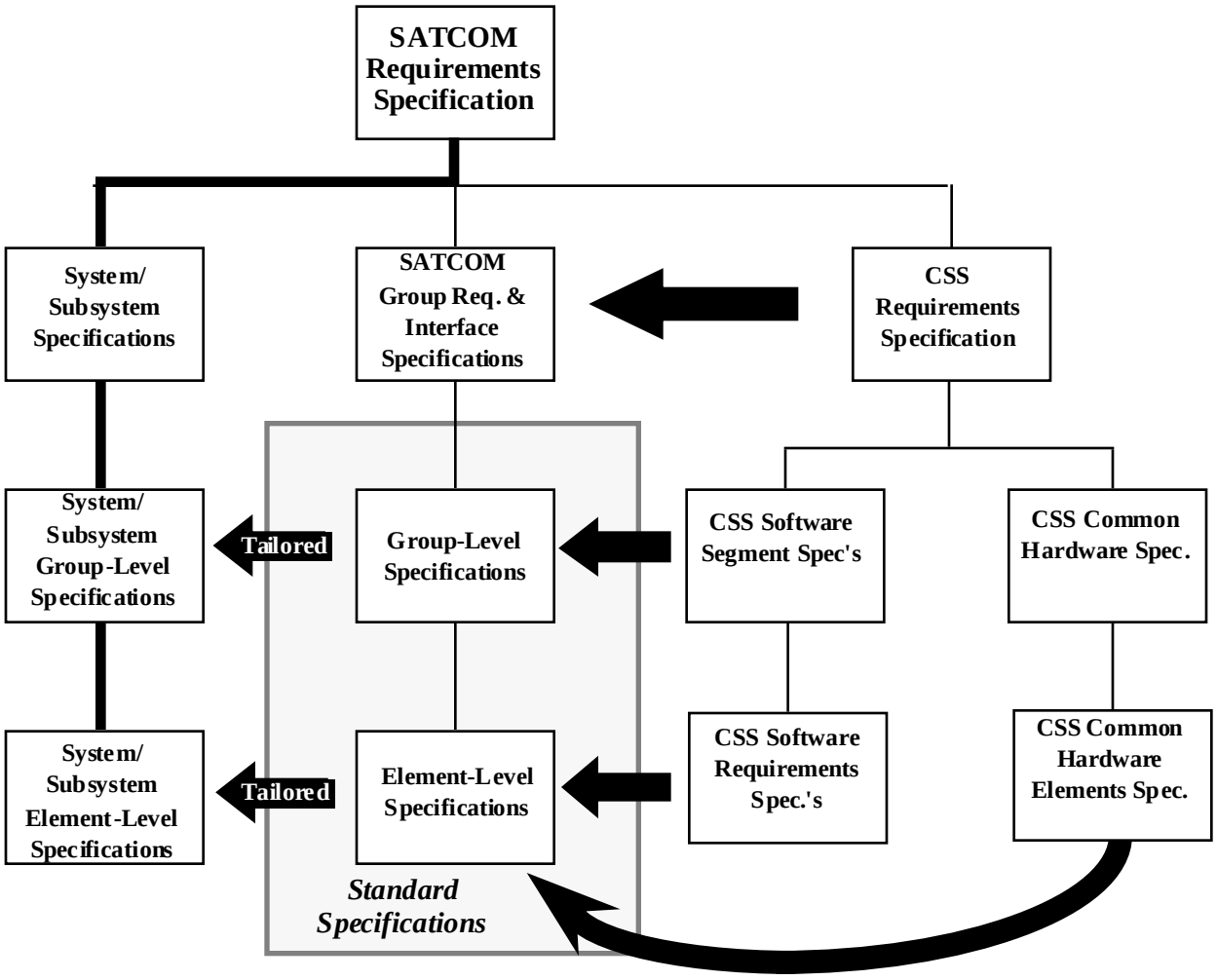


Figure 2.3.3.2-1 Basic Specification Tree Approach

To convey how the recommended hierarchy of specifications can be applied by the Program Manager or contractor, a real-world example must be considered. Figure 2.3.3.2-2 contains an example of how the Navy TACINTEL II Specification would be built. As can be seen, the TACINTEL II Communications Service Group requirements are derived by tailoring the standard Communications Service Group Specification that references applicable CSS Software Segment Specifications. This same process, of course would apply for each TACINTEL II group. If significant modifications of the standard group specifications are required for TACINTEL II application, these variances should be examined by the responsible organization to incorporate changes into standard group specifications that may be of general use for other programs.

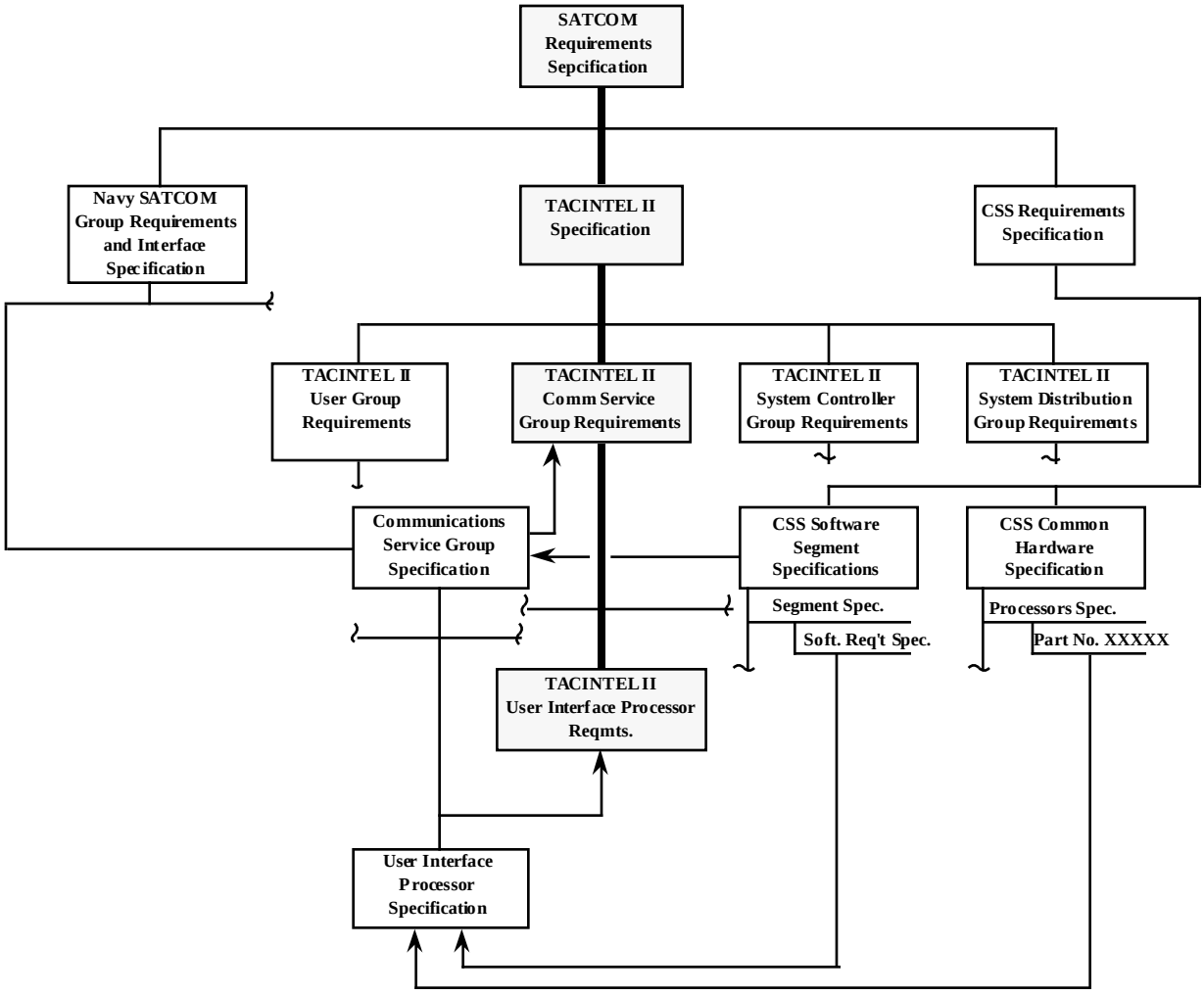


Figure 2.3.3.2-2 TACINTEL II Specification Tree Example

The TACINTEL II User Interface Processor requirements are derived from the standard User Interface Processor Specification that references the User Interface Software Requirements Specification and the part number for a standard CSS processor module. If for example, it had been determined that this standard processor module was inadequate for this application, a new processor module could be developed within the guidelines of the standard User Interface Processor Specification. Upon completion, the new processor can be added to the list of available CSS common hardware modules.

3.0 Integrated Communications System Description

3.1 Summary

The ICS makes the total RF capacity onboard a cutter available to ALL RF users. Allocation of the cutter's RF resources are allocated on a priority basis in accordance with a Communications Plan (COMMPLAN). Priorities are determined by each vessel based on user type and message characteristics (perishability, addressees, data precedence, etc.). The ICS provides automated network monitoring and management and assists operators in the assignment and control of communication equipment. The ICS is characterized by the following attributes:

a. Communication requirements of various Coast Guard user communities are satisfied within a single system design.

b. User mission area activities are not restricted to a specific communication service.

c. The modular "open system" architecture utilizes "standards" to promote rapid configuration, system growth, and enhance overall system survivability.

d. COMMPLANs provide users system control, allowing rapid and automatic system reconfiguration (e.g., transitioning to perform CTU functions).

e. Existing equipment is encapsulated, "non-standard" elements isolated within the "open" interfaces.

f. An adaptability to technological advances.

In summary, implementation of the ICS will resolve the issues of communications efficiency, RF channel scarcity, and the susceptibility of WMEC's and WHEC's to "lose" RF channels. The ICS provides users with a communication service independent of their message processing functions. Users will not be concerned with the specifics of the communications path taken by their messages. Rather, they will concentrate on their communications' destinations.

3.2 Integrated Communications System Framework

3.2.1 Overview

The ICS described in this study provides the Coast Guard with a dynamic and efficient communications service for multiple users onboard WHECs and WMECs. It provides communication services that are responsive to users and makes efficient use of available communications channel capacity. Rather than dedicating single RF resources to small communities of users, or single interests, as is currently done in the Coast Guard, the ICS provides a set of automated mechanisms that allow communication resource sharing and multimedia RF access. The performance realized by each user is enhanced because the functionality provided by the ICS is tailored to the user's end-to-end message transport requirements and includes improved technical capabilities not presently available.

The ICS layered network design is an "open architecture" that provides a framework for introducing new technology as it becomes available, ensuring a continuous improvement in the overall quality of communications service. In contrast, today's cutter systems are tightly coupled to specific communications equipment and RF media. Technology improvements cannot be incorporated without serious disruption or fundamental redesign of the systems.

In the ICS performance is enhanced through the availability of advanced network and multimedia gateway functions. The proposed ICS provides security mechanisms that permit the flow of information at multiple security levels. Figure 3.2.1-1 illustrates the ICS concept proposed for the Coast Guard WHEC and WMEC communications.

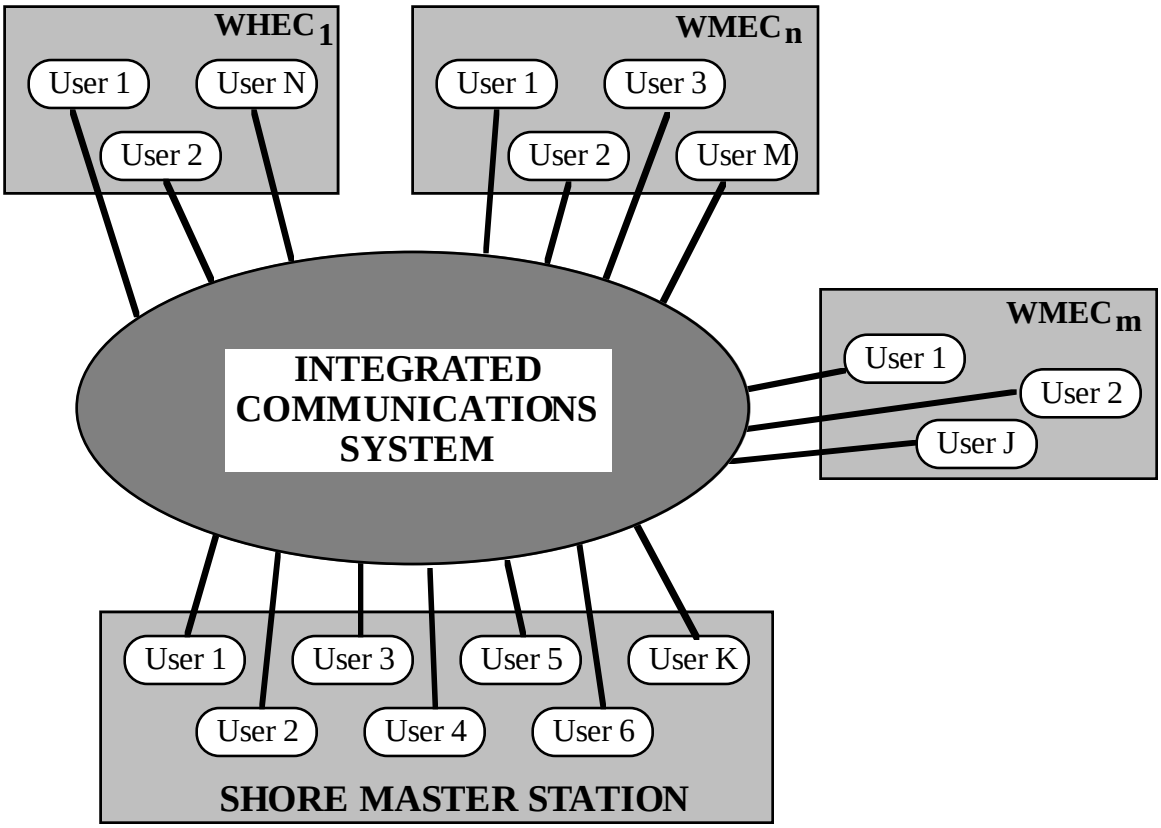


Figure 3.2.1-1 The ICS Concept

The ICS layered network architecture adheres to the International Standards Organization (ISO) OSI 7-layer model. Among the numerous benefits, this allows data link and subnetwork layer protocols to be designed and optimized for each specific RF media. This decouples the generic routing and end-to-end reliability functions from the signaling and link access functions which are highly media-dependent. Survivability is increased as the availability of multiple assets compensates for the vulnerabilities of any single circuit. By sharing media through the use of packet switching techniques, a significant improvement in the overall efficiency of Coast Guard communications is realized.

The ICS functional organization separates users into “communities of interest”. Each “community of interest” accesses the ICS through a Communications Server. The “community of interest” typically represents an application or a mission area distributed among multiple cutters and, possibly, a land-based communications facility. This approach enables data from each “community of interest” to be isolated from other “communities of interest” and from the ICS itself. For instance, users dealing with administrative messages could be associated with one “community of interest” while users dealing with highly sensitive drug interdiction information could constitute another “community of interest”. This isolation is handled by each ICS Communications Server through the use of data encryption. Header information containing

control and routing instructions bypasses the encryption process and is treated as GENSER SECRET by the ICS.

Each ICS Communications Server interfaces to the ICS Intelligent Gateway. The actual interface is based on communication services to be provided. Each Communications Server may have multiple logical service interfaces. Each service is customized to support specific information transfer requirements of the mission of the "community of interest". For instance:

a. Real-time data communication services (e.g., track updates) require minimum transit and processing delay.

b. Bulk file transfer services require accurate transfer of the information.

c. Organizational record messages require timely writer-to-reader delivery, accountability, message integrity, and, possibly, security.

The ICS Intelligent Gateway analyzes the message header and control information to make RF media selection and routing decisions in accordance with the Communications Plan. This plan is formulated in advance on a service-by-service basis for each "community of interest" and is coordinated amongst all platforms (cutters, aircraft, shore facilities, etc.) in an area of operation (e.g., Caribbean operations).

Each ICS instantiation communicates with other ICSs through the ICS RF resources. Conceptually, each resource represents a single manageable communications path over a specific RF media. The Intelligent Gateway selects the appropriate resource for user data based on the current operating conditions and resource allocations defined for the message's associated service as defined by the ICS COMMPLAN. This plan may limit the selection of resources that a particular service is permitted to use and may allocate a specific sharing of the resource's capacity among multiple services. The route selected by the Gateway may include multimedia networking through an authorized gateway (e.g., ICS instantiation aboard a WHEC in CTU). The ICS COMMPLAN authorizes specific ICSs afloat or ashore as gateways for specific services.

Each resource performs all necessary functions to process message data to the next destination site. Depending on the resource, this may include subnetwork, data link, error correction, modulation, and TRANSEC functions. It will always include full link-level encryption for communications security. Figure 3.2.1-2 illustrates the functional overview of an ICS platform.

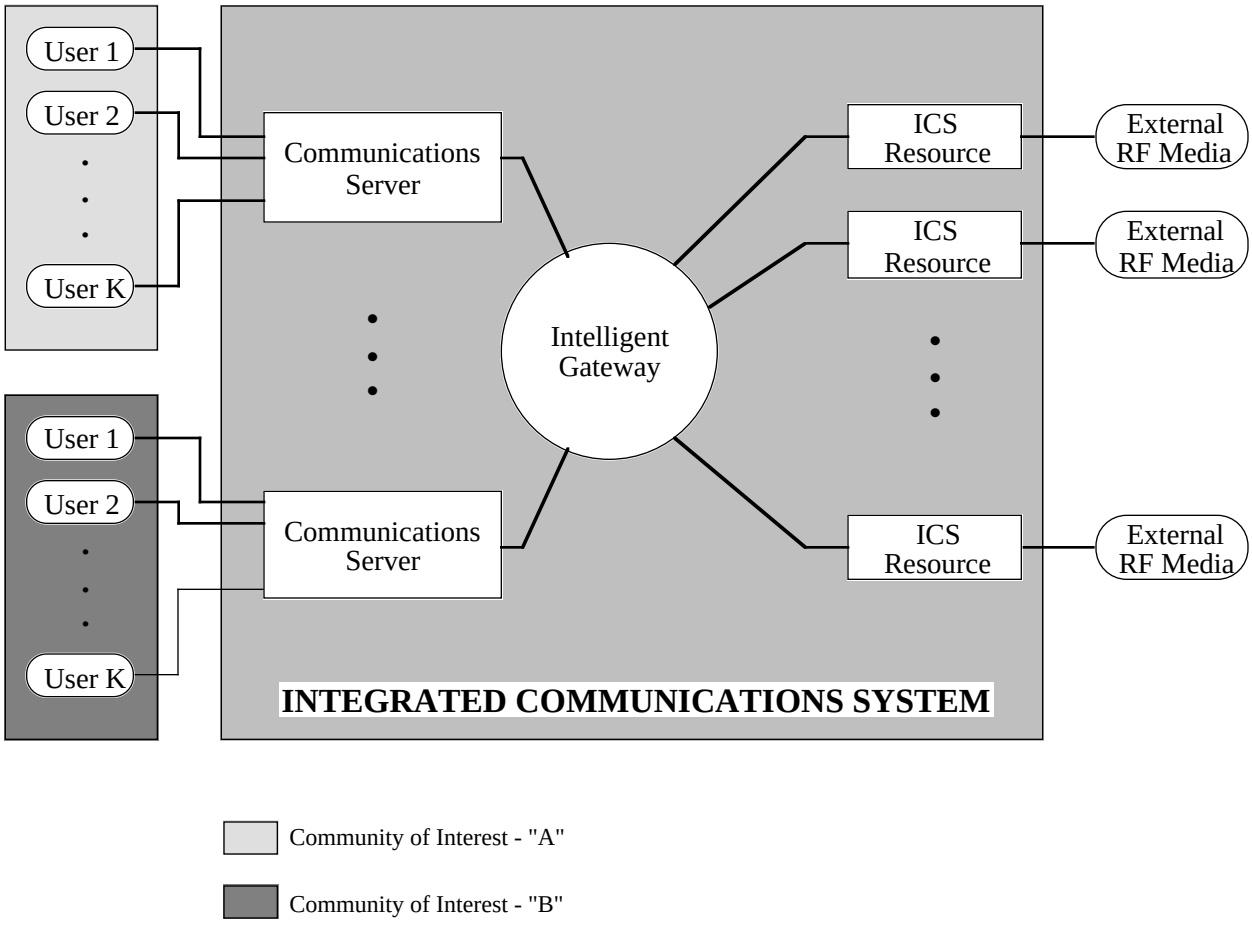


Figure 3.2.1-2 Functional Overview at ICS Site

3.2.2 Layered Protocol Abstraction

The ICS processing functions are allocated in accordance with the seven-layer OSI model. Any Application, Presentation (e.g., data compression), or Session layer functions required by the end-to-end users are performed by the "community of interest" specific ICS Communication Server. The Intelligent Gateway performs the Transport layer and the upper portion of the network layer. Both connection oriented (e.g., Transmission Control Protocol (TCP) or OSI Transport Protocol Class 4 (TP4)) and connectionless (e.g., User Datagram Protocol (UDP) or OSI Connectionless Transport Protocol (CLTP)) transport protocol are provided by the Intelligent Gateway. The Intelligent Gateway also implements the Subnetwork Independent Sublayer of the Network layer (e.g., Internet Protocol (IP) or the OSI Connectionless Network Protocol (CLNP)). This is the layer at which internetworking is performed.

The ICS Resource hosts the Subnetwork Dependent Sublayer of the network layer. This sublayer is responsible for converting any subnetwork unique characteristics into the standard protocol (CLNP or IP). The ICS Resource implements the Subnetwork Access Sublayer. This sublayer permits subnetwork protocols to be implemented to take advantage of the specific characteristics of the subnetwork and RF media. The ICS Resource implements the data link protocol layer using protocols designed specifically for the particular media. Finally, the ICS Resource implements, if required by the underlying RF media, the Media Access Sublayer of the data link layer**.**

3.2.3 Proposed Implementation Architecture

Figure 3.2.3-1 illustrates the proposed architecture for the implementation of the ICS aboard WHECs and WMECs. The ICS Communications Server is a VMEbus based multiprocessor unit incorporating a "modular security device" (MSD) as a means for providing security isolation for the "community of interest." Users interface with the ICS Communications Server via a shipboard Local Area Network (LAN) utilizing a standard protocol. The Intelligent Gateway exchanges information with each Communications Server (via a standard protocol) over a communications LAN physically isolated within the domain of the ICS. The ICS Resources are implemented physically on VMEbus single board computers. Illustrated in Figure 3.2.3-1 are UHF SATCOM and HF resources. Each resource is accessed via a single board modem, single board receiver/exciter, and the MSD.

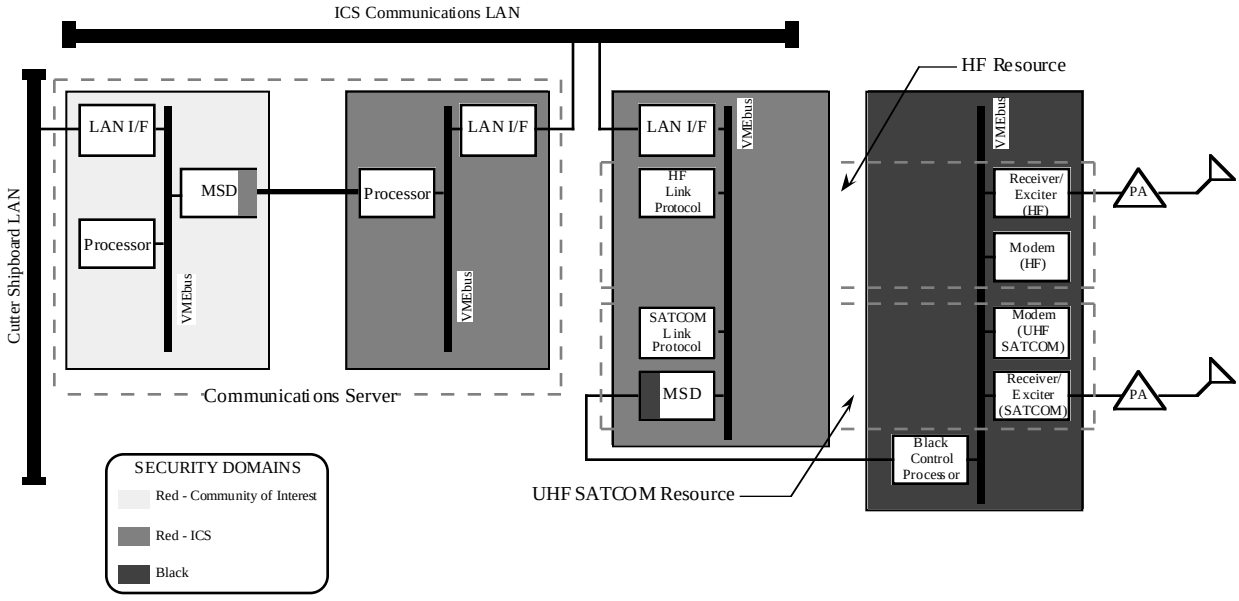


Figure 3.2.3-1 Proposed ICS Architecture

3.2.4 ICS Security Architecture

The proposed ICS provides an effective approach for integration of communications resources, communications services, and security mechanisms into a unified architecture. As already discussed, ICS is based on an "open system" architecture, layered to provide service options for implementation of various message processing subsystems. The ICS security architecture, as discussed in the previous subparagraphs, divides the ICS into a "black" (radio resources) security "zone", a "red-ICS" (ICS network management and resource access) security zone, and a "red" (user/ICS data processing) security zone. The red zone processes plain text information for both secure and GENSER users. The red-ICS zone contains encrypted user information identified as BLACK (encrypted) secure and (encrypted) GENSER information, BLACK (encrypted) non-real-time ICS control information (e.g., routing database updates), and unencrypted ICS real-time resource management information. In the BLACK zone, all user information and non-real-time management information undergoes a final, link encryption for transfer between ICS shore facilities, cutters, and airborne platforms.

Figure 3.2.4-1 shows how the ICS would be implemented using a centralized, trusted system. A trusted operating system (kernel) would enforce all security operations of the system and mediate

operations among ICS elements. ICS elements (or processes) would intercommunicate via the InterProcess Communications (IPC) shell under control of the trusted operating system. The IPC would also provide trusted downgrade of data, such as headers or Link COMSEC signaling information, where necessary for separation from classified data. Within those areas where multiple levels of data may be simultaneously processed, multiple domains would be partitioned to guarantee separation for all protocols and data storage.

Users would enter the ICS at a SYSTEM HIGH level and be processed within a common security domain at a pre-specified security level. Thus, referring to Figure 3.2.4-1, User Group B would be accepted by the ICS at security level i, while User Group A (composed of two users, user 1 and user 2) would be operating at level j. If levels i and j are not equivalent (including authority and privileges), then "COMPUSEC" is required to maintain trusted separation of the users. Likewise, if user 1 and user 2 of User Group A transfer data at different security levels, “COMPUSEC" is required to maintain separation at the User Interfaces.

Data ready for transfer across the link would be separated into transmission data and signaling data and output via a Link process to the Link COMSEC.

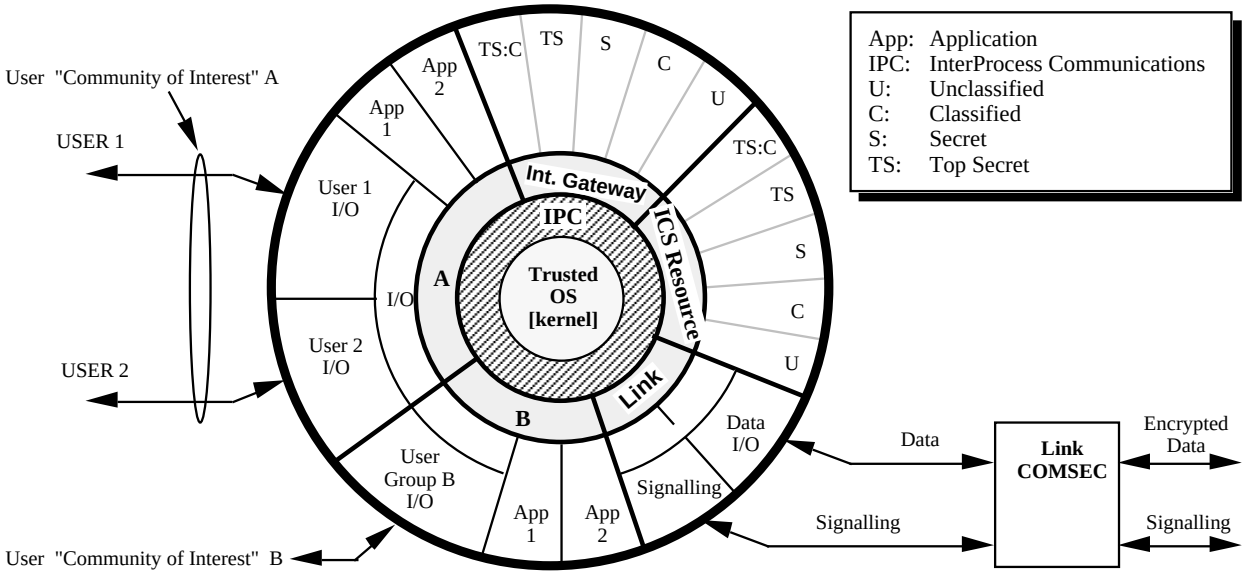


Figure 3.2.4-1 ICS Implemented With Centralized Trust

The centralized approach of Figure 3.2.4-1 can be distributed for realization within ICS. This is indicated in Figure 3.2.4-2.

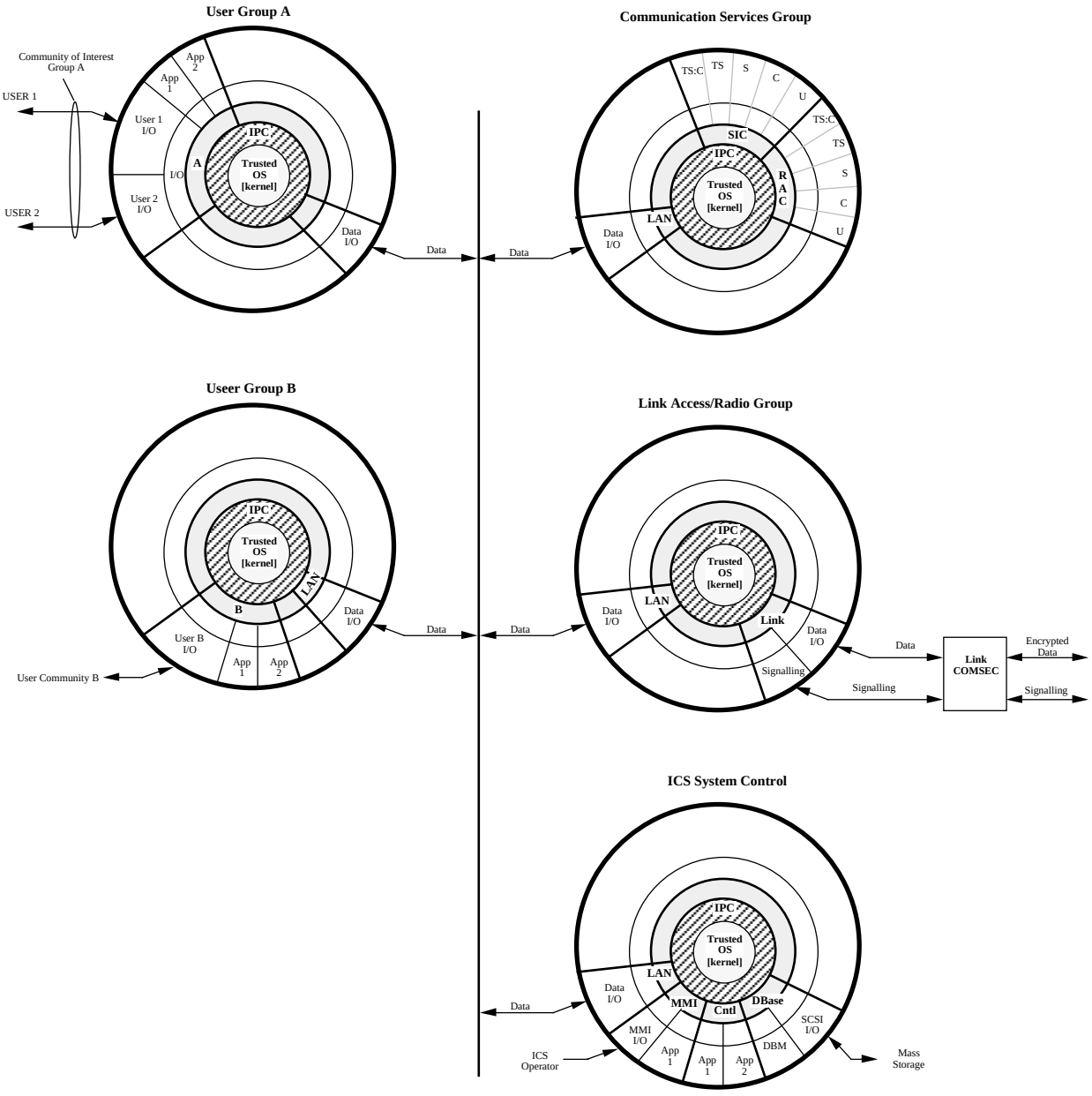


Figure 3.2.4-2 ICS Implemented With Distributed Trust

3.3 Operator Interface

This study proposes that the GUI use the X-Window/MOTIF System. This is a COTS product. The proposed Open Software Foundation (OSF) MOTIF widget set has been accepted as the standard (Navy Standard for C4I Systems) for Navy systems and Coast Guard users of the JOTS system. Users aboard WHEC's are already familiar with the "look and feel" of GUIs built with this interface standard. The MOTIF system provides consistency and high readability. The operator uses the standard point and click method to select operations to be performed.

The recommended ICS operator interface provides a window-based user access capability to the ICS functions. This graphic user interface (GUI) is color, bit-mapped, graphics-oriented and

user-extensible. It provides functions to concurrently control and monitor the system while simultaneously performing other tasks such as message editing. Functional controls available to the operator are provided in a graphical context. Graphics minimize the learning curve for the operator and minimize the amount of training required.

This multi-display, X-Windows-based operator interface has many advantages.

a. It supports concurrent operator activity, high efficiency, and ease of operation.

b. Enormous growth potential and flexibility are provided through decoupling of data processing from the presentation of the data. This approach allows the system developer to change the functionality of the system by simply adding applications and their respective X-client rather than modifying existing applications. This strongly facilitates the ability to incrementally improve the operator functionality.

c. This approach facilitates iterative prototyping (iterative feedback from the Coast Guard community and future users) during development phase of the ICS virtually guaranteeing the development of an operator interface well received by the WHEC and WMEC crew.

A key feature of the X-Windows/MOTIF implementation is the separation of the physical data from the actual presentation of the data. ICS software processing the data forwards it in "raw" format to the operator interface software. The operator interface software is then responsible for the "presentation" of that data to the operator via the display. This approach provides unlimited flexibility since the data presentation can be changed without any impact to the data processing software. This decoupled approach provides the flexibility to migrate to future window systems as these new standards and technology emerge.

The X-Window System operates using the client-server model paradigm depicted in Figure 3.3-1, where an independent collection of loosely-coupled data processing software modules (clients) interact with a display server controlling the visual presentation of data as a "window manager" onto a display(s). It permits easy expansion by the activation of additional X-clients performing the same and/or different functions. Multiple X-clients can be associated with a single X-server window manager. As shown in the figure below, each X-client controls the actual presentation characteristics of data on a display. The X-server operates on behalf of clients. It also provides the overall management of the windows on the display(s) and drives the physical interface to the display device. Introducing additional display devices does not require any changes to the X-server, only the mapping of new X-clients to the new devices.

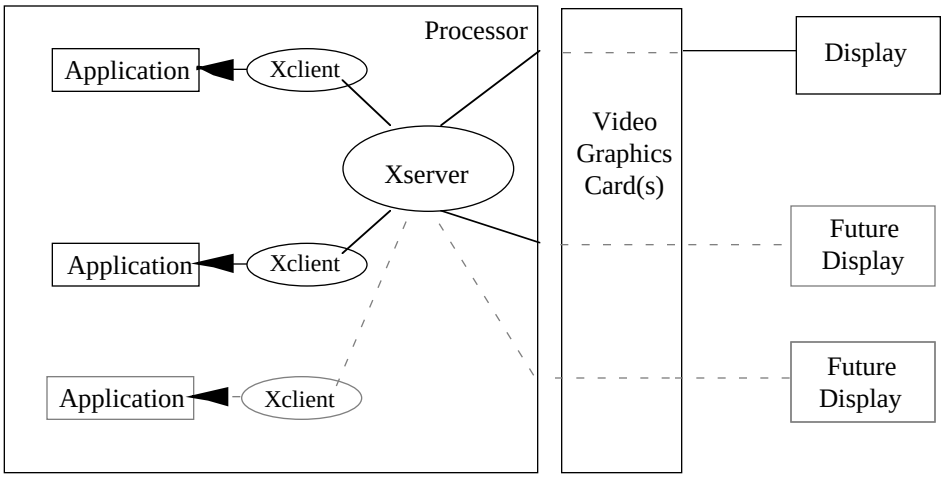


Figure 3.3-1 X-Client to X-Server Relationship

The proposed operator interface is based upon a model where system functions are "selected" from a main menu and cascading selections. The main menu bar, shown in Figure 3.3-2, is common across the top of all displays and is presented upon system startup. All functional windows are presented in the open space below the menu bar. The following figures and paragraphs present a possible implementation of the operator interface for the ICS.

Figure 3.3-2 Sample Prototype ICS Main Menu Bar

In the proposed model, the main menu bar provides access to the presentation of system alarms. All detected anomalies result in an alarm that is presented in an alert window (Figure 3.3-3). The alert window presents the alerts in sequential order and provides a time-stamp of when the anomaly was detected. All alarms are stored in the mission log as well. Alarms may be classified as critical, serious, minor and informational depending on the impact to the system mission. Critical and serious alarms result in a pop-up window that provides a description of the alarm conditions and prompts the operator to acknowledge the alert condition; operator acknowledgment is required.

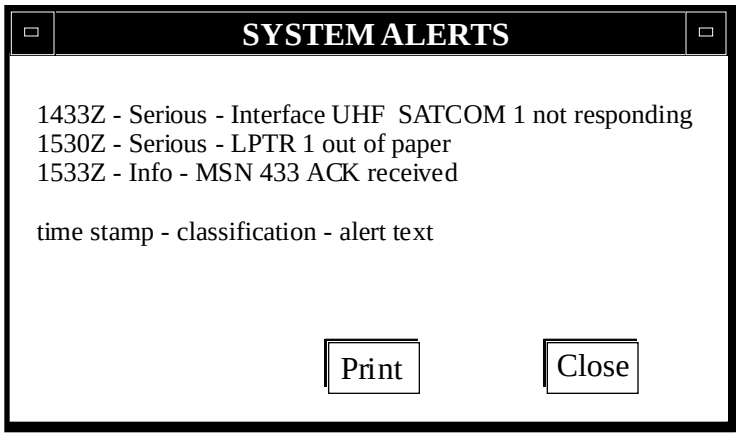


Figure 3.3-3 Alert Window

Message Processing and Communications Control applications are selected from the main menu. These application functions are implemented as separate processes that execute independently. As such, they control their own windows and can be updated (i.e., software modified) with no impact to other functions. As additional functions are added to the system, the selection menus are updated (without impacting existing function) and the application is easily integrated into the system.

Figure 3.3-4 shows a message processing window that allows the editing of messages, both previously received and those created "from scratch." The editing capabilities provide the manipulation of messages and for retrieving messages from the system database for editing purposes. Included in this window is the ability to select the disposition of the message, such as:

a. Save for later processing

b. Transmit over a specific interface

The states of any operator actions are preserved while that window is not the active window.

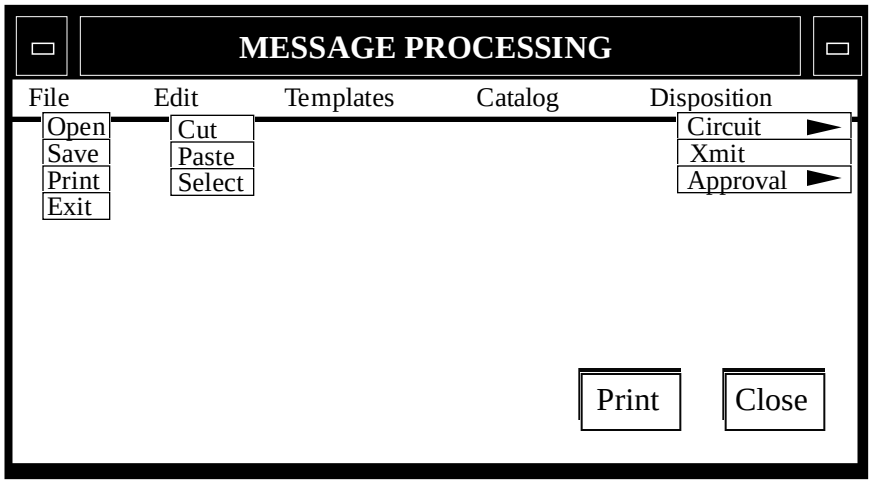


Figure 3.3-4 Message Processing Window

During the course of a cutter mission, significant amounts of labor intensive time are spent in the creation, command approval, accountability, and transmission of narrative messages. The implementation of pop-up windows is well suited to the current mission activities associated with this whole message generation process. Within the proposed ICS architecture multiple graphic display devices are implemented. The following scenario demonstrates how this proposed operator interface could easily be implemented to automate this labor intensive process.

A message is created by an operator working at a remote display. He forwards the message to the command authority responsible for approving transmission. An audible alarm is triggered at the command authority's display . The message processing pop-up window appears (as shown in Figure 3.3-5) containing the message text, time of receipt and associated attribute information. The narrative message pop-up supersedes and hides any current window activity, highlighting its importance. The message can be forwarded to any display consoles to allow the command authority to order any other officer to process it.

The officer accepts responsibility by selecting the "take control" button, thus locking out others from processing the message. An indication is provided on the original message creator's window to show where the message is being processed. All the standard word and file processing functions are available, including edit, save, and "save as". The specific layout and operation of the windows will be defined by the Coast Guard. However, as shown by this example, one can easily envision the multitude of available options available in this GUI.

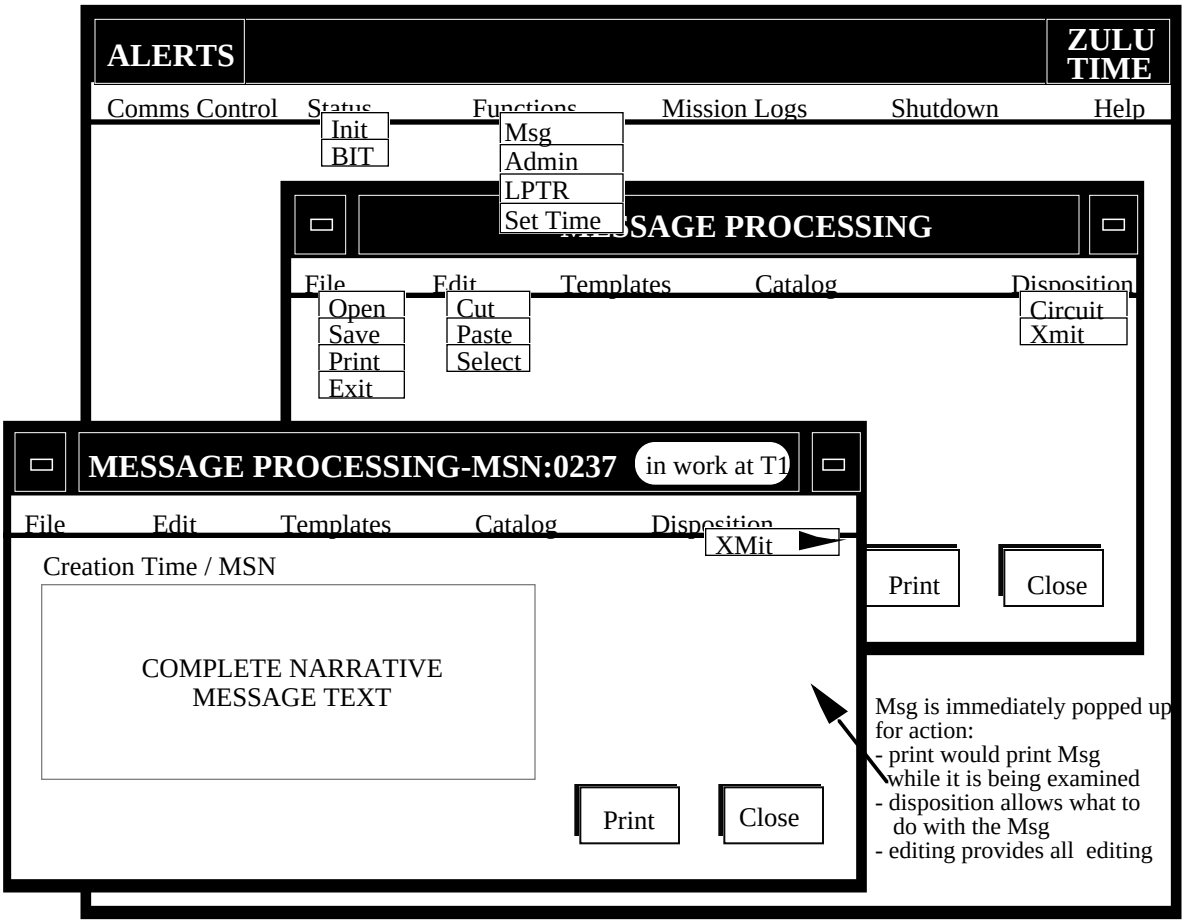


Figure 3.3-5 Narrative Message Pop-up Window

Another capability of the GUI is the Mission Log. This log contains data for post-mission analysis. A GUI Mission Log would consolidate mission information on a single media and improve the operations to facilitate a more efficient, automated command environment.

The windowing system allows for the stacking, in foreground or background, of any windows. Alternatively, if desired, windows can be tiled and iconified to avoid overlap. Windowing allows the operator to simultaneously work on many tasks and increases the effectiveness of the operators. It allows the operator to easily switch between functions as events occur.

This proposed operator interface adheres to the standard X-Windows/MOTIF based “look and feel” being promulgated within the Navy. For comparison purposes, Figure 3.3-6 illustrates window configurations for the recently deployed NAVMACS-II system.

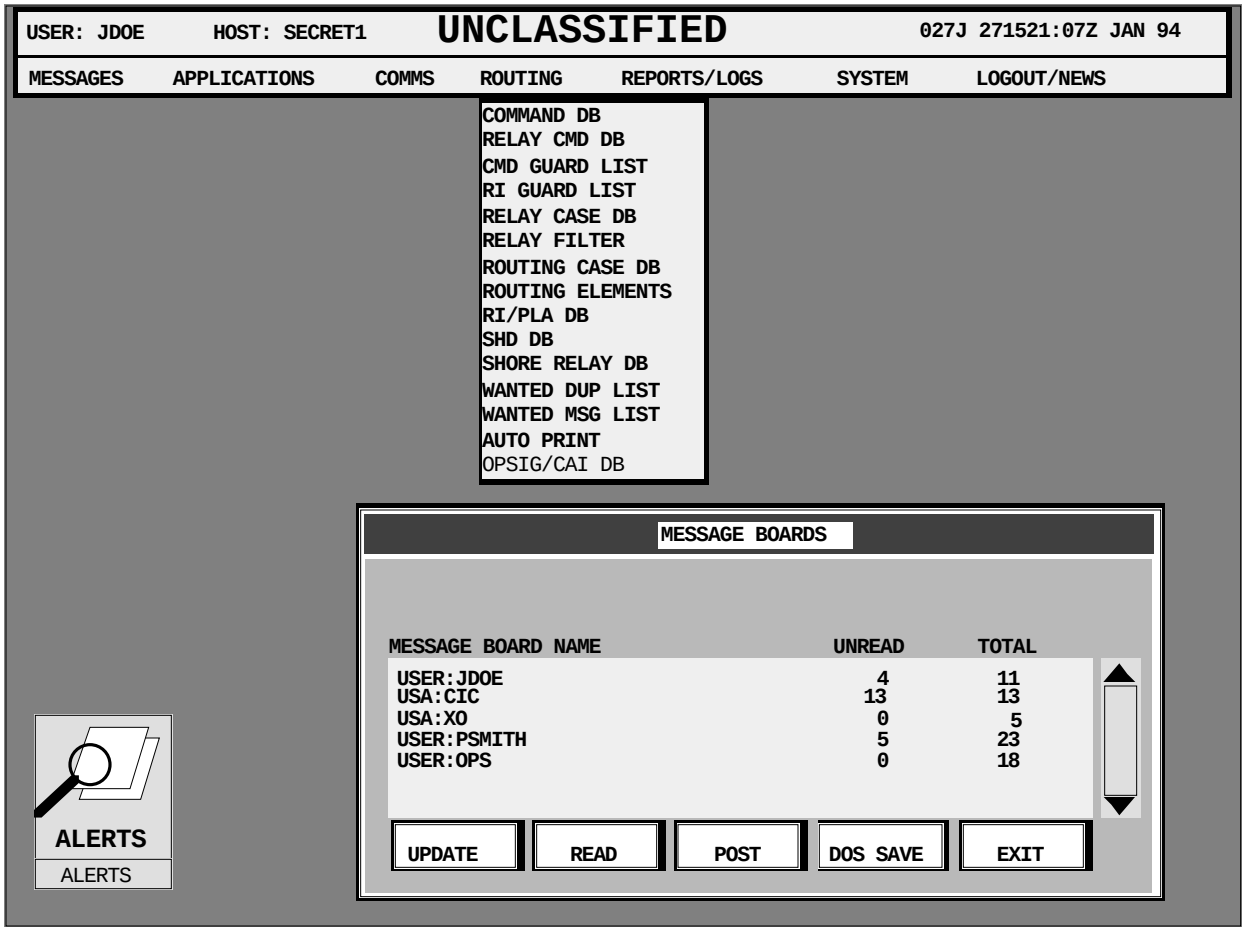


Figure 3.3-6 NAVMACS-II Main Screen

3.4 Hardware/Software Architecture

The recommended ICS hardware/software architecture for the Coast Guard WHECs and WMECs is a *loosely-coupled* distributed system. The term "coupling" is a common term, used to measure the strength of interconnections between modules, processes or components of a system or software program. A high coupling would indicate strong dependencies between one process and another. Loose coupling allows greater flexibility in the design and better traceability, isolation, and correction of faults. The strength of coupling depends on the number of references of one process by another, the amount of data passed (or shared) between processes, the complexity of the interface between processes, and the amount of control exercised by one process over another. Significant inherent advantages are gained by this approach, including:

a. Promoting future expandability/changes. User functions can be added, modified, or removed without impact to communication functions. Likewise, future communication circuits handlers can be implemented, upgraded, or eliminated without affecting existing user functions.

b. Increasing overall fault tolerance. The effects of software failures are localized and isolated; failures are not propagated through the system.

c. Obtaining greater implementation options. The user and communications functions can be distributed onto hardware components better suited to host

their respective processing needs. As greater communication requirements are imposed on the ICS, communication functions can be migrated onto an upgraded or replacement hardware host with no effect on the user functional domain (software and hardware host).

The hardware architecture proposed for the ICS has been driven by requirements for fault tolerance, open architecture, and expandability. The proposed architecture satisfies these requirements through a distributed hardware architecture that is based on commercial technology and standards and is field-proven in numerous critical communication applications.

In the proposed ICS hardware architecture, the communication functions and user functions are hosted in separate distributed subsystems. In this manner, this study can apply to each subsystem the unique fault tolerance, processing power, and expandability requirements of that subsystem. In the recommended ICS architecture an industry standard fiber-based high speed Ethernet LAN serves as the systems communications backbone. This provides a significant expansion capability to the ICS. Any device or computing systems with this high speed Ethernet interface can be seamlessly introduced to the system. Examples include laptop computers, workstations, PCs, printers, and storage devices.

Furthermore, each subsystem includes the industry standard Small Computer Standard Interface (SCSI) bus. This is a high-speed peripheral bus over which processing units can access peripheral devices. These peripheral SCSI devices can include additional random access mass storage devices (Winchester, Bernoulli, optical, etc.), tape units (DAT, 1/4" Streaming, 8 mm, etc.), as well as printers.

Within each subsystem, the components communicate via the VMEbus, another industry standard communication medium. These components are standard “6U” format VMEbus SBCs. The VMEbus based approach is recommended because of the demonstrated reliability, capacity, processing density, and flexibility of the technology. Operator control of the system is effected through bit-mapped color display terminals. These may be implemented in the ICS in any of the following manners:

a. Stand-alone workstation connected via LAN to the ICS.

b. Standalone X-Windows terminal connected via LAN to the ICS.

c. Keyboard, mouse/trackball, graphic display hardware attached to a VMEbus graphic interface card.

The minimum requirements recommended for the ICS operator interface is a display exhibiting at least a 640 x 480 pixel resolution on a viewing surface exceeding a 14 inch diagonal. The operator interface protocol must also conform to the X-Windows MOTIF based GUI as described in section 3.3.

The software architecture proposed for the ICS is based on an open, layered, modular, and distributed architecture. ICS software components are distributed horizontally across the ICS network, stacked atop a UNIX operating system layer. These horizontally distributed ICS application components are ICS external RF communication control, ICS system control, and message processing functions. Figure 3.4-1 illustrates the horizontally distributed architecture of the ICS.

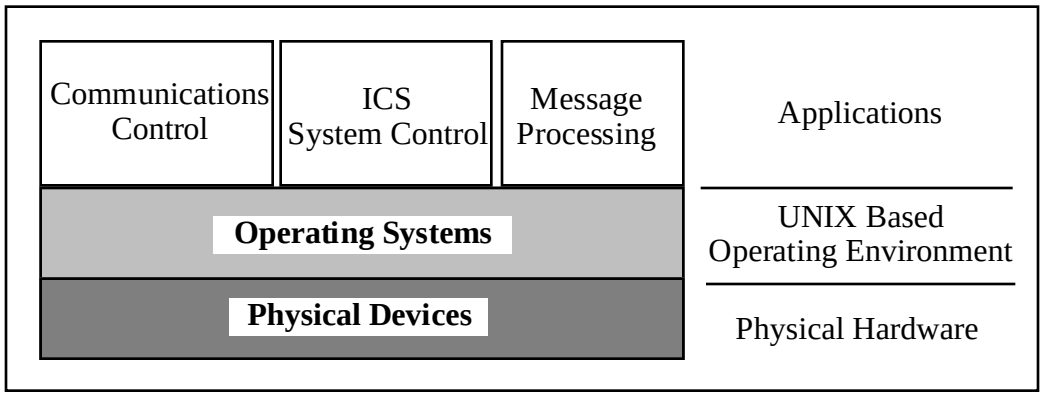


Figure 3.4-1 ICS - Horizontally Distributed Architecture

ICS software components are designed to operate horizontally across a loosely coupled collection of individual VMEbus based single board computers (SBCs). These SBCs are coupled via a VMEbus backplane or an Ethernet-based LAN. The VMEbus and UNIX-based hardware framework permits the use of many different COTS operating systems which operate simultaneously on SBCs within a given VMEbus chassis. This architecture permits the individual processors in the system to use shared resources in the network. Resources are any component in the system that provides a service. For the ICS, this includes the printers and display/keyboard devices. Resources include software applications or functions that are purposely decoupled as a standalone server to be shared by any software application. Examples of such servers include data conversion servers and expert system inference engines. Resources are shared across the system open to use by any application.

For the ICS, minor enhancements will be required (layered over the UNIX-based operating system) on each SBC in the ICS network. These system enhancement modules will use the Ethernet and the VMEbus backplane to coordinate their activities and transfer data between them. This system architecture is known as a loosely-coupled, distributed system and is depicted by Figure 3.4-2 below. The ICS enhanced UNIX operating environment provides the framework for a scaleable, fault tolerant open system architecture for the ICS by defining an operating environment whereby the details of system components and details of their separation and location are concealed from the ICS functional applications. Interaction (synchronization, communication, etc.) amongst applications and between applications and system resources occur irrespective of the actual physical distribution.

Scaleability is provided by the horizontal distribution of software components. If greater processing power is required by the ICS, additional instantiations of the enhanced UNIX and its associated SBCs are introduced into the system. The existing ICS applications are then redistributed accordingly, over the SBCs without any software modifications. Fault tolerance is inherently provided through the enhanced UNIX framework as the effects of hardware and software faults are naturally localized without disrupting the entire ICS system.

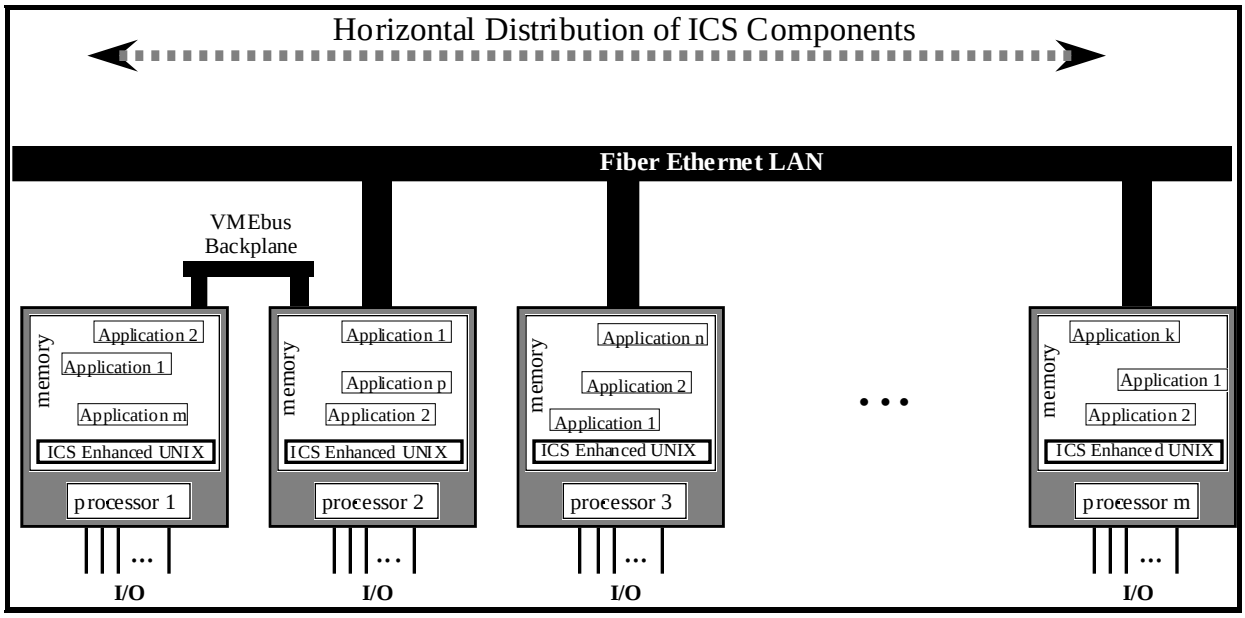


Figure 3.4-2 Loosely Coupled Distributed System

The inherent ability to use heterogeneous processors for the ICS is a critical element of the requirement for a flexible and open architecture. This requires the definition of a consistent interface to the application regardless of the architecture of the Central Processing Unit (CPU). In support of this requirement, the ICS UNIX enhancements modules provides machine-independent extensions as shown in Figure 3.4-3.

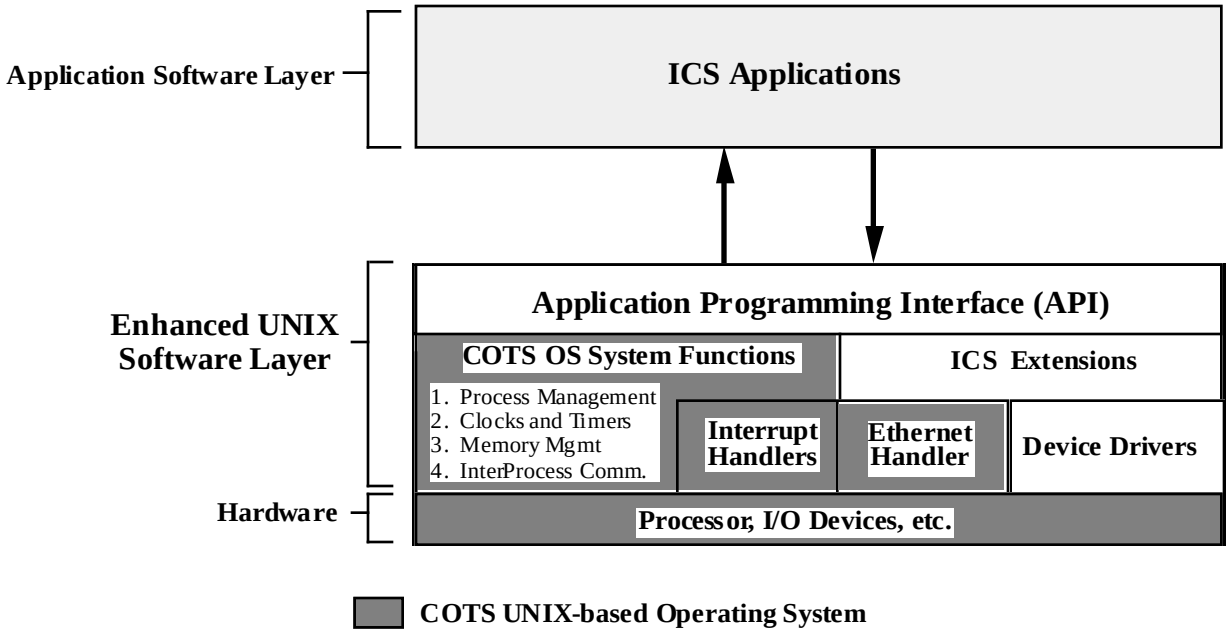


Figure 3.4-3 Enhanced UNIX High Level Architecture

The ICS operating environment incorporates other NDI software in addition to the COTS UNIX based operating systems. This includes the MIT X-Window System, X-Network Protocol and Base Window System for the MOTIF GUI implementation, and BIT and board support packages from the commercial SBC manufacturers. Custom serial interface drivers for specific radio/cryptographic equipment can also be used.

The enhanced UNIX Application Programming Interface (API) provides a standard interface to all ICS applications. This interface completely abstracts the physical details of the ICS hardware and software topology from the applications. Internal changes to the ICS operating environment may be made transparently to the ICS applications. This allows the ICS to take advantage of emerging COTS technologies in hardware, communication protocols (e.g., OSI Transport Protocols, Express Transfer Protocol (XTP), etc.), and operating systems during the course of the ICS life cycle. These advantages may manifest themselves in cost savings, performance improvements, size savings, increased reliability, or any combinations of these.

3.4.1 VMEbus

The hardware basis of the ICS is the VME backplane. The blossoming popularity of the VMEbus in the commercial marketplace has created a large vendor base, offering a wide range of high performance processor boards for use in real-time applications. For the Coast Guard, adopting the VMEbus open-bus architecture offers the benefit of access to this wide and readily available collection of COTS computing elements. These components can be integrated in a modular and expandable fashion into high performance processing engines.

The topology of the cutter radio room is based upon a collection of interconnected backplane networks. Each backplane network is hosted by a single VMEbus chassis. These networks are, in turn, interconnected via a fiber-based LAN. Communication functions (i.e., software application modules) are distributed onto the various VMEbus CPU boards within the system. A key element of this architecture is its "dynamic" (vice "static") nature. Communication functions are not statically assigned to specific processor domains, but are dynamically distributed throughout the ICS as dictated by operational needs. Likewise, processing components are not "hard-wired" for specific physical placement into a specific VMEbus chassis and slot. The number and the slot locations of CPU boards populating a particular ICS VMEbus chassis are not fixed.

For the ICS, two important requirements are the bootstrap and dynamic reconfiguration capabilities of the system. A key feature of the ICS architecture is the concept of "no single point-of-failure". During bootstrap, no single hardware component is required to initialize the system. Hardware components need to engage in adjudication processes for initialization. Likewise, system recovery from anomalous conditions such as power-outage conditions are rapid, even with the presence of failed hardware components. The rapid replacement, removal, and insertion of CPU components with minimal impact on the overall system are also key characteristics. Bootstrapping entities are able to detect, locate, and recover from the effects of hardware errors. This requirement, coupled with the need to minimize operator intervention during the bootstrap process, implies substantial adjudicating intelligence at the bootstrap level. Bootstrap logic determines the physical configuration of the system and adjust its processing accordingly. Board level bootstrap activities within a VMEbus chassis are coordinated, and the collective bootstrap activities between separate VMEbus chassis are also coordinated.

The ICS initialization/recovery/restart requirements impose an implicit requirement on a processor at the bootstrap level to determine its physical location and the existence and locations of other processors. This capability could easily be met if the VMEbus supported geographical addressing. However, since the VMEbus lacks this design characteristic, the VMEbus address range at which a board's onboard memory decodes on the VMEbus must be carefully set for each board. Normally, this is performed via configuration jumpers, very carefully set to avoid any

processing conflicts (overlapping VMEbus addresses) prior to insertion into the backplane. However, in order to further minimize operator intervention in this rather involved complicated procedure, a pseudo-geographical addressing scheme is recommended for the ICS. One possible scheme would be to artificially assign to each VMEbus slot a specific VMEbus address range. This simplifies and codifies VMEbus addressing conventions in very simple terms. Cards could readily be inserted into and exchanged between chassis. All that would be required of operators would be to ensure that a card's VMEbus address conforms to the base address defined for its destination slot.

The recommended approach to use the VMEbus does not preclude the future transition to FUTUREBUS+. The transition process to FUTUREBUS+ components mirrors and is, in fact, identical to the earlier discussion regarding growth and flexibility.

3.4.2 Transition to FUTUREBUS+

The advantages of FUTUREBUS+ over VMEbus are significant in the area of throughput and flexibility. Consequently, FUTUREBUS+ must be kept in mind for future integration into the ICS. Data throughput in FUTUREBUS+ is approximately 120 Mbps. This is four times the maximum theoretical VMEbus rate and is actually ten times the typical VME transfer rate. The advantage for communication systems in general translates to less bus latency and shorter data transfer queue times. Another advantage of FUTUREBUS+, of particular significance for the ICS, is that it provides a means to replace modules without removing power (i.e., shutting down) from the chassis hosting the FUTUREBUS+ backplane (“hot insertion”, “hot extraction”) as FUTUREBUS+ does not employ daisy chained data or arbitration signals like the VMEbus.

The hardware design of the FUTUREBUS+ accommodates the best qualities of current design practice. It also incorporates features most appropriate for future designs. The bus is not modeled after any vendor specific CPU control signal pattern but, rather is a true open architecture capable of use by many manufacturers. Even the newest massively parallel and data flow designs can be interfaced into the master bus environment. Since the bus defines a method of communication between peers, any high performance application requirements within the aggregate bandwidth of the bus (400 to 3200 Mbytes/second) can be designed using FUTUREBUS+. Therefore, the bus does not limit the of CPU or the mixture of widely differing CPUs in the same system.

FUTUREBUS+ was a product of the joint Navy and industry group - the Next Generation Computer Resources (NGCR) program and the IEEE. Both groups were instrumental in promulgating a standard which is flexible to satisfy industry R&D planners as well as NGCR planners. COTS procurement was the stated Navy objective for the joint Industry/Navy NGCR working groups. The commercial participants were given some advance looks at the future directions of Navy programs. Some of the commercial participants disclosed the direction of their applicable planning. At all times the objective of the NGCR working group and IEEE was to produce a non-proprietary bus standard which would appeal to the broadest spectrum of commercial and Government users. This can be contrasted with the VMEbus standard which, though now considered an universal standard, was an offshoot of a proprietary Motorola backplane bus (the Versa Bus) which was designed using embedded Motorola processors.

Thus, FUTUREBUS+ developers are able to more fully focus their energies on other issues other than how to talk between dissimilar boards. There is, in fact, a parallel which occurred in the DARPA (now ARPA) community. Vendor, hardware, and software independence were among the goals of the Internet project. Once the network protocols were standardized, then almost all commercial vendors began to offer TCP/IP software and hardware options. So too, FUTUREBUS+ should allow designers to advance the state of the art in CPU, memory, and I/O

designs because there is a common universally defined method of communicating among these system components.

There will be an obvious ramp-up time for commercial vendors before COTS benefits will accrue and the Coast Guard can begin taking advantage of this technology. However, an important ICS implementation and architectural consideration to be taken into account is the currently available "bridged" solutions which will run commercially available VME controllers on carrier boards which mate directly to FUTUREBUS+. This technique is currently widely used by a number of vendors such as SUN Microsystems, Harris, Bull, Unisys, and others to incorporate VME I/O controllers onto proprietary backplanes. As industry has already determined the physical and module interface characteristics required to simultaneously operate both the VMEbus and FUTUREBUS+ buses within the same physical package, this means that any VMEbus based implementation of the ICS is easily upgradeable and transferable to FUTUREBUS+.

3.5 Coast Guard Standard Interior Communication Protocol Architecture

Of significant importance to the ICS, is the definition of a message routing system which would allow PC or workstation based message processing subsystems to interface with the ICS for the purposes of sending and receiving messages as well as to provide the capability to exchange bit-oriented messages (BOM) correctly with other message processing subsystems possessing differing hardware architectures (i.e., internal data representations). This information routing system would be used by miscellaneous workstations, servers, sensor systems, and other elements internal to a cutter. The ICS Communications Server serves as the central element in this proposed message routing system. Figure 3.5-1 illustrates the relationships between message processing subsystems and the ICS.

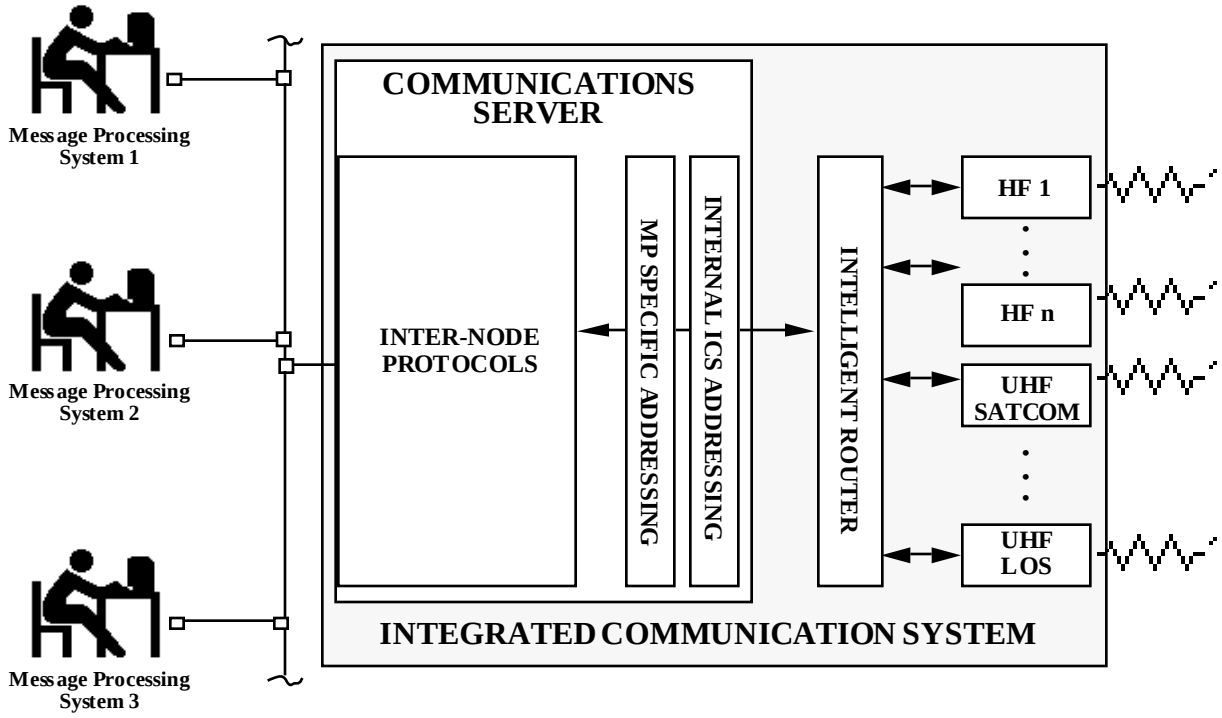


Figure 3.5-1 Internal Message Processing Subsystems/ICS Relationship

The ICS Communications Server interfaces to the locally networked "dissimilar" message processing subsystems via a Local Area Network (LAN). “Dissimilar” subsystems are computers with different magnetic storage and data representation. Magnetic storage and data representation differences include different data alignment (store data by individual byte or multiple byte boundaries), data sequence (most significant byte ordering), and floating point representation (IEEE or a proprietary representation.). Although, SAFENET has often been mentioned for eventual adoption as the Coast Guard standard for intra-platform information exchange network, Fast-Ethernet (CSMA/CD), Switched Ethernet (CSMA/CD), or a cell-switched based LAN is recommended for this shipboard information highway. The basic rationale for this recommendation is the assumption that emerging end-user technologies for the Coast Guard will be data intensive and will boost the bandwidth requirements of the LAN while also imposing deterministic and extremely low latencies.

The ICS Communications Server interface to the Intelligent Gateway provides to local message processing systems, access to ICS RF communication resources. The ICS Communications Server itself provides the actual interface between local message processing subsystems and the ICS Intelligent Gateway. Through the message processing subsystem to ICS Communications Server interface, the ICS inherently provides a communication capability to locally attached message processing subsystems to transmit to and receive data from users located both locally on the cutter as well as on external Coast Guard platforms or shore facilities operating in dissimilar workstations. The two distinct interfaces are illustrated in Figure 3.5-2.

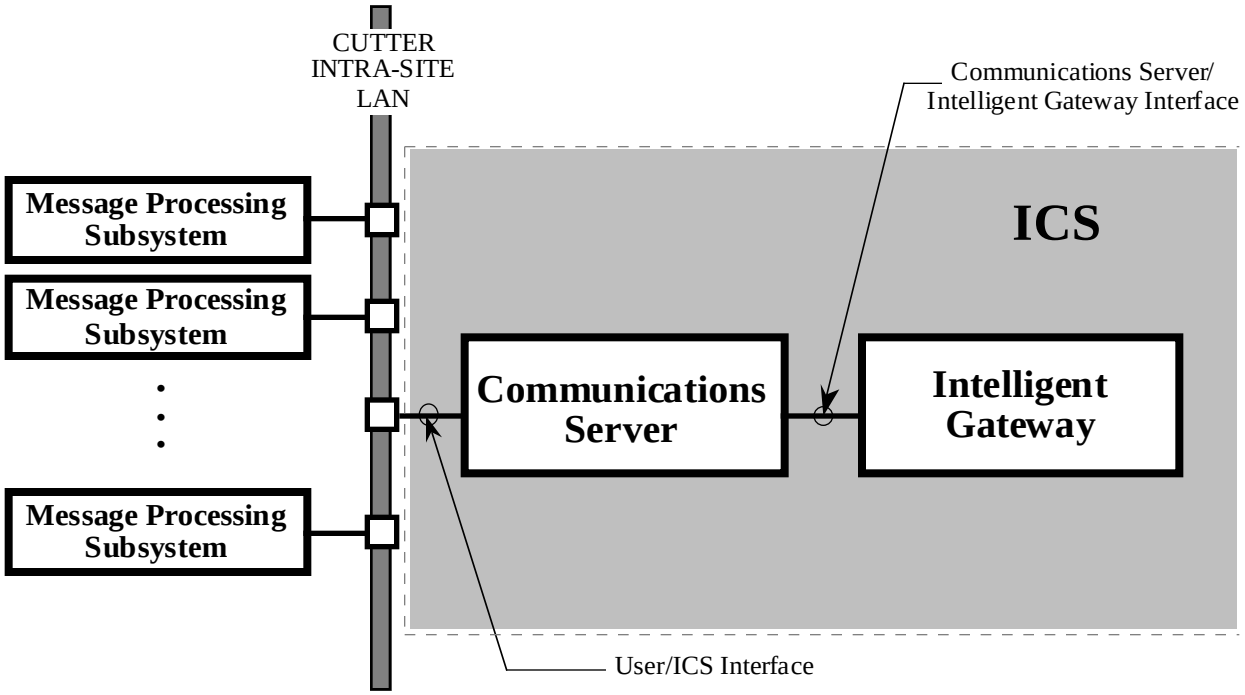


Figure 3.5-2 ICS Communications Server Interfaces

3.6 Integrated Radio Control

This study recommends that RF subsystems are implemented in accordance with an open system architecture. Standalone modems and radios for the next generation of WHECs and WMECs will become less acceptable due to size, weight, cost, and reliability penalties associated with separate enclosures, power supplies, logistics support, etc.. This study recommends that modems, receivers, exciters, and other communication elements be integrated with the RF elements on the ICS. RF modules are implemented in the standard VMEbus form-factor. These modules are housed in a double-compartment VMEbus chassis providing RED/BLACK separation as illustrated in figures 3.6-1 and 3.6-2.

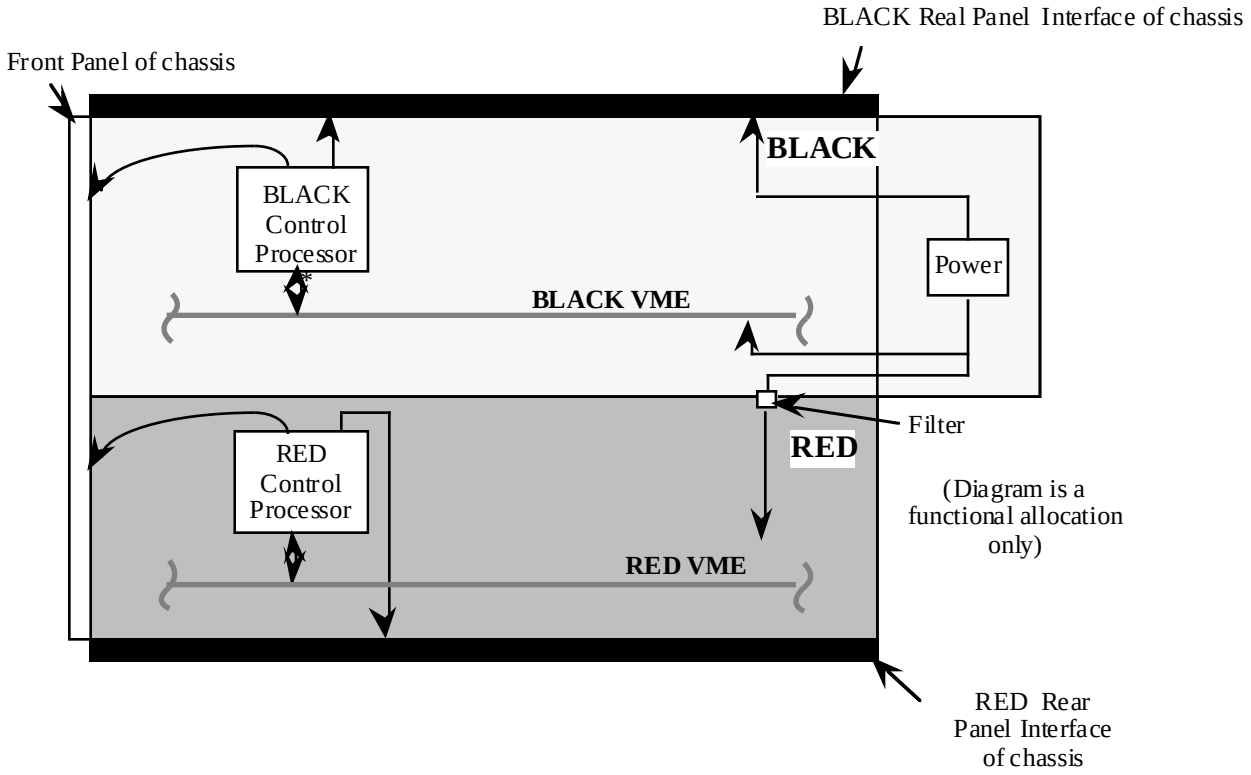


Figure 3.6-1 Chassis RED/BLACK Configuration

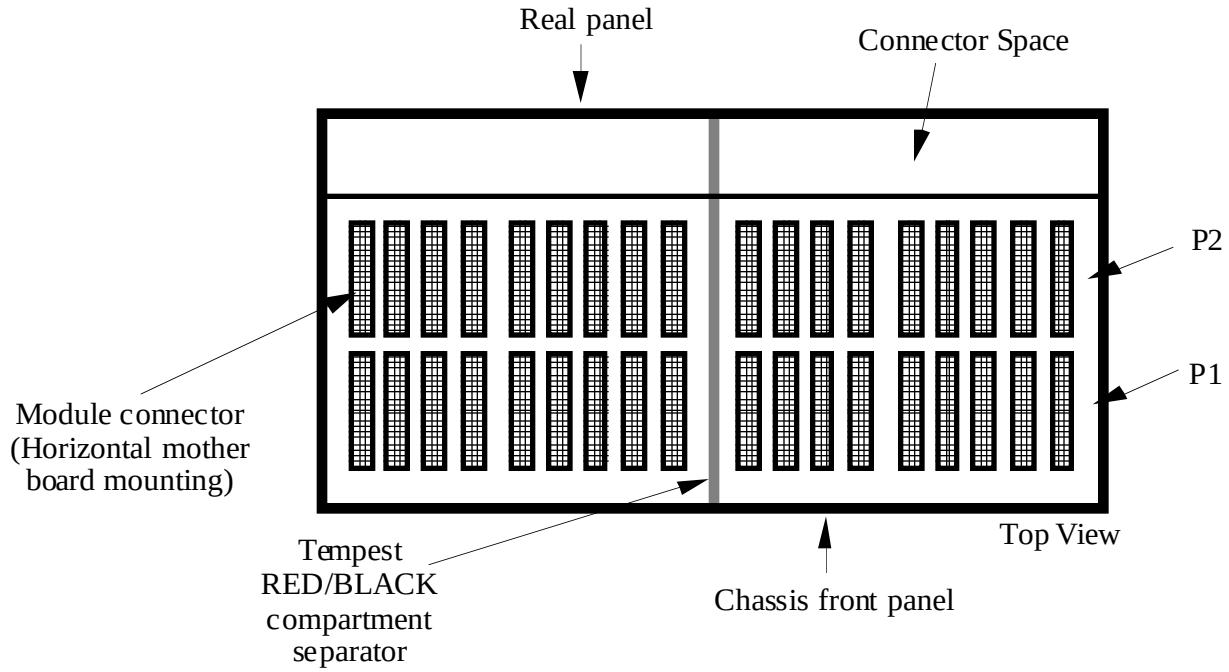
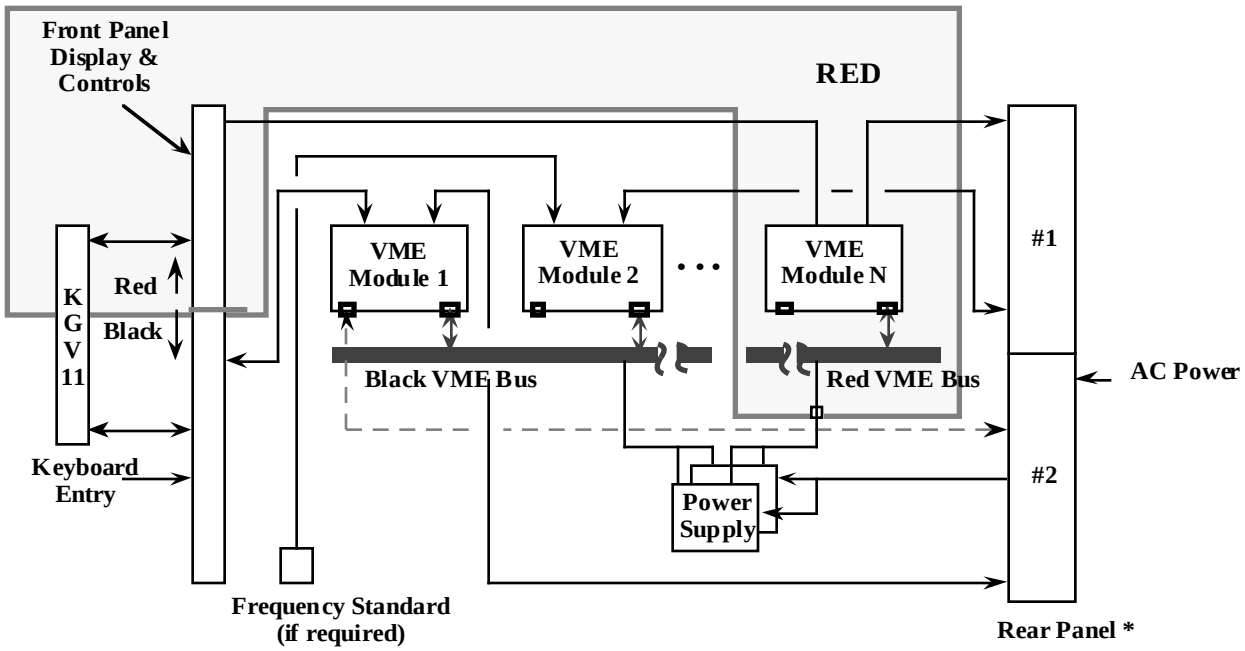


Figure 3.6-2 Chassis RED/BLACK Partition

When the multi-compartment chassis is combined with VMEbus-based Ultra High Frequency (UHF), High Frequency (HF), Very High Frequency (VHF) receiver/exciter functions, modem based functions and interface/control functions, they form the composite RF subsystem for the WHECs and WMECs. The RF communication capabilities provided by this integrated subsystem includes Line-of-Sight (LOS), extended Line-of-Sight (ELOS), and satellite communications (SATCOM).

The RED/BLACK chassis provides power, frequency standard (if required), front panel display, and external interface connections for the VMEbus based RF modules. This chassis housing also contains all emissions and spurious signals to prevent interfering radiation to/ from the enclosed modules. The chassis is designed in a configuration for rack mounting per EIA RS-310-C. Figure 3.6-3 illustrates the proposed chassis interface configuration



***Rear panel has two environmental panels, each supporting an independent set of configurable connectors**

Figure 3.6-3 Chassis Interfaces

The chassis is designed as a functionally configurable equipment having a multiple mode capability depending upon subsystems module set selection. Provisions are inherently provided within the chassis for each functional variation to support the different translations, receptions, transmissions, and processing requirements. Variations of each functional set are made possible by insertion or removal of VME modules which form the composite configuration. The operator interface with the chassis via a remote graphic display/input device provides for flexibility and procedural simplicity of operating the RF subsystem in each functional configuration and mode.

The chassis provides a minimum of two rear panel interface panels. Each panel provides a mounting plane for the various connector configurations. The interface panels mechanical mounting to the chassis provide an environmental seal insuring compliance to necessary environmental and emission requirements. RED or BLACK connections are mixed on the same rear panel interface. The rear panel interface connector panels are compatible with the following connector types:

a. Digital. Discrete multi-pin connectors complying with MIL-C-28840 or MIL-C 38999, or MIL-C-3124.

b. RF. Single source RF connectors compatible with coaxial cables.

c. Analog. Shielded connectors for analog baseband signals having a maximum spectral content of 25 MHz.

d. Fiber optics. Optical connectors (FC/PC) compatible with single (9/125) and multi-mode (50/125) cables.

The chassis supports both RED and BLACK interfaces with COMSEC equipment using rear or front panel data interfaces. The chassis uses interface circuitry on a removable board for the direct TSEC/KGV-11 and provides access to the RED KGV-11 side using the front panel RED-BLACK interface. The chassis is compatible with the embedding of COMSEC devices when contained on VME modules or cards. The COMSEC devices mounting and electrical interfaces are provided by the VME modules. The chassis also provides a front panel connection compatible with a key loading device. The front panel provides the following indicators:

a. Calibrated RF signal strength indicator.

b. Signal-acquired indicator when the demodulator(s) is acquired.

c. Carrier-on indicator to indicate when the exciter/receiver(s) is keyed.

d. Input alternating current (AC) power-on when the AC power on/off switch is in the on position.

e. Built-in test (BIT) alarm indicator when BIT circuits within the chassis indicate a failure.

f. Cryptographic alarm that is illuminated when the INFOSEL alarm circuits are activated.

The operator interface with the chassis is via a remote graphic display/input device.

The ICS operator possesses the capability to remotely control the operation of the modem, exciters, receivers, and power amplifiers. More than one operator graphic controller device at any given time can be utilized for this remote control. Furthermore, identical (functional) control capabilities are provided to the operator locally via the chassis front panel. Figure 3.6-4 depicts the interfaces between the RF subsystem chassis and the numerous possible controllers.

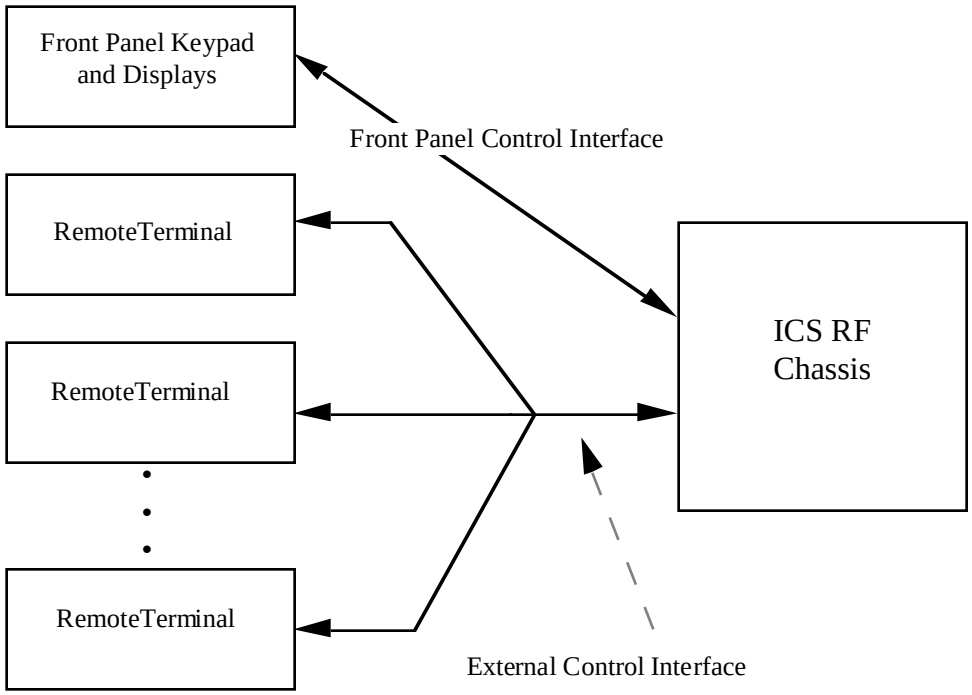


Figure 3.6-4 External Interface Diagram

The External Control Interface provides a reliable connection over which the remote controller(s) may perform initialization and remote control of the RF subsystem. The RF subsystem is defined to be the composite collection of those RF functions provided by a single RF chassis. Typical remote control functions include, but are not limited to, setting the initial and operational modes and control parameters of a modem, exciter/receiver, and power amplifier(s), providing the current settings to requesting controllers, and providing a mechanism for requesting diagnostic checks and accepting alerts regarding the operation of the RF subsystem.

Both the remote controller(s) and the front panel keypad/display (both hereafter referred to as "controllers") will operate in a concurrent manner with the RF subsystem. To resolve contention caused by multiple controllers attempting to simultaneously access control of the RF subsystem, the master-slave session management protocol illustrated in Figure 3.6-5 is proposed for the ICS. The following, in combination with the session management state diagram, provide full definition of the proposed session management protocol:

a. The RF subsystem assumes the role of slave.

b. Controllers assume a master role over a RF subsystem pending the outcome of the session management logic.

c. At initialization, none of the RF subsystems have an assigned master.

d. Regardless of the number of controllers which are logically connected to a particular RF subsystem, only one of these controllers is assigned as master of the subsystem at a time.

e. All controllers may request status information from their logically connected RF subsystem, but only the assigned master can perform control functions.

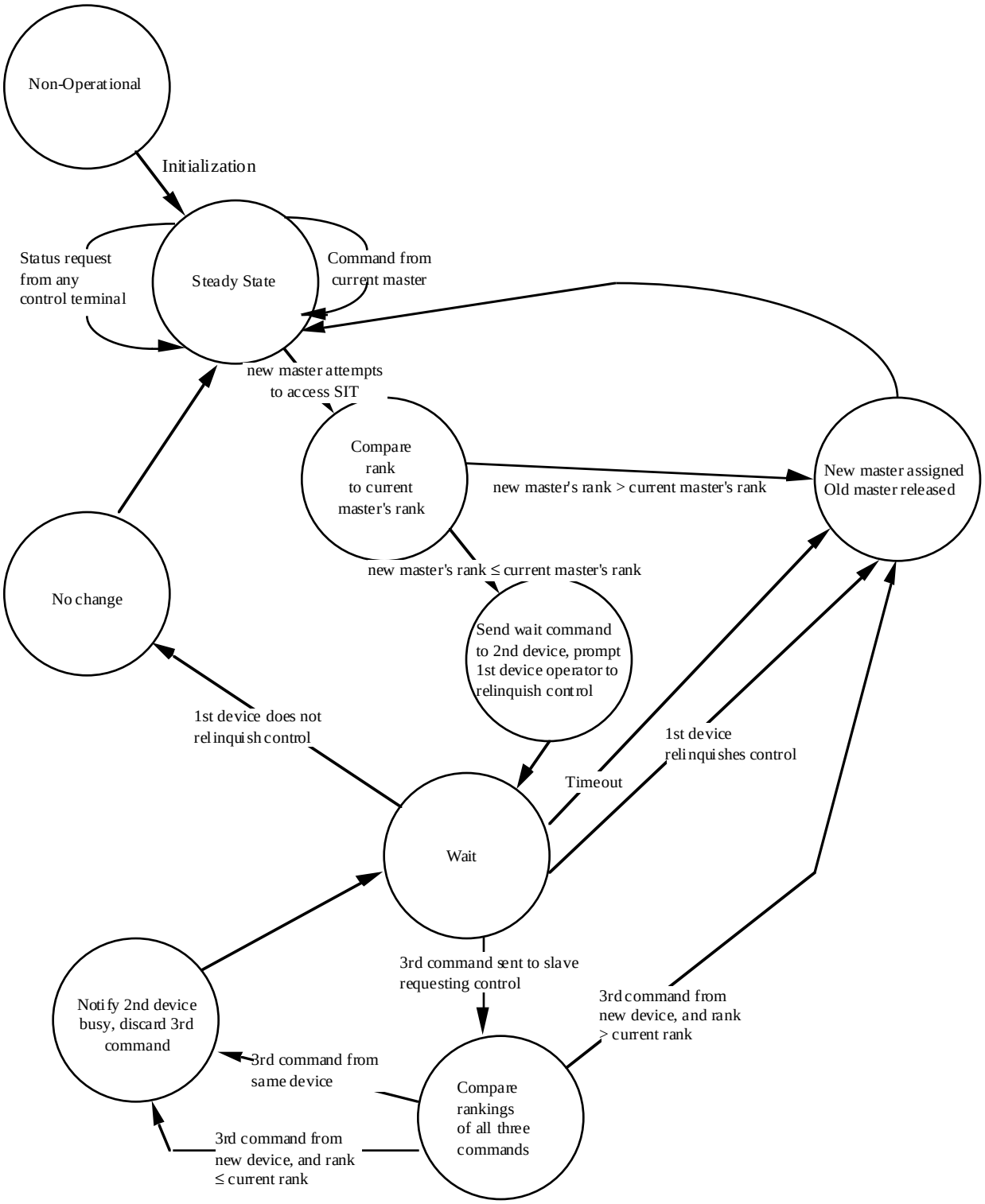


Figure 3.6-5 Session Management Logic

f. Contention among controllers for master status over a particular subsystem is resolved using a controller ranking scheme.

g. Failure on the part of a controller to respond to a request for release of control within a predetermined time-out results in an automatic transfer of control to the requesting controller.

The controllers interface to the RF subsystem(s) via a high speed LAN interface. The front panel keypad/displays interface to the RF subsystem via a serial interface. The sessions between controller(s) and the RF subsystem(s) are controlled by a ICS RF control session management protocol. The application level data elements passed between controller(s) and the RF subsystem are not dependent on the underlying physical connectivity. The communications protocols between the external controller(s) and the RF subsystem as well as the front panel keypad/display are illustrated in Figure 3.6-6.

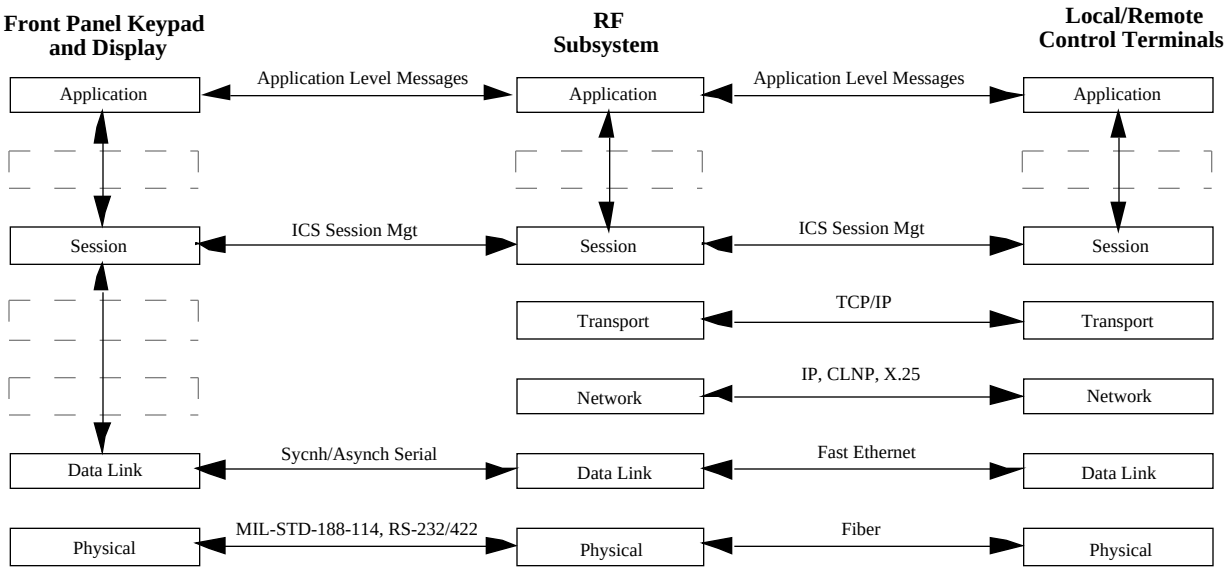


Figure 3.6-6 RF Control Protocol Architecture

For the ICS RF control architecture, one possible implementation consists of ten discrete messages types, as illustrated in Figure 3.6-7.

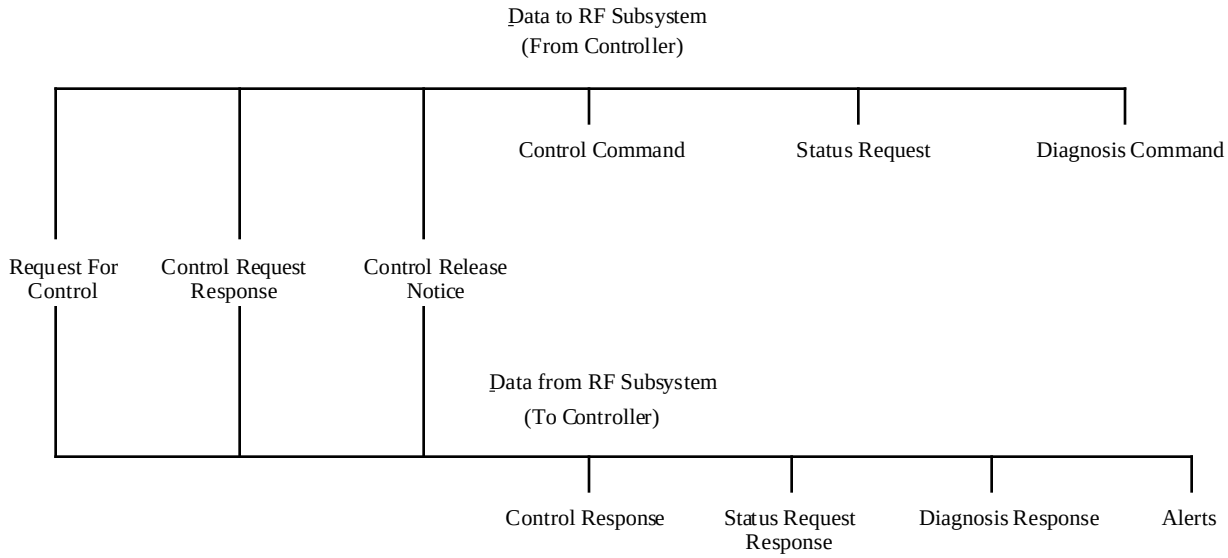


Figure 3.6-7 RF Control Messages

4.0 Physical Groups

This section addresses the progress to date regarding operational configurations and physical implementations for each physical architecture group. It presents conceptual solutions for implementing new equipment and for supporting transition issues and interoperability with existing equipment.

4.1 Antenna Group

The Antenna Group interfaces with the RF equipment and primarily includes the antenna, control assembly, bandpass amplifier-filter, and RF distribution assembly (e.g., cable assemblies, multicouplers, patch panels). There are a wide array of existing Antenna Groups located on surface ships, submarines, aircraft, and shore stations that will be used by the new systems implemented over the next several years.

4.1.1 Existing Equipment

The existing Antenna Groups operate in the following frequency bands: LF, MF, HF, UHF, and UHF SATCOM. Several of the Antenna Groups for these frequency bands are identified in Table 4.1.1-1. Each class of ship has different types of antennas and Table 4.1.1-1 does not attempt to separate antennas by class.

The Antenna Group is composed of a large number of different types of antenna depending on class and size of the cutter. These types are made up of whips, trussed whips, stub whips, fans, folded fans, blades, floating wires, log periodic, etc. Table 4.1.1-1 provides a selected group of antennas. The type of antenna selected is dependent on the particular frequency and transmitter or receiver to be used for transmission/reception. In general, antenna types and locations are a compromise between antenna requirements, other shipboard equipment requirements and mission capability requirements. Mission capability requirements include space limitations dictated by topside weight, etc.

An example of the previously mentioned types of interconnection components is found in Table 4.1.1-2. Table 4.1.1-2 provides a “system view” of antenna support components comprised of couplers controls, filters, and the like.

The UHF SATCOM antenna subassembly, OE-82/WSC-1, was designed primarily for shipboard installations to interface with the AN/WSC-3 (V) SATCOM transceiver. The complete installation consists of an antenna, bandpass amplifier-filter, switching unit, and antenna control. The antenna assembly is attached to a pedestal that permits it to be rotated through 360 degrees of azimuth and through elevations from near horizontal to approximately 20 degrees beyond zenith (elevation angles from +2 to +110 degrees). Frequency bands are 248–272 MHz for receive and 292–312 MHz for transmit. Polarization is right handed circular for both transmission and reception. This considerable subassembly total weight is about 443 pounds. Antenna group subassembly nomenclature, component sizes (inches), and weights (pounds) are given in Table 4.1.1-2.

Table 4.1.1-1 Existing Antenna Group

Antenna Type	Designation	Description
HF	CCEM-229A	Various HF Circuits
HF	CCEM-390-2	FM Voice Circuits
HF	Fan	5/16" Wire
HF	MLA-115	Mini-Loop
HF	MLA-1E	Mini-Loop
HF	MLA-2D	Mini-Loop
HF	MLA-324	Mini-Loop
HF	TD-C-338HS	Various HF Voice Circuits
HF	URC-116(V)	Various HF Voice Circuits
LF/MF	AT-924	Voice Circuits
LF/MF/HF	Long Wire	5/16" Wire
MF	AN/SRA-17B	Voice Circuits
MF	AN/SRA-17D	MF Voice Circuits
UHF	AS 390	UHF Voice Circuits
UHF	AS 3439	SATCOM Receiver
UHF	AT-150	UHF Voice Circuits
UHF SATCOM	OE-82C	Directional SATCOM
UHF SATCOM	SSR-1A	Omni Directional SATCOM
VHF	CCEM-396-1	VHF-FM Voice Circuits
VHF	D2216	VHF Voice Circuits
VHF	NT-66095	VHF Voice Circuits
VHF-UHF	CCXQ-CA-1128-3U/V	Various UHF Circuits

Table 4.1.1-2 OE-82C/WSC-1(V) Antenna Group

	HEIGHT	WIDTH	DEPTH	WEIGHT	SUBASSEMBLY
Antenna	54.5	54.0	27.4	294	AS-3018A/WSC-1(V)
Amplifier-Filter, bandpass	15.1	42.6	22.1	24	AM-6691A/WSC-1(V)
Switching Unit	22.1	24.5	14.6	107	SA-2000A/WSC-1(V)
Antenna Control	5.3	19.0	9.6	18	C-9597A/WSC-1(V)

4.1.2 Recommended Improvements

A specification tree for the Antenna Group is shown in Figure 4.1.2-1. As can be seen, the most effective structure was determined to be by subgroup; then by application; platform frequency band; and a break-out to existing and new elements.

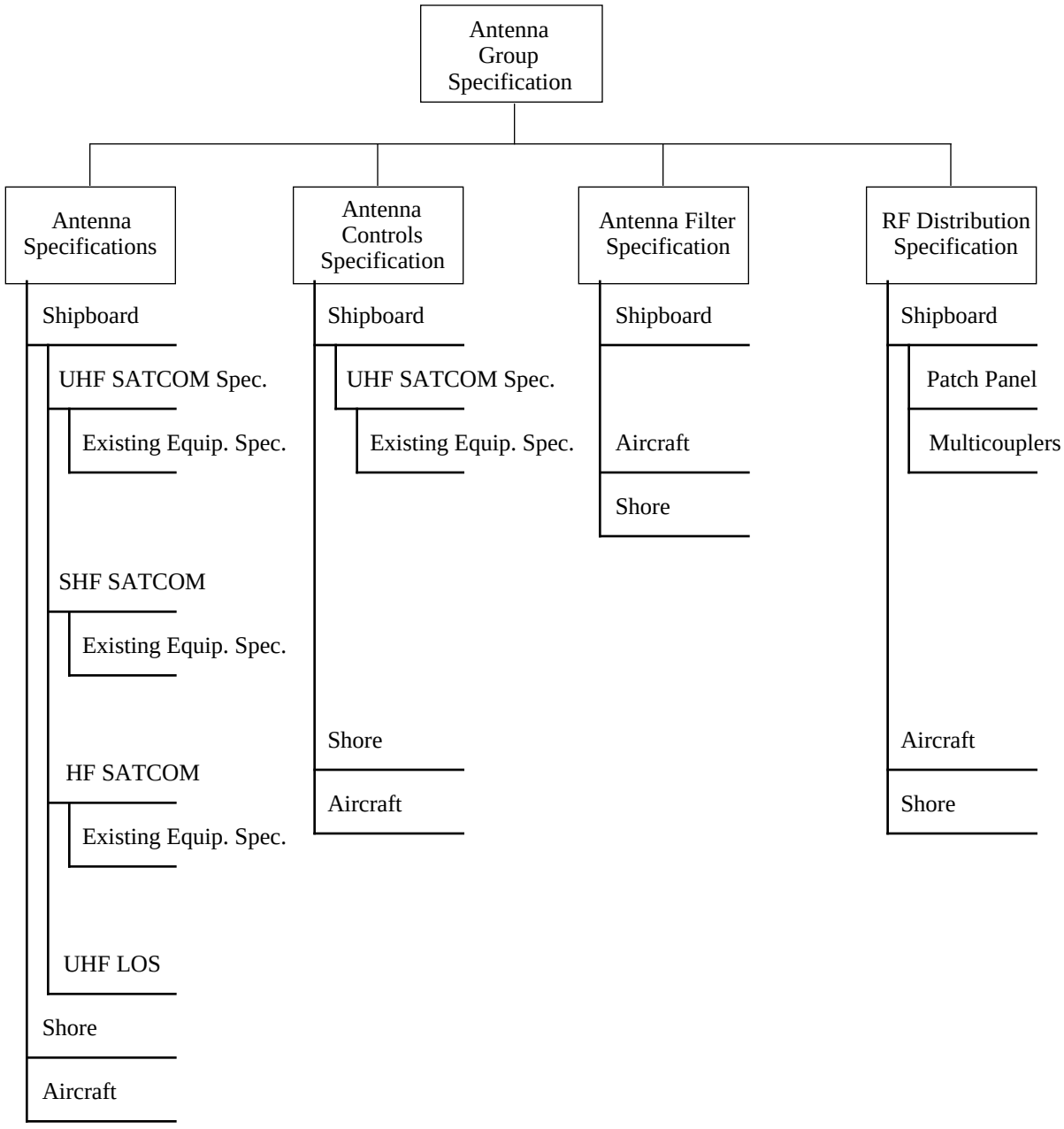


Figure 4.1.2-1 Lower Levels of Specification Tree for Antenna Group

The Coast Guard does not currently employ SHF SATCOM as part of cutter communications. This could potentially impact interoperability with the US Navy as the US Navy and other service components are moving toward SHF SATCOM for high data rate communications. SHF SATCOM will especially be used for the transmission of imagery products of interest to the USCG.

The size and weight of these antenna components presents a severe installation problem for most USCG platforms. It is important for the USCG to follow Navy efforts concerning compatibility with platform types similar to the WMEC/WHEC.

The US Navy SHF SATCOM antenna subassembly, AS-3399/WSC, a large microwave dish, is part of the OE-279/WSC-6(V) Antenna Group that provides continuous, automatic tracking of

the selected satellite. The WSC-6 system can simultaneously transmit and receive wideband, high rate, data or voice signals. The antenna unit consists of the reflector dish, feed structure, wave guide assembly, servo and drive system, vertical reference gyro, and a radome. The antenna is located in the radome which is 72 inches in diameter, 86.5 inches high and weighs 580 pounds. Since it is essential to maintain full hemispherical coverage, a pair of these SHF SATCOM antennas may be required on a ship. Installation of an additional large antenna could cause severe electromagnetic interference and radiation hazard problems.

Currently the primary problems with USCG shipboard communication antennas are caused by space limitations. In simple terms antenna designs are generally dictated by physical factors inherent to the signals the antenna is designed for. Simply building a bigger platform for improved antenna installation is not the answer. Optimum antenna design and installation is a complicated and expensive undertaking. Since the USCG desires to remain compatible with US Navy communications it would seem that following the appropriate ship class design would be a smart low risk alternative and cost effective.

USCG manning is however not tied to US Navy manning levels and a good place to cut manning requirements and training costs is to automate antenna switching and alignment equipment. The control for such automation would be performed by the System Distribution Group under direction of the Communications Services and System Controller Group as defined by the user inputs to the User Group.

Additional recommendations in this area would require study beyond the scope to this task.

4.2 Link Access/Radio Group

The LARG establishes the link and physical layers for the ISO modeled RF media architecture and therefore contains a majority of the more conventional radios, modem, and information exchange switch group (e.g., ON-143) processors. The LARG is the only communications subgroup besides the antenna which is dependent upon frequency bands. Consider Figure 4.2-1, the LARG is seen spanning the antenna input signals and transducing the emitted RF energy media or RFI to the electrical data or linear electrical signals. This figure identifies the frequency dependence of the LARG and the unique system implementation characteristics.

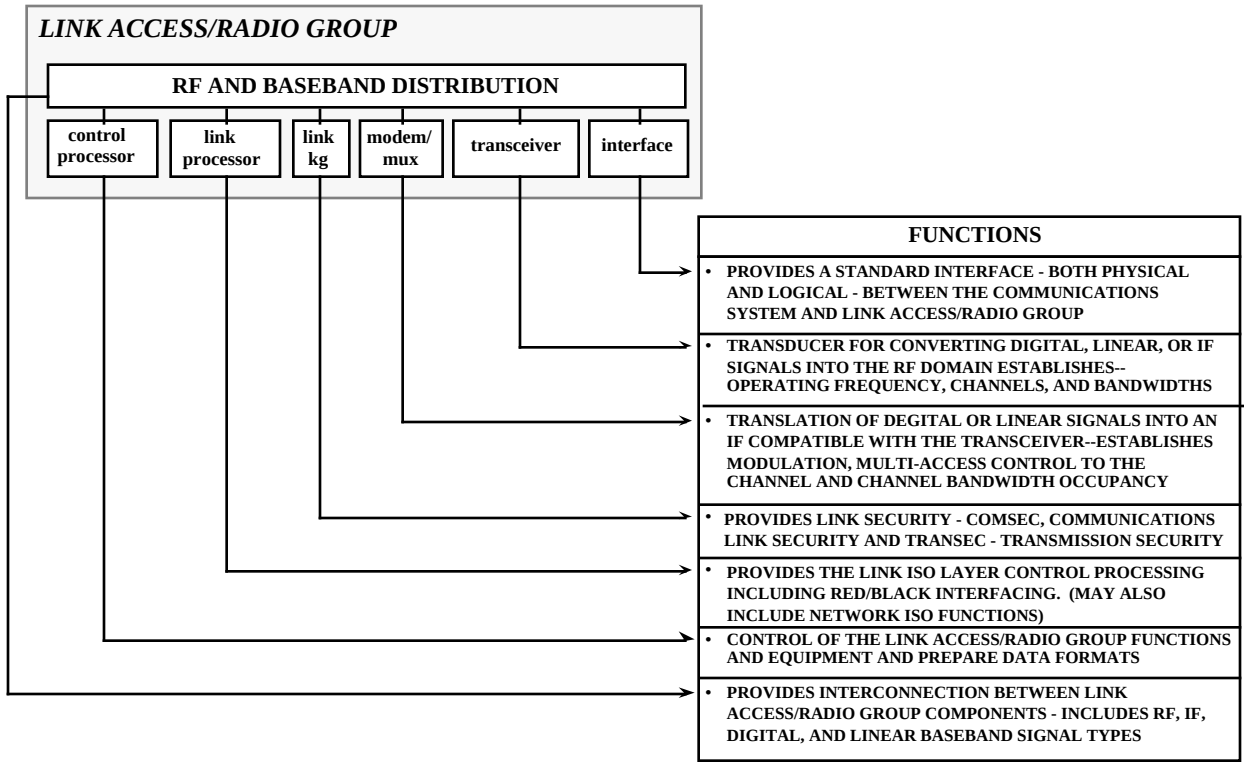


Figure 4.2-1 Functional characteristics of the LARG

4.2.1 Existing Equipment

Existing Link Access/Radio group elements are summarized in Table 4.2.1-1.

4.2.2 Recommended Improvements

The performance of the LARG is critical to the projected multimedia communications architecture since the first two ISO communication layers are performed in the LARG. The performance of the LARG is dependent upon several media characteristics: the propagational characteristics, required link margins, frequency increments, and media bandwidth constraints. Each of these constraints establish a operational availability for the LARG equipment to operate within. As an example, the propagational characteristics of a Line of Sight (LOS) communications path at the UHF frequency band does not have the same scintillation affects, bandwidth restrictions, interference criteria, of even signal level conditions as the UHF SATCOM link. Even more substantial comparisons are available between the HF and UHF media when considering the propagational characteristics and the detection requirements such as adaptive equalization.

A key requirement of the LARG is to transform and translate the digital and analog modulating signal into the RF or transmission medium. This translation involves the filtering, conversion, and modulation or demodulation of the signals. Essentially, the translation and detection of the signal represents the physical ISO layer. In addition, the LARG requires the implementation of the data link layer in the LARG.

Table 4.2.1-1 Existing Link Access/Radio Group

Designation	Description	Frequency	210'	270'	378'
AN/CRT-3B	Emergency Transceiver	HF	X		
AM-6534/SSR1	Amplifier/Converter	UHF		X	X
AM-6691A/WSC-1(V)	Amplifier/Bypass	UHF		X	X
AM-7255/URR	Amplifier	HF		X	
AN/GRC-211	Transceiver	VHF		X	
AN/GRR-24	Guard Receiver	UHF	X		X
AN/SRA-12	Filter	HF	X		
AN/SSR-1	Receiver	UHF		X	X
AN/URC-114(V)	Transceiver	HF		X	
AN/URC-116(V)3	GSB-900 Transceiver	HF	X		X
C-11485/URC-114(V)	Receiver/Exciter	HF		X	
CDFL-MDT-1/OA	Mini-Loop Tuner	HF	X	X	X
CDIE-GSE-924	Exciter	HF	X		X
CDQC-SR-840	Code Keyer	MF	X	X	X
CEDJ-5003C	Receiver	MF		X	
CEJD-MSR-1020	Amplifier	HF	X		X
CEJD-MSR-6212	Power Supply	HF	X		X
CEPZ-VHF-7002	Transceiver	VHF	X		
CFEO-985-1008-001	Receiver	UHF	X		
CFEO-985-1009-001	Receiver	UHF	X		
CGG-AM-7175/URC	Amplifier	-	X		
CGG-LST-5C	Transceiver	UHF	X		
CGG-MCX-1000-RT	Transceiver	VHF	X	X	X
CGG-MCX-300RH	Transceiver	VHF	X	X	X
CGG-V2025A-13CH	Receiver	VHF	X	X	X
CGG-V2025A-16CH	Receiver	VHF	X	X	X
CV-1920A(P)/UCC-1C(V)	Converter	HF		X	X
CV-2460/SGC	Converter	UHF	X		X
CV-3883/UG	Modem	HF	X	X	X
MD-900/SSR-1	Combiner/Demodulator	UHF		X	X
MSR-6700/T3	Exciter	HF			X
R-2368/URR	Receiver	HF	X	X	X
RT-1107/WSC-3(V)17	DAMA Transceiver	UHF		X	X
RT-1107/WSC-3(V)3	LOS Transceiver	UHF	X	X	X
RT-1107/WSC-3(V)6	SATCOM Transceiver	UHF		X	X
RT-1479/URC-114(V)	Transceiver	HF		X	
RT-1495(P)/URC-116	Transceiver	HF	X		
T-1505/SRT-29	Transmitter	MF		X	X
TD-1063/SSR-1	Demultiplexer	UHF		X	X
TD-1271	DAMA Multiplexer	UHF		X	X
TN-539/SRA-17	Tuner	MF		X	
TSEC-KG-36	Crypto	-		X	X
TSEC-KG-84A	Crypto	-	X	X	X
TSEC-KG-84C	Crypto	-	X	X	X
TSEC-KWR-46	Crypto	-	X	X	X
TSEC-KYV-5	Crypto	-	X	X	X
TSEC-KY-58	Crypto	-	X	X	X
TSEC-KY-75	Crypto	-	X	X	X

The LARG subgroup requires link access processing and especially the Media Access Communications (MAC) within the data link layer. The MAC ISO sub-layer provides access to various media by using either a TDMA, DAMA, or CSMA type of data link layer implementation. A primary example of the MAC layer is the UHF DAMA waveform and system architecture. The processing of this MAC information is normally conducted within modem/MUX units such as the MACS modem. Unfortunately, a limitation in orderwire (OW) control and system lead propagation exists.

The functional allocation of the LARG is summarized in Figure 4.2-2.

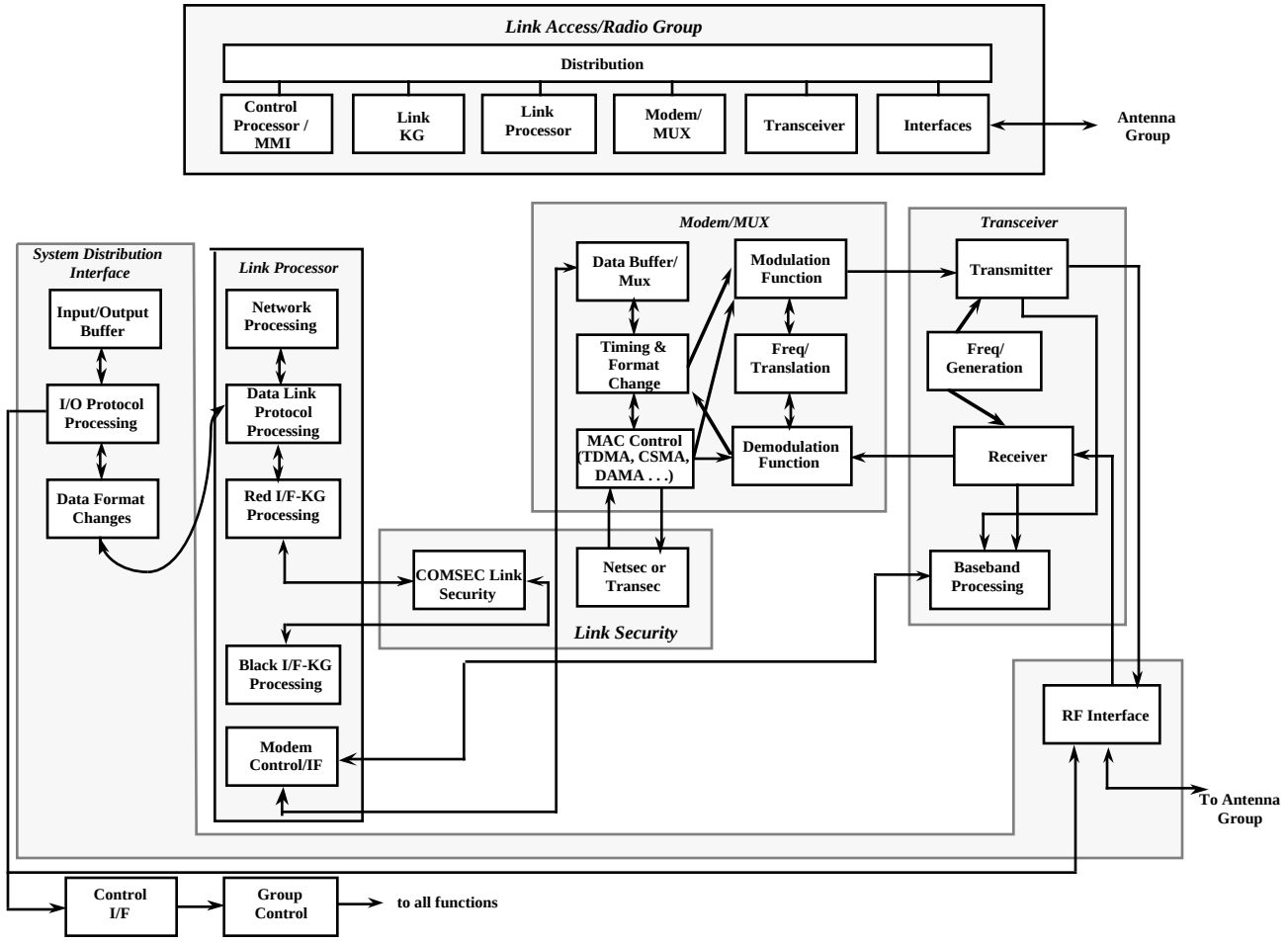


Figure 4.2-2 Link Access/Radio Group Functional

There is a significant question of supply support and repair of existing UHF transceivers. The US Navy is moving UHF communications toward an open system architecture with the WSC-3(V)XX program. The program business plan, approved in April 1995, outlines a phased approach to migrate from current systems to open systems.

The AN/USC-54(V) VME Integrated Communications System (VICS) is another example of open system efforts in UHF initiatives. In brief the VICS can support multiple channels of UHF SATCOM (DAMA and non DAMA) and LOS communications in an open system supporting OTCIXS, TADIXS A, TADIXS B (TRE) networks.

The Link -11 (TADIL-A) capability is found on some USCG WHEC cutters but was not a target for study. The addition of Link-11 to all USCG Cutters for high speed transfer of perishable data and US Navy interoperability would be a definite asset. VME based (Open system) Link-11 processors are available to enhance overall capability. Open system architecture makes the introduction of such enhancements feasible and not cost prohibitive.

Existing communications system installation in regards to "Link Access" are point-to-point, closely coupled, via switchboards, patch panels and system components designed for interconnection. These components are listed in the "Current Capabilities and Work Flow Analysis Report" and are not repeated here. However, an open system must employ methods to interconnect various components within the OSI parameters. Existing interconnects do not lend themselves to upgrade or redesign towards that end. Wholesale replacement may be cost prohibitive but incremental modernization to OSI standards is quite plausible. Incremental changes may not immediately impact manning or training but the goal system definitely would reduce both requirements considerably. The translation from the present equipment architecture to a new future architecture is dependent on several key architectural design parameters: the future channel allocations, the type of communication platform, and the implementation time. The future channel allocations are important since these determine the numbers of equipment and the overall interconnection of the equipment. The type of communications platforms is critical since the implementation of communications equipment is extremely dependent on the size, physical location of the equipment, and the different interfacing characteristics of the equipment. The final consideration involves the implementation time or the time from present equipment to the final or intermediate implementations times. The number of channels and the allocation of these channels determines the operational environment and the ultimate configuration in the RF implementation. The architectural constraint placed by the channel numbers involves the independent transceivers, modems and link processors required to support the communication needs. Figure 4.2.2-1 illustrates the recommended cutter configuration for the late 1990's timeframe.

The architectural implementation and recommended configuration is dependent on the security aspects within the LARG subgroup. There are basically two types of security concerns within the LARG, the Link COMSEC and the Link TRANSEC or NETSEC. The TRANSEC and NETSEC are security constraints placed on the transmission of the communications system, specifically order wire (OW), or the network security. Both the TRANSEC and the NETSEC are associated with the transmission protocol control rather than the actual security of the data or information portion of the transmission. The physical architectural allocation is the most critical configurational implementation aspect of the LARG group design. In particular, the allocation of the various LARG elements within the platform types is an extremely important variable in the physical structure and configuration of the system. It is important to recognize the importance that security and location constraints place not only on the physical make up of the equipment, but also on flexibility and the limitations placed on the data transferred.

4.3 Communications Services Group

The Communications Services Group (CSG) provides the networking protocols and interfaces between users and the real radio equipment (Link Access/Radio Group). CSG functionality includes:

a. Provide standard interface to User Systems

b. Select communication resources for Transmission of Data

c. Execute protocols - ISO communications subnet level protocols

4.3.1 Existing Equipment

Existing Communication Services Group elements are summarized in Table 4.3.1-1.

Table 4.3.1-1 Existing Communications Services Group

Designation	Description	210'	270'	378'
ON-143(V)8	NAVMACS		X	X
AN/USC-43(V)	ANDVT	X	X	X
ON-143(V)6 or VIGC	OTCIXS		X	X
CMX-MX-2400	INMARSAT	X	X	X
AN/SSR-1	Receiving Set		X	X
AN/URC-116(V)3	GSB-900	X		X
CV-3333/UG	Vocoder		X	X

4.3.2 Recommended Improvements

To perform the functions defined for the CSG (Section 4.3 a through c) within the context of the new technologies becoming available, additional component and interface requirements need to be defined. Utilization of various combinations of the components and interfaces, listed below, are required to perform CSG functions.

a. System Distribution Interfaces

b. Peripheral Components

c. Processing Component - Resource Access

d. Processing Component - User Interface

e. CSG Distribution Component

f. CSG Chassis Component

The Communications Services Group, System Control Group, and the User Group each will consist of specific application software tailored to the mission of that group, generic software such as operating systems, interface drivers, and data base packages, etc. that apply to all of these groups, and hardware platforms. Without consideration of intergroup packaging described in the System Distribution Group there are three major mechanisms for deploying the software:

a. Unix-based workstations (primarily the Navy based TAC-3 and TAC-4)

b. PC-based workstations

c. Bus-based single board computers (primarily the SPAWAR VME architecture)

Solutions can be provided which focus on a single homogeneous packaging technique or with a heterogeneous technique which uses all of the processing environments listed above. It is important to note that the top level architecture is not affected by the choice of packaging for each individual segment. The rationale for performing trade-off amongst these approaches includes:

a. Cost (Development, Integration, Test, Installation, communications operations (including equipment maintenance and repair and any channel costs).

b. Performance

c. Navy compatibility

d. Navy commonality

e. Software availability

f. Technological Tolerance (flexibility)

g. Schedule

The PC workstation approach (e.g., Standard Coast Guard Workstation) provides for a single processor controlled system. The generic advantages of using a PC include:

a. Low cost production. The mass production of PCs make this equipment the least expensive on a per box basis.

b. Commercial Software Availability. The PC has access to a wide range of standard word processing, spreadsheet, CAD/CAM, and data base programs which are sold much less expensively then their UNIX workstation counterparts.

c. Navy commonality. The wide variety of PCs used within the Navy, all of DoD, and other Government agencies provide a solid base of life cycle support. On the other hand, the configurations are so varied as to make it a maze. If the Coast Guard decides to implement the Navy message processing system, the fact that the Navy uses PCs for many of their message processing needs, makes this more important in the User Group area.

The generic disadvantages to the PC approach include:

a. Growth Potential. The PC is inherently limited in performance and growth because of the single processor limitation (with the exception of the evolving PCI bus which is limited to 4 slots). The newer PCs which have a standard bus and the PCI bus offer a limited hybrid configuration similar to the TAC-4 configurations.

b. The Navy SPAWAR standard operating environments (UNIX, X, VxWorks real-time OS, etc.) do not port easily to the PC world. Most of the Navy Software is not written for the PC (with the exception of some message processing software).

c. PC configurations often provide the smallest foot print in single user environments and the largest footprints in multiple user and multiple application environments.

In general, the PC provides the ideal host for a single user installation with a small number of applications. This is not the case with the Communications Services Group.

The Unix-based TAC-3/4 systems consist of a dedicated work station and an extension to a VME based chassis which can be utilized to host additional processing functions or additional I/O interfaces. Thus, the TAC approach inherently is a hybrid approach which uses multiple packaging technologies. Hardware implementation in a primarily VME approach consisting of standard COTS component integration is recommended for CSG modernization. To begin the process of modernizing the USCG cutter communications architecture, it is necessary to maximize the use of existing off-the-shelf technology and technology support equipment. The VMEbus is recommended to provide the initial installations of the USCG backplane components. As discussed previously, the VME approach provides greater flexibility and resistance to technological obsolescence, but there is no need to implement the graphics workstation in the VME configuration as this is easily satisfied by the TAC-4.

Figure 4.3.2-1 provides a detailed hardware block diagram for the modernized CSG. 6U and 9U component sizes are indicated by physical module representations (2 VMEbus connectors and 3 VMEbus connectors, respectively). The mechanical and electrical specifications for the so-called 220 mm high 6U module is addressed by the IEEE STD 1014-1987. The mechanical aspects of the 220 mm high 9U VME module is also defined by ANSI/IEEE STD 1101-1987. The ICS 9U module will maintain the same VMEbus electrical specifications as the standard 6U module.

As is shown in the figure, application environments may dictate that components may be located in one chassis communicating over VME or FUTUREBUS+ or in separate chassis communicating over the System Distribution Group LAN. Similarly, these cards can be identified as components of a TAC-4 work station and included in that packaging with VME used only for additional processors and I/O.

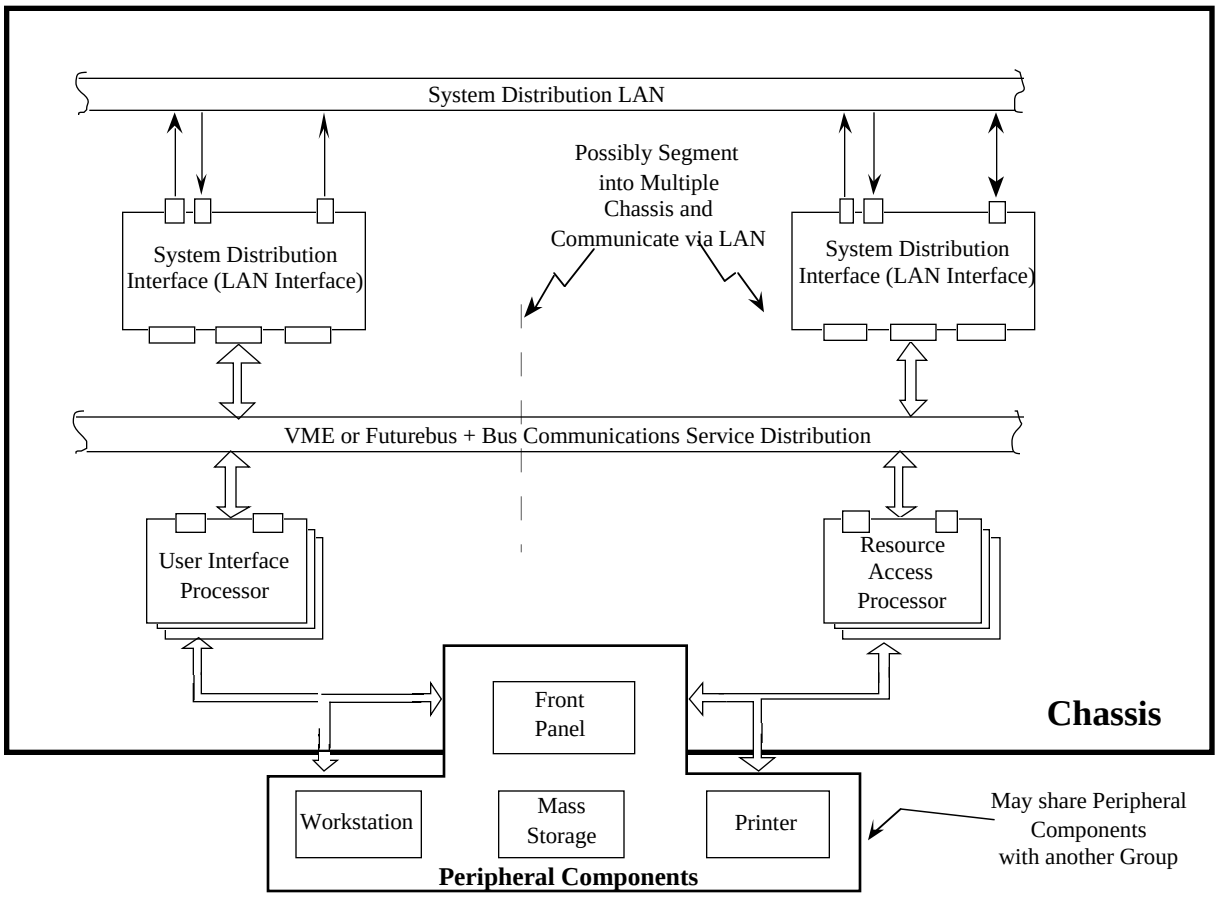


Figure 4.3.2-1 CSG Recommended Hardware Block Diagram

This configuration provides the lowest cost capability with the most commonality with the Navy systems and the greatest degree of flexibility to install future technology enhancements. Specifically, the Navy has established the TAC-4 as the standard desktop computer. The TAC-4 can be interfaced to the VME chassis via a bus extender or via Ethernet. The modularity provided with the VME allows the USCG to purchase the amount of processing power needed to solve its problems. It does not have to buy the largest Navy configurations, but can utilize the architecture in small configurations. The Navy communications software will be compatible with TCP/IP communications and that software is readily available to the Coast Guard from the Navy and several vendors. As the Navy increases capability, the USCG can increase capability via the

addition of new VME-based technology. This approach also permits rapid development and integration for the USCG as most of the components are off-the-shelf. This approach also permits shared use with other system segments to provide smaller footprint systems.

4.3.2.1 System Distribution Interface Components and Interfaces

The system distribution interface will be a VME card which interfaces to the LAN selected for system distribution.

4.3.2.2 Peripheral Components

The peripheral components consist of those devices necessary for the CSG to store and retrieve data, input system control parameters, and provide status monitoring and reporting information. The peripheral devices specified for the CSG are the same peripherals specified for the System Control Group and the User Group. Certainly, future user systems could employ the same peripherals. As discussed above the TAC-4 system provides most if not all of this capability. In the SCG section, all of the remaining peripherals will be described. The requirements for a Front Panel by the CSG are limited to only control and monitoring of BITE functions and power on/off selection and indication. In most cases the remaining peripherals will be shared with the SCG, as described in that section.

4.3.2.3 Resource Access/User Interface Processing Elements

The number of processors required to achieve all the CSG processing functions aboard an individual cutter will vary dependent upon the number of interfaces and communications resources aboard that cutter. In the future more powerful processors may be available and may be used to host these functions without disruption of existing interfaces or rewriting of CSG hosted software. Specifications for this processor and many of the processors used for Systems Control and the User could be common elements to reduce life cycle costs. These single board computers will contain a state-of-the-art processor, 256 megabytes of memory, serial I/O channels, and Ethernet access.

4.3.2.4 CSG Distribution Component

The CSG Distribution Component will consist of VME backplane bus technology, Ethernet local area network technology, patch panels and discrete connections as required.

4.3.2.5 CSG Chassis Component

Each USCG platform has different requirements in terms of size, weight and environmental protection. In the large shipboard environment, flexibility and modularity become overwhelming considerations while in the smaller craft space and weight are the packaging drivers. Ashore, prevention of unauthorized emissions via TEMPEST is of greater concern than it is aboard afloat platforms. The application of OSA principals provides the technique for developing standard equipment which can provide low cost implementation in many different environments. On many platforms two or more chassis may be required to fulfill the CSG requirements.

4.4 System Control Group

The System Control Group (SCG) provides the system wide control mechanisms necessary to tailor communications operations to the specific platform environment. SCG functionality includes:

a. System Site Initialization

b. System Site Configuration

c. System Site Performance Monitoring

d. System Site Fault Detection and Recovery

e. Intersite control information exchange

f. Site Data Base Control and Maintenance

4.4.1 Existing Equipment

Existing System Control Group elements are summarized in Table 4.4.1-1.

Table 4.4.1-1 Existing System Control Group

Designation	Description	210'	270'	378'
None	Coast Guard Standard Workstation	X	X	X
None	Master Standard Telecommunication System	X	X	X
ON-143(V)8	NAVMACS		X	X
AN/USC-43(V)	ANDVT	X	X	X
ON-143(V)6 or VIGC	OTCIXS		X	X
CMX-MX-2400	INMARSAT	X	X	X
C-10315/U	Remote Control	X		
C-10316/F	Interface Control	X		
C-11610(P)/URC-116(V)	Remote Control	X		
C-11612(P)/URC-116(V)	Coupler Control	X		
C-11828/U	TSEC Control	X	X	X
C-8839	Antenna Control		X	
C-9351/WSC-3(V)	Remote Control (UHF)	X	X	
C-9579-A/WSC	Antenna Control		X	X
OK-454	DAMA Control		X	X
SA-2000A/WSC-1	Switching Unit (antenna control)		X	X

4.4.2 Recommended Improvements

To perform the functions defined for the SCG (Section 4.4 a through f) within the context of the new technologies becoming available, additional component and interface requirements need to be defined. Utilization of various combinations of the components and interfaces, listed below, are required to perform SCG functions.

a. System Distribution Interfaces

b. Peripheral Components

c. System Control Processing Component

d. System Control Security Component

e. System Control Group Distribution Component

f. System Control Group Chassis Component These elements are the components of the recommended specification tree for the System Control Group. As previously discussed, the System Control Processor component is an embedded processor in some application, while in others it is integral to the workstation within the Peripheral Component.

4.4.2.1 System Distribution Interfaces

The system distribution interface will be a VME card which interfaces to the LAN selected for system distribution.

4.4.2.2 Peripheral Components

The peripheral components consist of those devices necessary for the SCG to store and retrieve data, input system control parameters, and provide status monitoring and reporting information. The peripheral devices specified for the SCG are the same peripherals specified for the Communications Services Group and the User Group. Certainly, future user systems could employ the same peripherals.

4.4.2.2.1 Workstation

The workstation provides an integrated operator interface to the various physical groups of the cutter's Integrated Communications System (ICS). The workstation is implemented via a keyboard, trackball and display via the X-Window GUI standard. It is an intelligent device in that it contains the processing and memory necessary to execute the protocol standard. The ICS Program Manager can select among various options for display screen size, color, and environmental considerations. Typically, the Program Manager would the select a Workstation for the SCG and, in most cases, would select one or more X-Windows based GUI workstations for implementing the operator interface with the CSG.

The workstation will also be available in a package which also provides the chassis, the System Control Processor, the System Distribution Interfaces, and SCG distribution components (VME backplane). This will provide a single package for integration of the SCG functions and may also host user applications.

4.4.2.2.2 Printer

The printer provides hard copy output of reports generated by the SCG. The Program Manager must select from among different printers offering variations in speed, print quality and environmental protection. As with the workstation, a dedicated printer for the SCG is not likely, but depends on the specific application.

4.4.2.2.3 Front Panel

The front panel requirements for the SCG are minimal and include power on/off, reset, and diagnostic indicators for BIT/BITE.

4.4.2.2.4 Mass Storage

Several mass storage devices will be available for selection by the Program Manager. The SCG requires mass storage to queue data for output to the LARG and the user. The mass storage device is one of the primary mechanisms the user will use for flow control. Different devices provide for short term transportable storage, long-term archival storage, and rapid access storage.

As discussed in section 4.3 these components can be satisfied by integration in a VME chassis or by the use of the TAC-4. Because commonality with the Navy is so significant in terms of purchasing power, software and life cycle support, it is recommended that the TAC-4 be used in conjunction with a standalone printer to satisfy the peripheral component requirements.

4.4.2.3 System Control Processing

Aboard larger platforms this may be the processor associated with the workstation. In more integrated installations, the processor will be an embedded processor such as that associated with the CSG Processing components.

4.4.2.4 Security

One of the paramount issues in the modernization of USCG cutter communications within the ICA architectural framework is the ability to share expensive peripheral components such as workstations and mass storage devices. The availability of secure LAN technology already permits data of various classifications to be stored on the same physical mass storage device. This multi-level secure technology is approved up to the B2 level. Certification for a B2 level O/S for the workstation environment is expected within the next year.

4.4.2.5 SCG Distribution Component

The SCG distribution component will consist of backplane bus technology, Ethernet local area network technology, patch panels and discrete connections as required. The SCG component is identical to the CSG distribution component.

4.4.2.6 SCG Chassis Component

As previously discussed, the USCG equipment will be placed ashore, in ship, and aircraft platforms. Each of these platforms have different requirements in terms of size, weight and environmental protection. In the shipboard environment, flexibility and modularity become overwhelming considerations while in the aircraft space and weight are the packaging drivers. Ashore prevention of unauthorized emissions via TEMPEST is of greater concern than it is afloat. The application of OSA principals provides the technique for developing standard equipment which can provide low cost implementation in many different environments.

On larger platforms and ashore the SCG will normally be packaged within the TAC-4 workstation as discussed above. In aircraft or smaller platforms a more integrated approach where the SCG is located in the same chassis with the CSG and LARG will be required.

4.5 User Group

The User Group provides the gateway between the users and the communications networks. User Group Functionality includes:

a. Translating unique user interfaces to standard ICS interfaces

b. Translation of user oriented addresses to ICS addresses

c. Data compression, filtering, duplicate search, character conversion and data formatting as required

d. Routing between local users

e. COMSEC

f. Flow Control between users

In addition, the User Group provides the functions of message generation, format verification, editing, local message distribution, and hardcopy generation. The User Group is representative of all users except that it has specific functions associated with formatted communications. There will be additional users such as JMCIS associated for which the User Group provides communications access.

The most difficult problem associated with this group is the wide variety of systems that are already available, yet are architecturally vague. For example, even the new NAVMACS Model II performs a subset of the functions of the CSG, SCG, and the User Group. It is not just a simple matter of applying an interface application, but an architectural issue.

4.5.1 Existing Equipment

Existing User Group elements are summarized in Table 4.5.1-1.

Table 4.5.1-1 Existing User Group

Designation	Description	210'	270'	378'
ON-143(V)8	NAVMACS		X	X
AN/USC-43(V)	ANDVT	X	X	X
ON-143(V)6 or VIGC	OTCIXS		X	X
CMX-MX-2400	INMARSAT	X	X	X
AN/SSR-1	Receiving Set		X	X
AN/URC-116(V)3	GSB-900	X		X
CV-3333/UG	Vocoder		X	X

4.5.2 Recommended Improvements

To perform the functions defined for the User Group (section 4.5 a through f) within the context of the new technologies becoming available, additional component and interface requirements will need to be defined. Component and interface elements of the recommended specification tree follow:

a. Unique user Interface Components and Interfaces

b. System Distribution Interface Components and Interfaces

c. Peripheral Components

d. User Security Component

e. User Processing Component

f. User Distribution Component

g User Chassis Component

4.5.2.1 Unique User Interface Components and Interfaces

The specifications for the interfaces to the user devices or systems will be unique for each user attached to each user. As these systems were developed without any consideration of open system architecture or ISO layered protocol structures, there is no model interface. Thus, the set

of possible interfaces is divided into a pseudo-layered architecture for discussion purposes. These layers will be referred to as the physical layer and the "hand shake" layer. In most instances the selection of a physical layer is made from the following list:

a. MIL-STD-188-114 (balanced and unbalanced)

b. MIL-STD-1397 (A, B, C, D, E)

c. Ethernet

d. MIL-STD-1553B

e. RS-232C

f. RS-422

The hand shake protocol applied to these physical interfaces varies with the user system and is indeed unique to the user system except for the few instances where TCP/IP is utilized for connectivity in a LAN environment (CDFTT and NCCS-A). Even the higher protocol layers associated with MIL-STD-1553 vary in most installations even, for example, in the same aircraft. It is this extensive set of non-standard interfaces which creates the need for this function of the User Group. The physical implementation of these unique interfaces within the User Group will be accomplished via execution of interface protocols by the User Processing component and by specific interface components which adapt to the physical standards and which may also execute portions of the protocols.

The major issue within the interface area involves the need to apply standard ISO interface methodology to the user-user interfaces. Certainly, adaptation of new standards by the existing user systems is costly and unlikely. If in the future, new user systems adopt these standards, then there will be a reduction in the need for unnecessary interface translation processing.

4.5.2.2 User and System Distribution Component Interfaces

The system distribution interface will be a VME card which interfaces to the LAN selected for system distribution.

4.5.2.3 Peripheral Components

The peripheral components consist of those devices necessary for the User Group to store and retrieve data, input system control parameters, and provide status monitoring and reporting information. The peripheral devices specified for the User Group are the same peripherals specified for the System Control Group and the Communications Services Group.

4.5.2.4 User Security Component

The User Security Component provides security protection for all data leaving the User Group destined for any other Group with the exception of the User Group. It also receives protected data and removes security protection for output to the User Group. The User Group may provide additional Security protection for selected compartments of information.

This architecture is necessary to maintain compatibility with future Navy systems being developed as part of Copernicus. The primary issues involved in implementation of the User Security Component involve:

a. Physical packaging

b. Type of security protection (Encryption or COMPUSEC or both)

4.5.2.5 User Processing Component

The User Processing Component shall consist of single board computers which include the CPU, random access memory, and input/output capabilities. In many cases one or more of the standard Processor Boards will accommodate User Group processing requirements. In cases where extensive mathematical analysis is conducted, higher speed/cost processors may be required.

At larger installations a Workstation with embedded processing power will be used to host the user function and perhaps certain communications oriented user functions such as Message Generation.

4.5.2.6 User Distribution Component

The User Distribution Component will consist of backplane bus technology, local area network technology, patch panels and discrete connections as required.

4.5.2.7 User Chassis Component

The hardware implementation will consist of a majority of components that are common with other groups such as the Communications Service Group. This common standard hardware must be combined with a variety of user interfaces that some cases may be unique to the application. A large number of user interfaces may need to be accommodated. The physical size of the electronics is not the driver in the number of these interfaces that can be implemented into a chassis, but rather the connectors on the back (ship) or front (aircraft) panels.

4.5.2.8 User System Improvement

The AN/SYQ-7(V)2 NAVMACS is a key Navy system used extensively aboard WHECs and WMECs for the exchange of GENSER message traffic. Significant enhancements to the NAVMACS have been recently implemented by the U.S. Navy. If implemented by the Coast Guard aboard their cutters immediate dividends would be yielded in terms of (1) automated message distribution and (2) providing an architecture conforming to the proposed ICS architecture which accommodates the addition or enhancement of communications technology with little or no impact to the base NAVMACS message processing system. Likewise, any changes to the NAVMACS message processing function has little or no impact on its communications function. This upgraded NAVMACS, generally referred to as NAVMACS-II, separates the communications function of NAVMACS from its message processing function. That is, this implementation of NAVMACS is segmented into a Communications Service Group and a User Group. Furthermore, these functional groups are tied together by elements of a System Distribution Group. The communications capability of NAVMACS-II has been designed to meet, not only near-term communication requirements, but also projected long-term data rate requirements. It has already been upgraded (and successfully tested) to permit simultaneous operation of the Common User Digital Information Exchange Subsystem (CUDIXS) SATCOM link at 9600 bps and a broadcast input at 1200 bps. Incidentally, the 1200 bps broadcast is the proposed GENSER High Speed Fleet Broadcast (HSFB). Additionally, the communications capability of NAVMACS-II has been successfully tested to operate 16 RF interfaces simultaneously at 9600 bps. In fact, the NAVMACS-II communications function has been implemented to be scaleable to support 32 channels.

The elements of NAVMACS associated with the User Group are collectively referred to as the NAVMACS Message Processor (NMP). It is physically hosted in a UNIX-based workstation. This host computer can be any UNIX-based workstation containing an Ethernet interface.

Therefore, the NMP can be hosted by a DTC-II, TAC-3, TAC-4, or even a PC-based system. The elements of NAVMACS associated with the Communications Service Group are collectively referred as the NAVMACS Communications Controller (NCC). It is physically implemented in a VMEbus chassis containing this RISC Motorola 68020-based I/O processors and one Motorola 68040-based subsystem control processor.

The subsystem control processor performs overall system control and contains an Ethernet interface to the NMP. The NMP is used to download all NCC software during initialization and, once operational, is used as the communications interface between the message processing component (User Group) and the communications controller component (Communications Service Group) of NAVMACS. One I/O processor and the RISC emulation processor are used in conjunction with the system control processor to allow for execution of the UYK-20 based NAVMACS software which executes the CUDIXS interface function. The system control processor along with two I/O controller processors contain the processing functions for supporting an additional 15 serial interfaces to include Fleet Broadcast and Full Period Termination (FPT) circuits.

The NCC software uses the commercial off-the-shelf (COTS) VxWorks™ operating system from *Wind River Systems, Inc*. This COTS operating system is available for several families of microprocessors and can be networked with any UNIX-based host systems, or any other operating environments possessing TCP/IP networking facilities. The actual NCC software is divided into segments with each segment performing a specific function. This loosely coupled and layered architecture provides an extremely open environment which lessens the impact of adding changes to the NCC system.

One final implementation note of significance should be noted. The VIGC, currently implemented aboard WHECs and WMECs to provide OTCIXS capability, is hosted in hardware nearly identical to the NAVMACS-II communications controller. The VIGC is hosted by three VMEbus cards - (1) a Motorola 68020 based I/O controller (2) a Motorola 88100 based RISC emulation processor (3) a Motorola 68030 based subsystem controller processor. The system controller processor used in both the VIGC and NAVMACS-II are supplied by the same commercial vendor (Force Computers). The VIGC uses a less powerful 32-bit microprocessor (the Motorola 68030 rather than the 68040). Furthermore, the VIGC also uses the same COTS VxWorks™ operating system used by the NAVMACS NCC. Finally, the VIGC utilizes a UNIX-based workstation in the same manner as the NAVMACS NCC. Therefore, the VIGC and NAVMACS-II NCC can be hosted in a single VME chassis accommodated by a four card set - RISC Emulation Processor, System Control Processor, and two I/O Controller Processors. The long-term net effect is that only one I/O controller board would need to be added to the current VIGC to support the currently known Navy GENSER narrative message requirements.

4.6 System Distribution Group

The System Distribution Group (SDG) provides distribution of baseband data and control among groups throughout the ICA architecture. SDG functionality includes:

a. Inter-Group Communications Connectivity (Link Access/Radio, Communications Service, System Controller, User)

b. Inter-Group Control connectivity

c. Inter-Group Security Control

d. Interprocess (software components) Control

4.6.1 Existing Equipment

Existing System Distribution group elements are summarized in Table 4.6.1-1.

Table 4.6.1-1 Existing System Distribution Group

Designation	Description	210'	270'	378'
CDIE-GRC-980	URC-116 Interface	X		
CEJD-MSR-6600	Mackey Interface	X		X
CV-3591(P)	ANDVT Interface	X	X	X
SB-4124/WSC	Patch Panel		X	X
SB-4125/WSC	Patch Panel		X	X
IEEE-802	Ethernet Local Area Network	X	X	X
MIL-STD-188/114	Serial Interface	X	X	X

4.6.2 Recommended Improvements

To perform the functions defined for the SDG (Section 4.6 a through d) within the context of the new technologies becoming available, additional component and interface requirements need to be defined. Utilization of various combinations of the components and interfaces, listed below, are required to perform SDG functions.

a. MUX/DEMUX Component

b. Local Area Network Component

c. Baseband Patch Panel Component

These elements have been arranged into a recommended specification tree, as shown in Figure 4.6.2-1. The tree is organized by component and then by elements.

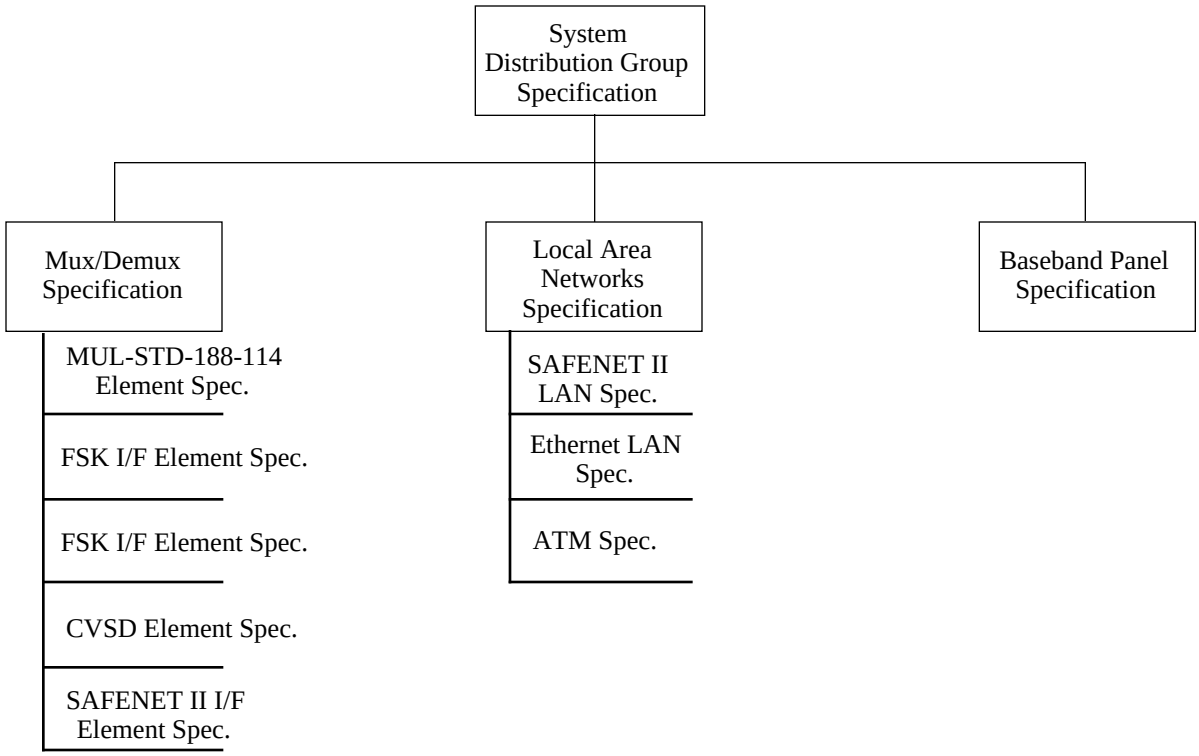


Figure 4.6.2-1 SDG Specification Tree

The first Specification Tree subgroup is the Mux/Demux used for interoperability with existing equipment necessary during transition to the ICS. It contains MIL-STD-188-114 interfaces and a LAN interface to support new and existing equipment. The FSK interface and CVSD Vocoder are required for complete compatibility with the U.S. Navy TD-1389 SHF Mux/Demux. SAFENET II and Ethernet are the primary candidates for the interconnecting LAN. A baseband patch panel specification is also included as a subgroup element within this Specification Tree.

The group must accommodate interfaces to both new and existing communications equipment and represents the key to an effective transition to the next generation USCG ICS. A wide variance of requirements must be addressed to support each of the application platforms and their unique interfacing and installation issues.

Existing communications system connectivity is characterized by a point-to-point, closely coupled, via switchboards, patch panels and system components interconnection architecture. These components are listed in the “Current Capabilities and Work Flow Analysis Report” generated under this delivery order and are not repeated here. However, an open system must employ methods to interconnect various components within the OSI parameters. Existing interconnects do not lend themselves to upgrade or redesign towards that end. Wholesale replacement may be cost prohibitive but incremental modernization to OSI standards is quite plausible. Incremental changes may not immediately impact manning or training but the goal system definitely would reduce both requirements considerably.

Presented in the following subparagraphs are proposed improvements for supporting both transition (1997-time frame) and the longer term (2005 time frame) next generation USCG system architectures. These concepts are also further expanded throughout Section 4 of this report to address specific equipment replacement and installation considerations.

4.6.2.1 Mid- to Long-Term - Internet Connectivity

Incorporation of internet connectivity into the USCG must consider on both DoD (U.S. Navy) and commercial initiatives. The Navy has incorporated internet for shipboard and shore applications. Almost exclusive use of TCP/IP protocols for LANs allows systems like JOTS/JMCIS, NAVMACS, and VIGC to join clusters of similar systems by using existing Internet Wide Area Network (WAN) connectivity techniques. Commercial enterprise networks regularly use TCP/IP's WAN connectivity and newer WAN switches to tie remote facilities together into virtual workgroups.

Navy applications have, historically, been closely focused on mission objectives. This typically yields a myopic vision of how to communicate information from system "A" to another application of system "B". Both "A" and "B" have well defined missions. However, the independent implementation teams (and management funding chains) may have different views of interoperability requirements. System "A", implemented earlier, may not even have sufficient capabilities to interconnect with another system. The planners for "B" may view data contained in "A" as essential. However, the internetworking of the two systems may prevent "A" from accomplishing its original mission.

Recent DoD activities have consistently included network interoperability requirements to reverse this historic trend. For example, instead of continuing to require mission specific display designs, open architecture must be required in order to easily reconfigure the display system which uses standards-based internetworking capabilities. Thus generalized, the display element may be re-used in other applications or easily cross-connected using LAN and WAN internetwork technologies.

In a USCG context, this means that incorporation of newer commercial initiatives will be less costly than incorporation of U.S. Navy elements EXCEPT where those systems have designed-in open system architectures. By incorporation of internet and related technologies a richer communications pathway is made available to USCG for both afloat, dockside, and shore facilities. Communications diversity is provided wherein both DoD & commercial communications equipment are viable.

4.6.2.2 Public Internet and Private Internet

The popular view of the Internet fails to give sufficient emphasis on the existence of both private and public internets. The USCG must incorporate this distinction into its planning.

In the strictest sense, an internet is a set of protocols by which heterogeneous systems may communicate. Equipment, software, and applications from many different developers simply agree to use these protocols while passing information to each other. Each end is said to be privately implemented. That means that one end of the internet communication should assume nothing about the nature of the machine(s) at the other end.

A single network is a collection of machines communicating with each other over a private or enterprise WAN. This is typical of a large corporate or proprietary value added network. These private networks are frequently cross-connected to other networks via a gateway-link. This gateway-link typifies the thousands of similar links by which the Internet is created.

Creation of a private USCG internetwork is the first step to incorporation of internet technology. A private USCG network adds internet-style secure gateways between existing USCG shore-based LAN/WAN networks. A wide area USCG private network is implemented with public carrier circuits using permanent virtual circuits and link level encryption.

At key points in the private network, secure gateways would link to the public Internet. Likewise, the USCG private network would create secure gateways to dockside and afloat cutters.

4.6.2.3 Public Network Security

The USCG's private internet implementation not only needs to be physically separated from the public Internet but also needs to employ a logical firewall to block unwanted probes from the public. Use of packet level filtering, carefully constructed proxy services, robust logging, automated security sweeps, and frequent security audits are all required. Fortunately, most of these techniques are built into the latest COTS internet routers and firewall equipment. Strict enforcement of these firewall protections at the public gateways is absolutely mandatory.

4.6.2.4 Private Network Security

In addition to commercial security measures, DoD security measures are also mandatory to prevent disclosure of sensitive or classified messages. Inside the public gateway firewall, the USCG private internet implementation must be constructed to guidelines appropriate to segregation of traffic.

4.6.2.5 Mid- to Long-Term - USCG Shipboard Network Connectivity

Review of existing USCG cutters shows that a variety of media are already in use. These include older voice wireline and traditional coax media. Ethernet coax, unshielded twisted pair, (UTP) and fiber-optic cables have been used or are planned for recent upgrades. An open architecture standard needs to be employed to ease adoption of newer technologies into the USCG cutter environment. Because of the diverse mixture of physical interface requirements between older systems and newer technologies, there is no single media standard which can be exclusively used. Table 4.6.2.5-1 illustrates the diversity within the group of new high speed network solution contenders.

Table 4.6.2.5-1 High Speed Networks

Technology	Fast Ethernet	Switched Ethernet	FDDI	ATM
Bandwidth	100 Mbps	10/100 Mbps	100 Mbps	25 - 622 Mbps
Access Technique	CSMA/CD	CSMA/CD	Token	Cell-based switching
Marketed Position	Desktop-to-Backbone	Desktop-to-Backbone	Backbone	WAN, LAN, Backbone
Physical Media	UTP (Cat. 3,4,5), fiber, STP	UTP (Cat. 3,4,5), fiber, STP	UTP (Cat. 5), fiber, STP	UTP (Cat. 5), fiber, STP
Cost	$300	$100-$500	$1000	>$1000
Advantages	Wide vendor support	Compatible with existing network interface cards	Established standard	Scaleable, supports voice, video, data

The issues are not restricted to physical media. Communications protocols in use on a USCG cutter exhibit a broader mixture than the physical media.

The leading candidate for both high speed media and protocols is Asynchronous Transfer Mode (ATM). Commercial and government network designers are adopting ATM based switches and routers. Commercial workstation vendors are introducing second generation ATM interface cards. Mixed interface routers, called generically, "ATM Edge Routers" have been introduced to provide Ethernet (Coax, AUI, UTP), T1 (V.35, RS449), asynchronous (RS232), and FDDI interfaces which provide both access to the ATM backbone and multi-protocol gateway capability.

For USCG shipboard applications, existing LANs should be connected via Edge technology to an ATM switch. When multiple, independent, LANs exist the ATM switch can be used to either bridge between them or to create private virtual LAN workgroups.

Bridging means that traffic flows easily between the individual LAN segments but the only traffic which crosses the bridge is only that which has been specifically addressed to stations on opposite sides of the bridge. Traffic between stations on either side of a bridge flows in an ad hoc manner. Otherwise, the traffic on each LAN segment remains isolated from traffic on all other segments.

A virtual LAN workgroup is created by logical grouping rather than physical LAN segment location. Groups of workstations are assigned to virtual workgroups regardless of their physical LAN segment. Once assigned, all members of the virtual workgroup have uniform access to each other but are logically isolated from the traffic of other workgroups. Traffic flow among members of the same virtual workgroup is ad hoc. Traffic flow between members of different workgroups requires specific gateway routing.

4.6.2.6 Mid- to Long-Term - LAN/WAN RF Capability

Older RF based systems with only RS232/MIL188 require integration efforts to incorporate them into uniform LAN access. This integration may be as simple as re-connecting the serial terminal port from the older system into a port on a LAN terminal server. This technique allows LAN users to access the older RF based system from any workstation. More extensive integration may be required to accommodate emulation of older TTY/serial terminal characteristics.

Recently updated RF based systems such as NAVMACS-II or the VIGC have LAN capabilities. Because of this they may be more easily incorporated into USCG shipboard internet technology. Integration efforts may be required for these systems as well. For example, JOTS/JMCIS originally specified a serial interface between OTCIXS/TADIXS rather than a LAN. However, the VIGC is fully LAN integrated. Because JOTS/JMCIS did not expect LAN input for Navy Information Exchange Subsystem (IXS) communications, the VIGC had to provide the older serial port interface to JOTS/JMCIS even though both systems had full LAN hardware capabilities.

4.6.2.7 Mid- to Long-Term - LAN/WAN Routing Capability

USCG shipboard LANs need WAN access capabilities. This is accomplished by adding a router with wide area interfaces. This LAN/WAN routing capability can be designed for dockside and afloat operations. Dockside operations require integration with shore based LAN systems. Afloat operations require integration with both shipboard LAN and with some ship-to-shore RF system.

For dockside operation, the WAN interface may be a low speed asynchronous analog line, low speed digital ISDN line, a higher speed synchronous line, or a wireless LAN circuit. The analog line is the easiest to install but the slowest at 28.8 kbps. The ISDN 64 kbps line is faster and more reliable but is not uniformly available. A leased T1 (1.544 Mbps) would be ideal but is more costly to install and operate. The newer wireless LAN interfaces are slightly faster than T1

and cost about the same to install. Wireless LAN technology has a much lower operational cost than the T1, its closest speed rival.

If wireless WAN/LAN is used for connection of in-port vessels, each vessel (or each berth) would need a wireless node radio/antenna. Commercial nodes available today operate with inexpensive equipment and antenna systems (less than $7K each). Commercial DES hardware encryption is available on better units.

4.6.2.8 Near-Term LAN Based Protocol Stacks - Intra-Ship Network

Standard "open" commercial communication protocols are becoming mandated for Navy systems. Consequently, a strong and critical recommendation is proposed whereby the Coast Guard employ those communication protocols associated with the presentation, session, transport, network, data link, and physical layers of abstraction as defined by the ISO OSI Reference Model for the interconnection of the major functional components of the Communications Service Group, as defined in Section 3 of this document for the ICS architecture (Intelligent Gateway, Communications Server) as well as that between the Communications Service Group and the User Group.

4.6.2.8.1 Common Protocol Definition

The following protocols are recommended to be used for both the Communications Server/Intelligent Gateway and the User/ICS Interface:

a. IEEE 802.12 Local Area Network Standard - This fast Ethernet protocol, also referred to as 100-Base-VG, establishes the data link communications protocol over either a four-pair category 3,4, and 5 unshielded twisted pair, two-pair category 5 shielded twisted pair, or fiber optic cable (both single-mode and multi-mode fiber). The 100-Base-VG scheme was developed by the IEEE 802.12 committee. It diverges from the standard media access control (MAC) layer defined for standard Ethernet by adding demand prioritization. 100-Base-VG eliminates packet collisions and permits more efficient use of the LAN bandwidth. Instead of collision detection or circulating tokens, the 100-Base-VG MAC protocol is a round-robin polling scheme. This feature permits special priority to be set for low latency traffic often referred to as isochronous traffic. 100-Base-VG exhibits extremely low and predictable latency due to its rapid "on the fly" frame switching and dual prioritization levels - one for "normal" traffic and the other for isochronous time-sensitive traffic requiring precisely predictable delivery rates (e.g., motion video and voice)

b. Transport Control Protocol (TCP) - This transport protocol provides a reliable data communication service. TCP is connection oriented; it maintains a connection, or virtual circuit, between a pair of communicating processes. TCP incorporates mechanisms to ensure the reliability of the connections and to control the flow of data over the interface. The TCP is implemented in accordance with MIL-STD-1778.

c. Internet Protocol (IP) - This network protocol permits data to be transmitted and received across networks. Unlike TCP, it is connectionless and neither checks data for errors nor performs flow control. It provides the means to communicate across multiple networks. The IP is in accordance with MIL-STD-1777.

d. BSD Socket Conventions- This session protocol is used in conjunction with the TCP/IP transport/network protocols. It provides a session interface to the TCP/IP protocol suite using the “socket” based abstractions as defined by BSD UNIX version 4.3. This protocol defines the manner in which a pair of processes communicating over the reliable point-to-point connection establish and terminate their “communication session.” The protocol is based on a client-server architecture whereby one side (server) of the potential point-to-point communication circuit must be listening before the other side (client) attempts to connect with it. Once a dedicated software connection (“socket”) is established between communicating processes, the processes “converse” over a full-duplex virtual circuit. BSD Socket Conventions for the ICS interfaces adhere strictly to BSD UNIX 4.3 TCP/IP interface conventions.

4.6.2.8.2 User/Communications Server Interface

The following protocols are recommended to be used for the Communications Server/User Interface:

a. BSD Socket Conventions - refer to definition in subparagraph 4.6.2.8.1

b. TCP/IP - refer to definition in subparagraph 4.6.2.8.1

c. 100-Base-VG - multi-mode fiber implementation, refer to definition in subparagraph 4.6.2.8.1

d. External Data Representation (XDR) - a presentation protocol which permits dissimilar computers to communicate by specifying a common data representation format. This representation standard allows for interoperability between systems running on dissimilar computers using a standard representation format for highly formatted messages (i.e., bit-oriented messages) such as track data. Using this representation format, strongly “typed” messages containing data items with computer dependent interpretations (ASCII, 2/4 byte integer, 4/8 byte floating point) can be easily exchanged between dissimilar computers. The XDR protocol defines the manner in which messages are encoded when transferred between two computers.

XDR presentation protocol is recommended to eliminate data representation incompatibilities amongst both local and remote message processing subsystems for any highly formatted messages. The TCP/IP protocol suite is used to ensure reliable, point-to-point, network communications between a message processing subsystem and the ICS Communications Server. The BSD Socket Conventions protocol is used to define the manner in which connections are to be established between a message processing subsystem and the Communications Server. In establishing a connection, the message processing subsystem is the “client” and the Communications Server is the "server” with the so-called “well known" port number and IP address.

Inter-platform messages are passed between the message processing subsystem and Communications Server. Messages to be routed to remote platforms are passed from the message processing subsystems to the Communications Server. Likewise, messages destined locally received by the ICS are passed to the local message processing subsystems via the ICS Communications Server.

This User/ICS Communications Server interface becomes active once a point-to-point connection between a client (message processing subsystem) and the router (Communications Server) has been established by the underlying *BSD Socket Conventions* session protocol. Once

activated, the message processing subsystem sends a *User Registration* message to the Communications Server. This message identifies the message processing subsystem in "plain language" terms. The message processing subsystem identifies the subsystem by cutter area, its operational function, or by an actual human user (e.g., “CDR Smith”). The message processing subsystem identity may also be established by a combination of these identification types. The registration message also identifies the messages of interest to the registered message processing subsystem. This serves as an automated screening function for incoming messages. The ICS Communications Server will only forward to the registered message processing systems these specified messages. Once a message processing subsystem identity has been registered with the ICS Communications Server, the message routing session is established and inter-platform user-to-user messages are exchanged between the ICS Communications Server and the message processing subsystem. Following registration, the message processing subsystem may elect at any time thereafter to send additional *User Registration* messages reflecting new message processing subsystem identity (different user, different function, new messages of interest, etc.). The message routing session is terminated when either the message processing subsystem or the ICS Communications Server sends a *Disconnect* message to its peer. The peer will be closed by the underlying *BSD Socket Conventions* session protocol.

4.6.2.8.3 Communications Server/Intelligent Gateway Interface

The following protocols are recommended to be used for the Communications Server/Intelligent Gateway Interface:

a. BSD Socket Conventions - refer to definition in subparagraph 4.6.2.8.1

b. TCP/IP - refer to definition in subparagraph 4.6.2.8.1

c. 100-Base-VG - multi-mode fiber implementation, refer to definition in subparagraph 4.6.2.8.1

A high level message exchange interface based on IDS-8648 is layered over the above specified protocol suite. Messages containing user data exchanged across this interface are termed ICS Data Units (IDUs). IDUs transferred from the Communications Server to the Intelligent Gateway are defined as "transmit" IDUs and those transferred from the Intelligent Gateway to the Communications Server are defined as "receive" IDUs. Full-duplex IDU transfers are supported by this interface - Communications Server-to-Intelligent Gateway and Intelligent Gateway-to-Communications Server IDU transfers, as well as control information exchange, may occur concurrently over the interface. Figure 4.6.2.8.3-1 depicts the three transfer sequences supported by this high level message exchange protocol.

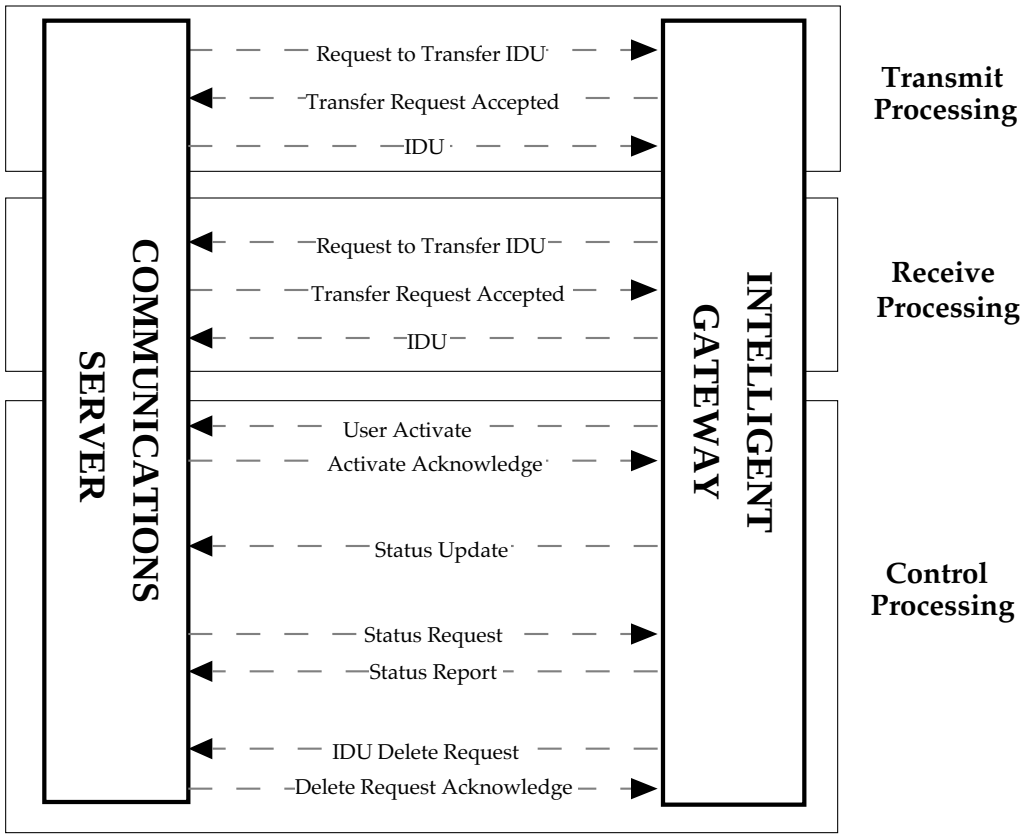


Figure 4.6.2.8.3-1 Communications Server/Intelligent Gateway Transactions

This interface is characterized as follows:

a. Interface initialization - the Intelligent Gateway establishes the interface by sending an *Activate* message to the Communications Server. After the Communications Server responds with an *Activate Acknowledge* message to the Intelligent Gateway, the interface is activated for IDU transfers.

b. Transmit IDU transfers - the Communications Server initiates each transfer by sending a *Request to Transfer IDU* message to the Intelligent Gateway. Depending on its ability to accept the IDU, the Intelligent Gateway responds with either a *Transfer Request Accepted* or *Transfer Request Rejected* message. If the Intelligent Gateway accepts the transfer request, the *IDU* is transferred to the Intelligent Gateway. If the Intelligent Gateway rejects the request, the Communications Server must wait until a *Status Update* message is received from the Intelligent Gateway indicating its ability to accept IDUs before once again attempting to transfer IDUs.

c. Receive IDU transfers - the transactions associated with the transfer of receive IDUs are symmetrically identical to that defined for transmit IDUs.

d. Control message exchanges - both the Intelligent Gateway and the Communications Server may send a *Status Update* message indicating its operational status at any time once the interface between has been established for IDU transfers. No response is generated by the receiver after receiving this message. Other control transactions currently defined for the interface are

initiated by the Communications Server. The Communications Server will send *Status Request* and *IDU Delete Request* messages to the Intelligent Gateway. The Intelligent Gateway will respectively respond with *Status Report* and *Delete Request ACK/NAK* messages.

4.6.2.9 Modular Security Architecture

Significant work has been expended recently by both the U.S. Navy and industry with respect to the development of modular security devices (MSD). MSDs are clearly the wave of the future insofar as security equipment is concerned and, consequently, its integration into cutter communication systems is highly recommended. The major functions of the MSD are shown in Figure 4.6.2.9-1. The MSD can be used for both COMSEC and "selective" data encryption. This latter capability allows the MSD to be an interim solution (prior to the implementation of multi-level secure operating systems) to the security issue involved with multi-level security classifications of user data aboard cutters. Trusted processes partition plain-text data into encrypt/decrypt and bypass paths. The bypass path would support control/status bypass in addition to header bypass, and would provide signaling I/O for Link COMSEC use.

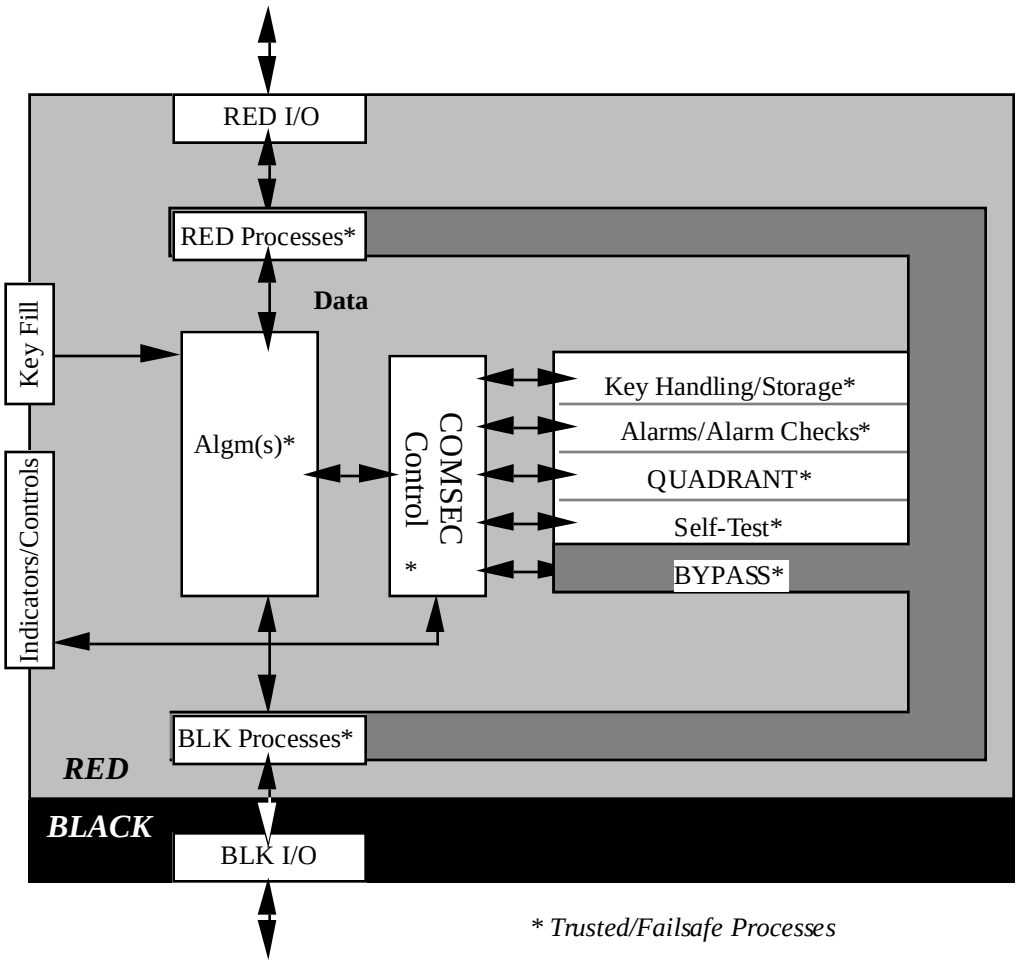


Figure 4.6.2.9-1 Major Functions of the MSD

Many of the available MSD devices under development are VMEbus based. Consequently, the MSD based recommendation also includes the use of a multi-compartment VMEbus chassis.

Figure 4.6.2.9-2 illustrates the MSD based security implementation recommendation.

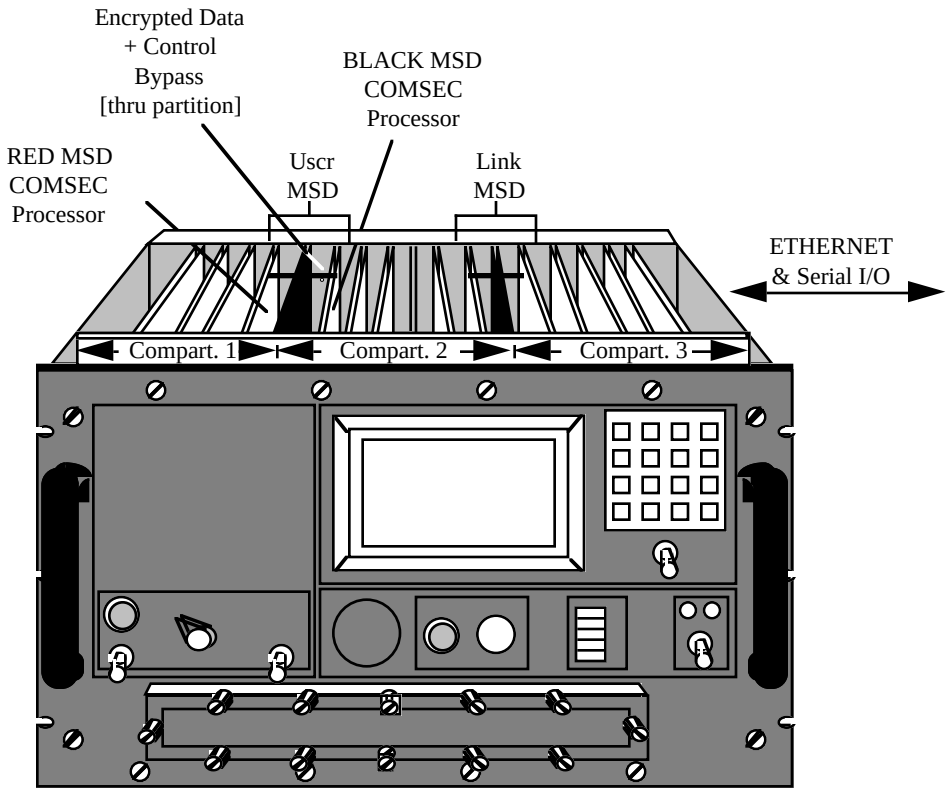


Figure 4.6.2.9-2 Ideal ICS Compartmented Chassis Implementation

Implementation of the link or user level MSD would be accomplished via partitioning MSD functions into 2 VME cards with data encryption/decryption and control/signaling bypass functions which cross a compartment boundary between the cards. In fact, all COMSEC operations are performed on the RED side card, and the BLACK side card can be placed in a local or remote compartment. User “communities of interest” are placed in individual compartments, such as compartments 1a and 1b, each with a unique user interface Fast Ethernet card and a MSD. Once a B2/B1/C2 real-time operating system adaptable to a distributed environment with trusted applications becomes available, users would be able to interface to the Communications Service Group through Fast Ethernet interface cards in compartment 1. A B2/B1/C2 real-time operating system (OS) on a single-board computer (SBC) would provide the requisite separation of multiple user “communities of interest” sharing a common interface card and operating in compartmented mode. This would eliminate the need for a trusted SBC in VME slot 1 of the chassis compartment.

Compartment 2 of Figure 4.6.3.6-2 correlates to the “RED-ICS” zone previously attributed (in Section 3) within the ICS security architecture, while Compartment 1 is the “RED” zone, and compartment 3 is the “BLACK” zone. Alternatively, the “BLACK” zone could be provided out-of-chassis by an interface from compartment 2 to existing equipment, and compartment 2 extended to accommodate multiple Communications Service Group processor cards. This chassis concept will allow free partitioning of multiple compartments and multiple VME 6U/9U board sizes. Multiple chassis would be interconnected by Fast Ethernet LANs for larger numbers of user “communities of interest”, or to accommodate additional Communications Service Group processing cards.

4.6.2.10 Additional Recommendations

Additional modernization recommendations specific to large (i.e., WHEC) and small classes of cutters are discussed in the following subparagraphs.

4.6.2.10.1 Large Class Cutter System Distribution Group

These applications environments will have large numbers of User Groups (segmented by application, location and security) and large numbers of Link Access/Radio Groups. Figure 4.6.2.10-1 contains a block diagram of the recommended approach for these applications. In the longer term (2005-time frame) ICA; the goal is for all baseband data and control information to be distributed over a fiber-optic LAN. The transitional architecture (1997-time frame) will include a combination of existing IXS and Link Access/Radio Group equipment and new technology equipment such as those described in the ICS. It is the transition architecture that is emphasized throughout this report.

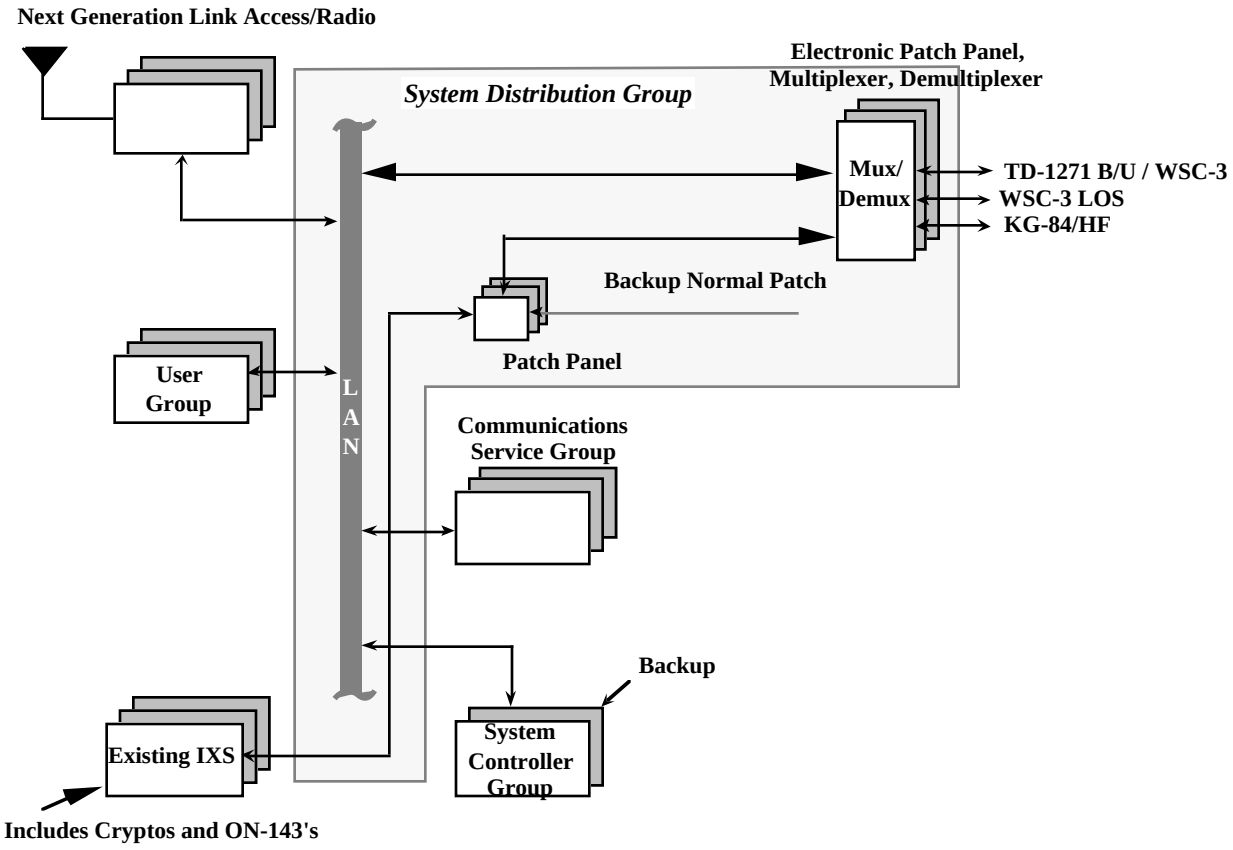


Figure 4.6.2.10-1Large Class Cutter Transition Configuration

As systems such as OTCIXS with the VIGC are installed a LAN approach will be used for connectivity of new equipment. The transition concepts for upgrading the USCG communications systems have considered primarily interoperability between the ICS and existing interconnecting groups (ON-143) and radio equipment. The transition approach from an existing IXS perspective is to maintain fixed dedicated connectivity between IXS and radio channels. IXS would be incorporated into the multiple media, resource sharing benefits of the new architecture as they are upgraded one-by-one. Several significant drawbacks of this approach are listed below:

a. This transition period for upgrading all IXS will likely take 10 to 15 years

b. Dedicated IXS radio channels are lost from the pool of potential resources

c. Two separate Communication Control Operational environments will have to coexist (IXS and Post ICS System Controller)

The USCG must operate in line with the Navy modes. This Mux/Demux also maintains a LAN interface. Through this LAN interface the radios connected to the Mux/Demux through a patch panel are now available for access by new equipment residing on the LAN. This LAN connection is also used to send control information from the System Controller Group to the Mux/Demux for configuring connectivity between existing IXS or the LAN and radio resources. In this approach an interim capability is provided for pooling of radio channels under the centralized control of the new System Controller Group. Patch panels are provided on each end of the Mux/Demux to permit manual patching when necessary. Another related feature of the Mux/Demux is its ability to act as a port expander for either the TD-1271 B/U DAMA or the WSC-6 radio. This configuration provides multiple DAMA access capability for multiple end user channels. It allows a single Mux/Demux to operate as a low-rate modem with multiple channels to interface its composite channel directly into a single 1200/2400/4800 bps DAMA port. Mux/Demuxes configured as multiple low-rate modems are attached directly into multiple DAMA ports. This extends the access opportunities for limited availability DAMA ports without frequent operator patch panel changes. The Mux/Demux can easily be implemented in a COTS single board computer possessing the requisite serial I/O channels. Transition to a Mux/Demux implemented in COTS VMEbus single board computer consists of installing a VME chassis with the desired number of Mux/Demux single board computers and establishing cable connections from user equipments, DAMA ports, and the chassis's connector panel.

4.6.2.10.2 Small Class Cutter System Distribution Group

The application environment for small class cutters requires many fewer users and radio resources to be considered. Close proximity of equipment and the fewer number of users and interfaces offers an opportunity for consolidation of groups. Similar to large class ships, it is recommended that the System Controller Group be implemented by a workstation (e.g. TAC-4). Other groups can most likely be consolidated into fewer chassis. Recommended guidelines for consolidating groups are shown in Figure 4.6.2.10.2-1. Multiple steps are shown leading toward a totally consolidated solution. It is anticipated that most shipboard applications will be supported by consolidation steps #1 or #2. Steps #3 and #4 are highly applicable to the smallest cutters with even more limited space for communications equipment. This same four step consolidation methodology is applicable across all platforms.

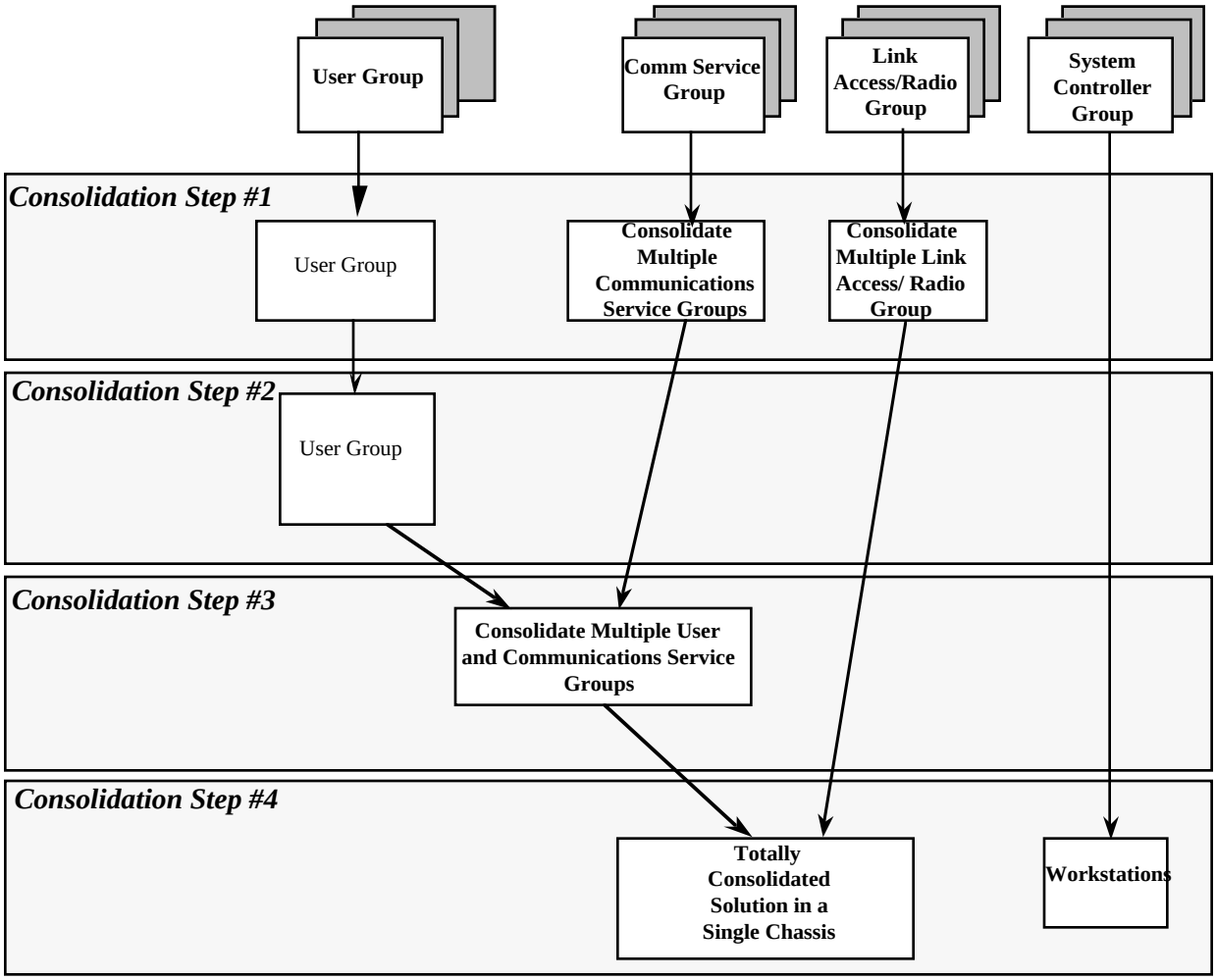


Figure 4.6.2.10.2-1 Guidelines for Consolidating into Fewer Chassis

As solutions reduce down to fewer chassis, more System Distribution Group requirements are satisfied by bus interconnects or point-to-point cabling inside each chassis. In most applications, however, multiple chassis are still required. Therefore, to maintain modularity and flexibility for expansion, a LAN interconnect, similar to the large class ship example, is recommended. Even in the totally consolidated situation, a LAN interconnect to the System Controller Group for transfer of control information is recommended. For these smaller platforms, the use of a fiber optic LAN may be cost prohibitive. Consideration is being given to recommend an Ethernet alternative for the small ship class or shelter applications. Figure 4.6.2.10.2-2 graphically represents this Ethernet alternative.

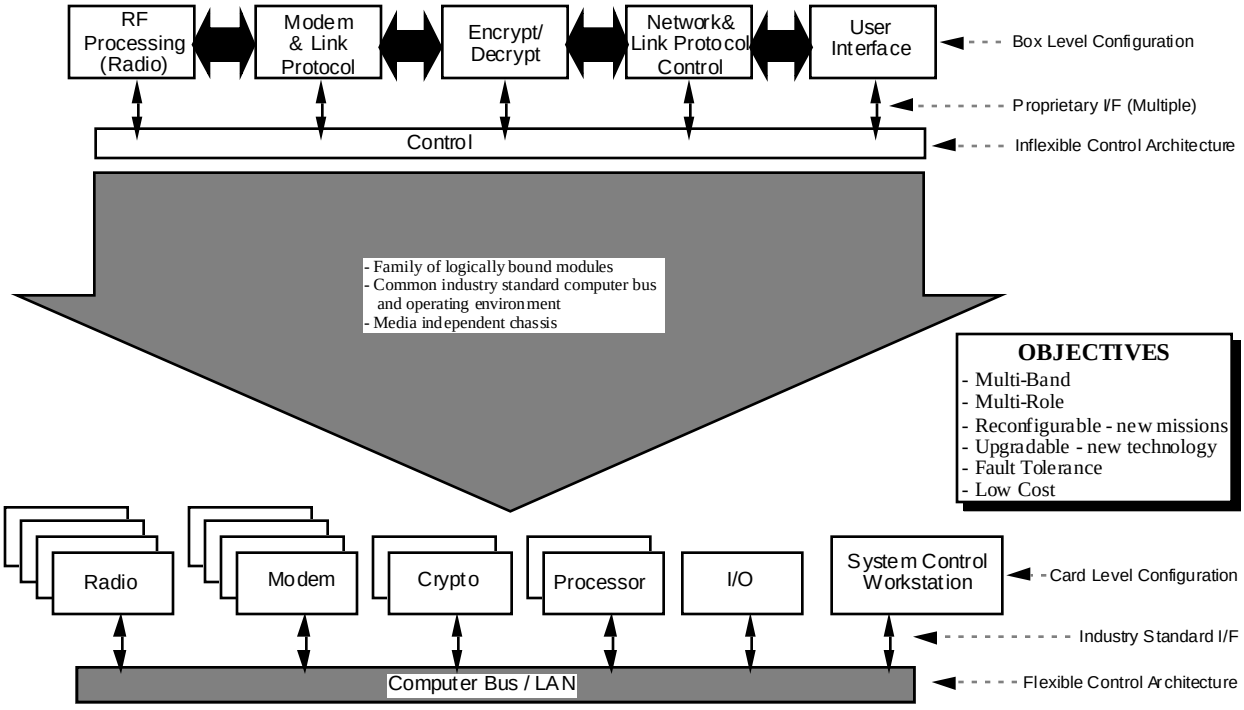


Figure 4.6.2.10.2-2 Consolidating Into Integrated System

Figure 4.6.2.10.2-3 depicts the significant size savings obtained in following these consolidation outlines by illustrating the difference in size requirements when transitioning from a WSC-3/TD-1271 based Link Access/Radio Group subsystem to a VMEbus based configuration.

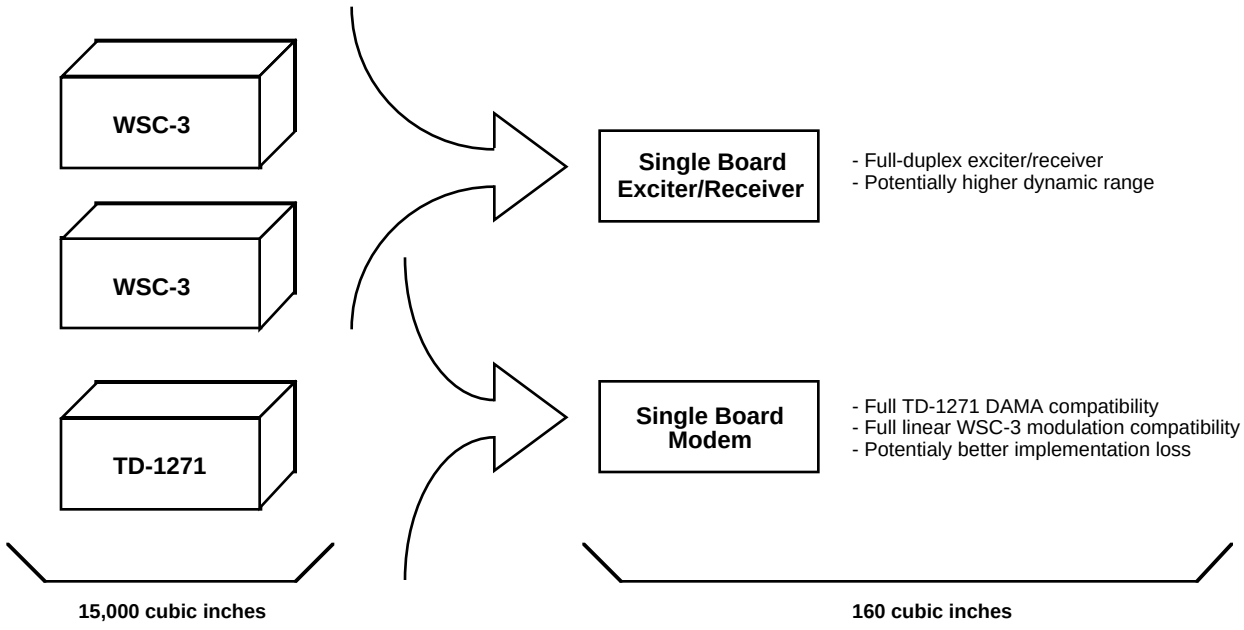


Figure 4.6.2.10.2-3 Translation of WSC-3/TD-1271 Into VME

Appendix A — Acronyms and Abbreviations

AAW	Anti-Air Warfare
ACK	Acknowledgment
ADCCP	Advanced Data Communication Control Procedure
ARPA	Advanced Research Projects Agency
ASUW	Anti-Surface Warfare
ATM	Asynchronous Transfer Mode
BIT	Built-in-Test
BOM	Bit Oriented Message
BPS	Bits per second
BSD	Berkeley Software Distribution
CBT	Computer Based Training
CCC	CINC Command Complex
CD	Carrier Detect
CDFTT	Combat Direction Finding Tactical Intelligence Terminal
CINC	Commander in Chief
CLNP	Connectionless Network Protocol
CLTP	Connectionless Transport Protocol
COMMPLAN	Communications Plan
COMPUSEC	Computing Security
COMSEC	Communications Security
COTS	Commercial Off-the-Shelf
CSG	Communication Services Group
CSMA	Collision Sense Multiple Access
CSS	Communication Support System
CTU	Commander Task Unit
CUDIXS	Common User Digital Information Exchange Subsystem
CWC	Composite Warfare Commander
DAMA	Demand Assigned Multiple Access
DARPA	Defense Advanced Research Projects Agency
DAT	Digital Audio Tape
DoD	Department of Defense
DTC	Desktop Computer
EIA	Engineering Institute of America
EHF	Extremely High Frequency (300 GigaHertz to 3 teraHertz)
ELOS	Extended Line of Sight
FDDI	Fiber Data Distributed Interface
FPT	Full Period Termination
FSC	File Server Control
FSK	Frequency Shift Key
GENSER	General Service
GLOBIXS	Global Information Exchange System
GUI	Graphical User Interface
HDLC	High-Level Data Link Control
HF	High Frequency
HSFB	High Speed Fleet Broadcast

ICA	Integrated Communications Architecture
ICS	Integrated Communications System
IDU	Integrated Communications System Data Units
IEEE	Institute of Electrical and Electronic Engineers
INMARSAT	International Maritime Satellite
I/O	Input/Output
IP	Internet Protocol
IPC	Interprocess communication
Iridium	*The 77th element in the periodic table of contents*
ISDN	Integrated Services Digital Network
IXS	Information Exchange Subsystem
JMCIS	Joint Maritime Computer Information System
JOTS	Joint Operational Tactical System
JTF	Joint Task Force
kbps	kilo-bits per second
LAC	Link Access Control
LARG	Link Access/Radio Group
LAN	Local Area Network
LF	Low Frequency
LOS	Line of Sight
MAC	Media access control
Mbps	Mega-bits per second
MF	Medium Frequency
MHz	MegaHertz
MIT	Massachusetts Institute of Technology
MMI	Man-Machine Interface
MSD	Modular Security Device
NAK	Negative Acknowledgement
NAVMACS	Naval Modular Automated Communication Subsystem
NCC	NAVMACS Communications Controller
NDI	Non-Developmental Item
NECC	Navy EHF Communications Controller
NETSEC	Network Security
NGCR	Next Generation Computer Resource
NMP	NAVMACS Message Processor
NOSC	Naval Ocean Systems Center
NRL	Naval Research Laboratory
OIC	Operator Interface Control
OSA	Open Systems Architecture
OSF	Open Systems Foundation
OSI	Open Systems Interconnect
OTCIXS	Officer in Tactical Command Information Exchange Subsystem
OW	Orderwire
PC	Personal Computer
PCI	Peripheral Component Interface
PDU	Protocol Data Unit

RAC	Resource Access Control
RF	Radio Frequency
RFI	Radio Frequency Interference
RISC	Reduced Instruction Set Computer
SAFENET	Survivable Adaptable Fiber Optic Embeddable Network
SATCOM	Satellite Communications
SBC	Single Board Computer
SCG	System Control Group
SCSI	Small Computer Standard Interface
SDG	System Distribution Group
SHF	Super High Frequency
SIC	Subscriber Interface Control
SOE	Standard Operating Environment
SPARC	Scaleable Processor Architecture
SPAWAR	Space and Naval Warfare Systems Command
SSC	System/Site Control
STP	Shielded Twisted Pair
TACINTEL	Tactical Intelligence
TAC-4	Tactical Computer-4
TADIXS	Tactical Data Information Exchange Subsystem
TCC	Tactical Command Center
TCP	Transmission Control Protocol
TDMA	Time Division Multiple Access
TP4	Transport Protocol - Class 4
TRANSEC	Transmission Security
TRE	TADIXS Receive Equipment
TTY	Teletypewriter
UTP	Unshielded Twisted Pair
VICS	VME Integrated Communications System
VIGC	VME Interconnecting Group Controller
XDR	External Data Representation
XTP	Express Transfer Protocol
UDP	User Datagram Protocol
UHF	Ultra-High Frequency
UNIX	*A computer operating system in wide use originally developed at Bell Lab*
USCG	United States Coast Guard
VHF	Very High Frequency
VME	Versa Module Europe
WHEC	High Endurance Cutter
WMEC	Medium Endurance Cutter