Advanced Communications Project

Communications System 2010 Intelligent Gateway Design Report

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

By
Ogden Government Services /
SEMCOR Inc. Team

June 1995

FUNCTIONAL DESIGN
FOR
U.S. COAST GUARD
INTELLIGENT COMMUNICATIONS
GATEWAY

February 27, 1995

SECTION I INTRODUCTION AND SUMMARY 1

1.1 SCOPE 1
1.1.1 Overview 1

1.2 SUMMARY 1
1.2.1 Prioritized Intelligent Gateway Requirements 1
1.2.2 Intelligent Gateway Design 3
1.2.3 Candidate User Screens 3

1.3 CONCLUSIONS 3

2.0 INTRODUCTION 5

2.1 TECHNICAL APPROACH/REQUIREMENTS 5
2.1.1 Initial SOW Requirements 5
2.1.2 Initial Architechural Considerations 7
2.1.2.1 *Architecture Considerations - Transport Media* 8
2.1.2.2 *Architecture Considerations - Client/Server* 8
2.1.2.3 *Architecture Considerations - Host Configuration* 8
2.1.3 Intelligent Gateway Workshop 8
2.1.4 Further Requirements from Workshop 9

2.2 ARCHITECTURAL CONSIDERATIONS 12
2.2.1 Client/Server 12
2.2.2 Open Architecture and OSI Standards 12
2.2.3 Minimization of Proprietary Components 13
2.2.4 Database-driven Structured Design 13

2.3 SUMMARY OF DERIVED DESIGN GUIDANCE 14
2.3.1 Gateway Interface Functions 14
2.3.1.1 *Mobile Unit Interfaces* 15
2.3.1.1.1 High Frequency 15
2.3.1.1.2 Air-to-Ground (A/G) 15
2.3.1.1.3 INMARSAT 15
2.3.1.1.4 Voice Communications 15
2.3.1.1.5 Additional SATCOM Systems 15
2.3.1.1.6 Shore Connections 16

2.3.1.2 *Fixed Interfaces* 16

2.3.1.2.1 MDT/PARS 16

2.3.1.2.2 CGDN 16

2.3.1.2.3 PSTN 16

2.3.1.2.4 DISN 16

2.3.1.2.5 STU-III 16

2.3.1.2.6 Sensing and Control 16

2.3.2 Communications Controllers 16

2.3.2.1 *Fault Tolerance* 17

2.3.2.2 *Additional Message Processing* 17

2.3.2.3 *Intelligent Routing* 17

2.3.2.4 *Message Handling* 18

2.3.2.5 *Message Queuing* 18

2.3.2.6 *Message Archiving* 18

2.3.2.7 *Inter-CAMS Link* 18

2.3.2.8 *Databases* 19

2.3.2.9 *Operator Interface* 19

2.3.2.10 *Message Logging* 19

2.3.2.11 *Event Handling* 20

2.3.2.12 *Duplicate Detection* 20

2.3.2.13 *Automated HF Link Optimization* 20

2.3.2.14 *RATT Requirements (CAMSLANT is NECOS*) 20

2.3.3 Operator Consoles 21

2.3.4 Unit Interconnection Medium 21

2.4 CONSTRAINTS ON DESIGN 21

2.4.1 Interface Gateway Unit Selection 21

2.4.2 Communications Controller Platform 22

2.4.3 User Interface Platform 22

2.4.4 Interconnection Medium 22

2.4.5 Voice or Video 22

2.5 ASSUMPTIONS FOR BASIS OF TECHNICAL DESIGN 22

2.5.1 Implementation Approach 22

2.5.2 Implementation Priorities 22

2.6 TECHNICAL DESIGN 23

2.6.1 Throughput Considerations 23

2.6.2 High-Speed Transmission Modes 23

2.6.3 Operator Interfaces 23

2.6.4 Internal Interface Medium 24

2.6.5 Redundancy Considerations 24

2.7 INTELLIGENT GATEWAY SYSTEMS DESIGN OVERVIEW 24

2.8 CONTROL AND MANAGEMENT SUBSYSTEM....................................... 26
2.8.1 Communications Control and Management.. 26
2.8.2 Network Planning and Engineering 26
2.8.3 Spectrum Management... 27
2.8.4 Security Management... 27
2.8.5 Network Management.. 27
2.8.6 Network Administration... 28

2.9 INTEGRATED ROUTER FUNCTIONS 28
2.9.1 Message Processing... 29
2.9.2 Message Routing 30
2.9.2.1 *User Profile Tables* 30
2.9.2.2 *Media Profile Tables*.. 31
2.9.3 Message Queuing 31
2.9.4 Message Archiving... 34

2.10 INTERFACES TO MEDIA.. 38
2.10.1 Interworking Functions to Media.. 38
2.10.1.1 *Bulk Encryption*.. 38
2.10.1.2 *Protocol Conversion*.. 38
2.10.1.3 *Control and Status Interfaces*.. 39
2.10.2 RF Media.. 39
2.10.2.1 *HF Transceivers*... 39
2.10.2.2 *SATCOM Transceivers*.. 40
2.10.2.3 *Other RF Media*.. 40
2.10.3 Terrestrial Communications Media.. 40
2.10.3.1 *CGDN*.. 41
2.10.3.2 *Leased-line* 41
2.10.3.3 *Dial-up PSTN* 41
2.10.3.4 *Other Terrestrial Media* 41

2.11 HARDWARE IMPLEMENTATION 41
2.11.1 Host Hardware Platform 42
2.11.2 Physical Port Interfaces 42
2.11.3 Communications Devices 43
2.11.4 Interworking Devices 43
2.11.5 External Off-site Hardware 43

2.12 SOFTWARE IMPLEMENTATION 43
2.12.1 Host Software Platform 43

2.12.2 Host-Resident Software 44
2.12.2.1 *Operating System Considerations* 44
2.12.2.2 *Database Backend* 45
2.12.2.3 *Common Applications/Utilities Library* 46
2.12.3 Specific Software Modules 46
2.12.3.1 *Logical Message Processor* 46
2.12.3.2 *Custom Protocol Adapter* 46
2.12.3.3 *Custom Interworking Services* 47
2.12.4 Logical Interfaces to External Software Processes 47
2.12.4.1 *Interface to MDC Gateway Protocol Adapter* 47
2.12.4.2 *Remote Control of External Devices* 47

2.13 USER INTERFACE 47
2.13.1 Local Operator Console 48
2.13.1.1 *Input and Control Devices*... 48
2.13.1.2 *Alert and Alarm Features*... 48
2.13.2 Remote Operator Terminal Access 48
2.13.2.1 *Windowed Display Screens* 48
2.13.2.2 *Input and Control Devices* 48
2.13.2.3 *Alert and Alarm Features*... 48
2.13.2.4 *Terminal Communications Support Link* 48

LIST OF FIGURES

Figure 1.1-1. Intelligent Gateway Functional Overview 4
Figure 2.1-1. COMMSTA Gateway Concept 6
Figure 2.3-1. Intelligent Gateway Logical Diagram 14
Figure 2.7-1. Intelligent Gateway Logical Diagram 25
Figure 2.9-1. Routing Task 30
Figure 2.9-2. Communications Controller Message Input Task 32
Figure 2.9-3. Message Output Task 33
Figure 2.9-4. Delay Monitor Task 35
Figure 2.9-5. Archive Task 36
Figure 2.9-6. Message Delivery Cost Reduction Analysis 37

LIST OF TABLES

Table 1.2-1. Required IG Functions 2

APPENDICES

Appendix A Acronyms A-1
Appendix B User Interface Sample Screen Views B-1

SECTION I INTRODUCTION AND SUMMARY

1.1 SCOPE

This report documents the functional design of hardware and software components necessary to satisfy the USCG requirements identified for an Intelligent Gateway (IG). The IG will transfer messages from USCG shoreside networks to transmission paths serving mobile users. In a similar manner, messages from mobile users will also be routed by the IG to shoreside networks. Figure 1.1-1 illustrates the IG functions. This document identifies candidate operating systems and hardware platforms, but as a functional design, does not specify a particular configuration of either. Based on additional USCG input on a preferred operating system or available government-off-the-shelf (GOTS) hardware, a detailed design can be accomplished for a specific operating environment. Furthermore, this IG design focuses primarily on the gateway functions as they pertain to record messages and datagrams as opposed to voice, video, or other information transfer modes such as File Transfer Protocol (FTP) or client/server data networks.

1.1.1 Overview

Detailed requirements for the IG are discussed in section 2.1 along with architectural considerations identified in the USCG Statement of Work (SOW). Additional considerations are developed in section 2.2 followed by derived design guidance (2.3), design constraints (2.4), assumptions (2.5), and other technical considerations (2.6). The IG functional design is described in sections 2.7 through 2.14 to include the control and management subsystem, router functions, media interfaces, candidate hardware and software, and the user interface. Appendix B includes prototype user interface screens for some of the major IG functions.

1.2 SUMMARY

1.2.1 Prioritized Intelligent Gateway Requirements

A number of sources have contributed to understanding the body of requirements for the design of the USCG IG which include the USCG SOW, CAMS Workflow Analysis (CDRL A001), the IG workshop held in December 1994, and technical discussions with USCG representatives. It became clear during these discussions, particularly during the IG workshop, that the initial IG design effort should concentrate on the automated handling of record messages. Within that broad guidance, the required functions of the IG as stated in the USCG SOW were prioritized with respect to their influence on this initial functional design. Table 1.2-1 lists these functions and the relative importance each had on this initial design.

Table 1.2-1.   Required IG Functions

REQUIRED IG FUNCTION (USCG SOW)	RELATIVE PRIORITY AND INFLUENCE ON THIS FUNCTIONAL DESIGN
Information Classification	High
Message Type (ACK/NAK, POSREP, Text)	High
Distant End Comms Capability	Medium
Message Format (voice, data, video)	Low
Mobile Unit Location	Medium
Error Rate of Transmission Channel	Low
LPI/LPD Considerations	Low
Message Priority	High
Circuit Availability	High
Message Length	Medium
IG Reliability	High
IG Cost	Medium
ACK/NAK Required	Low
Modular Construction for ease of Technology Insertion	High
User and Media Profile Database	High
Encryption and Digital Signature Stamp	Medium
Data Compression	Low
Routing Based on Message Content	Medium
Routing Based on Arriving Comm Link	Low
Routing Based on Destination	High
Comm Link Sensor Input to IG	High
Mobile User POSREP and COMMSTATREP	High

1.2.2 Intelligent Gateway Design

Media interface units (hardware and software conversion devices) will interface current messaging sources in the CAMS to the IG, and will interface the IG to transmit paths such as CGDN, dial-up modems, HF radio, INMARSAT services, and the CAMS local area network. Control and status interfaces to the IG will provide configuration status and management of resources. The IG performs rule-based message routing with manual override capability. A database containing mobile user and media profile information is updated in near-real time as parameters change and are reported to the IG communications controller. The user interface provides easy interpretation of primary IG functions and is the focal point for advisory information and alarms.

1.2.3 Candidate User Screens

Appendix B contains a number of prototype user screens for some of the main IG functions (output message queue status, message routing status, OPS NORMAL message status, OPS NORMAL message overdue, etc).

1.3 CONCLUSIONS

The functional design presented in this report satisfies the stated requirements for a USCG Intelligent Gateway within the assumptions and constraints identified. A follow-on task is necessary to complete the detailed design.

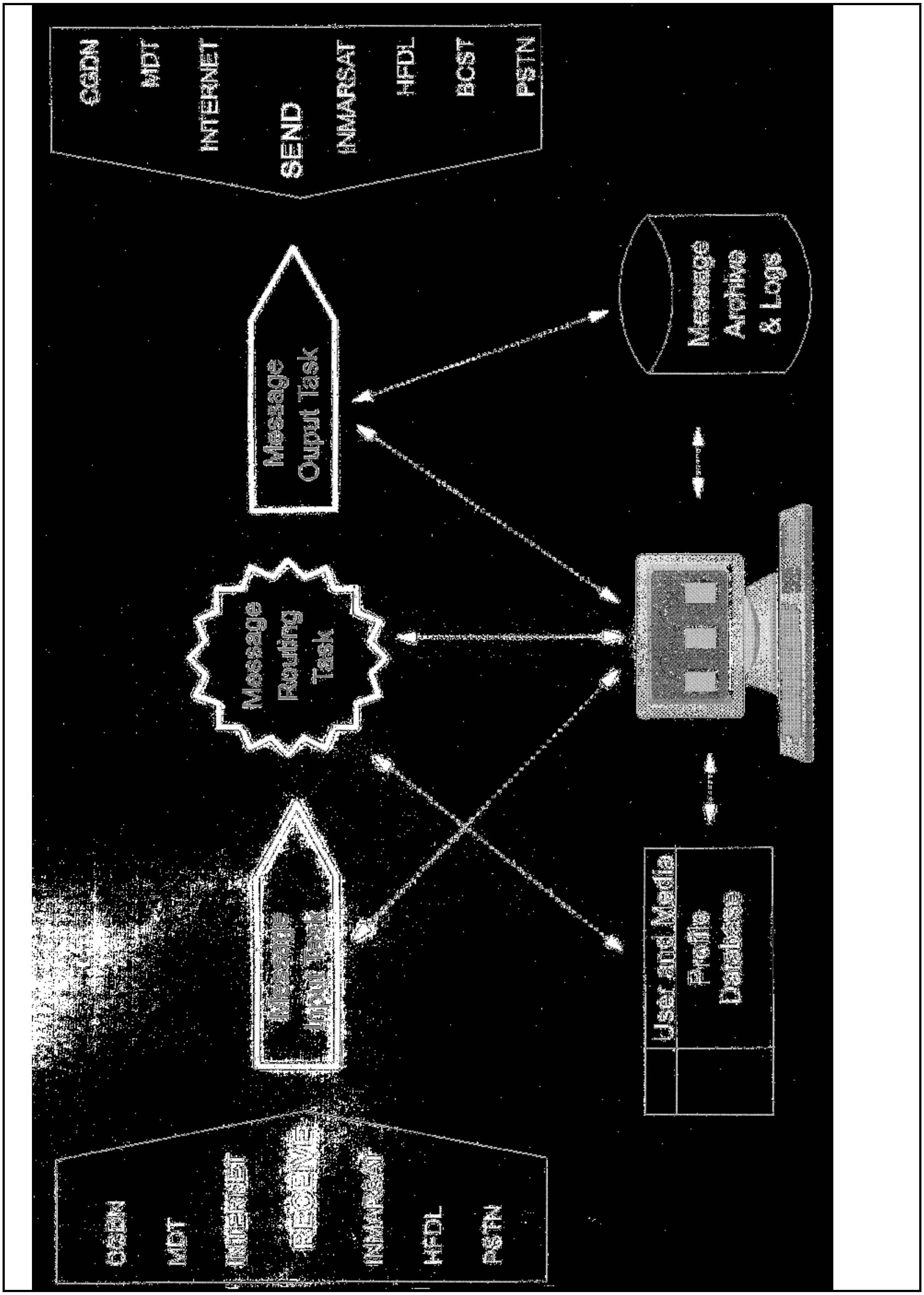


Figure 1.1-1. Intelligent Gateway Functional Overview

SECTION II INTELLIGENT GATEWAY DESIGN

2.0 INTRODUCTION

2.1 TECHNICAL APPROACH/REQUIREMENTS

2.1.1 Initial SOW Requirements

Guidance from the original Statement of Work was to design an "Intelligent Gateway" residing at communications stations that automatically routes information among RF links and shoreside networks. The workshop developed detailed gateway requirements that were to be documented.

The following diagram, figure 2.1-1, shows the selection of RF media on the left and the shoreside networks on the right. The intelligent router function is one of the center blocks within the overall gateway design.

Documented required functions of the intelligent router provide for routing of voice, data, and video information based upon a list of user parameters. These parameters include the following:

- Classification (security required)
- Type (position reports, e-mail,standard message, etc.)
- Recipient comms capabilities
- Message format (digital voice, data, real-time video, etc.)
- Location of mobile unit
- Error rate of channel (quality of service)
- LPI/LPD considerations
- Message priority
- Circuit availability
- Message length
- Reliability
- Cost
- ACK/NAK required or not

Additional Intelligent Gateway requirements extracted from the Statement of Work follow:

a. Modular construction to allow for technology insertion. Each communications link (RF or shoreside network) will be described by a configuration file of parameters. The system will allow for new modules to be added and old ones to be deleted as technology changes.

b. The system will include encryption, data compression, and digital signature stamp.

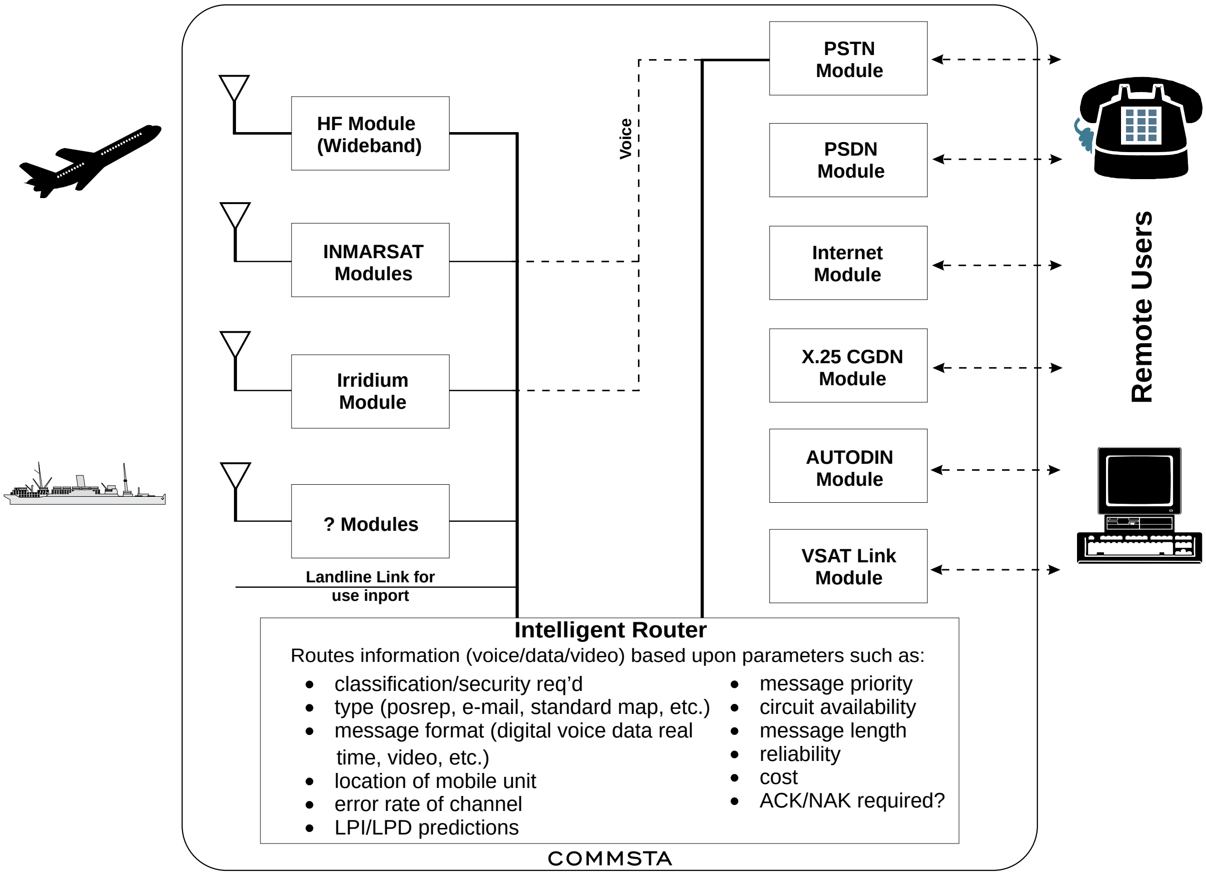


Figure 2.1-1. COMMSTA Gateway Concept

c. The heart of the gateway system is the "intelligent router," which routes the information (voice/data/video) based upon parameters available from the content of the message, the communications link the message arrives on, and the destination of the message.

d. The system will include sensor input to identify when communications links are down. Also, the system will receive "status" packets from mobile users, periodically giving the mobile unit position and communications systems status.

e. The system will maintain a database of mobile units with information such as name, unit type, position, communications links available, and other information to be determined. The system will also update this database as the status packets described above are received.

As part of the Intelligent Gateway design, a prototype user interface will be produced including candidate computer display screens that can be used to evaluate the effectiveness and user-friendliness of the interface design. We will produce a technical report documenting the gateway design.

2.1.2 Initial Architectural Considerations

The workshop discussed the generic ISO model and how it applied to the Intelligent Gateway prototype the Coast Guard desires to be designed, prototyped, and demonstrated. We discussed that a gateway, strictly and classically defined in the seven-layer ISO model, is any combination of software and hardware that performs a translation, simplex or duplex, between two dissimilar data streams above the ISO/OSI Network Layer Three, or packet level. A router is distinguished by doing a similar job at, but not above, the Network Layer. There is probably no vendor remaining in modern gateway technology today, however, that still markets products limited only to that definition. Even the simplest router product is now thought of as making routing decisions based upon message content which is a function well above Layer 4 in the seven-layer ISO model.

Modern gateway technology is, at a minimum, a simultaneous multiprotocol software product, with full duplex synchronous and/or asynchronous modes and a myriad of user-configurable parameters that enable a wide array of features to be added, modified, or deleted. Most gateway products are available as a turnkey, hardware-hosted rack-mounted product form factor with all the appropriate Physical and Link Layer interfaces totally integrated with Network Layer functions.

In addition, "smart" gateway products embody a wide range of Layer 4 through 7 features, either as custom-tailored limited-purpose products or as comprehensive communications environments providing a complete network solution to all foreseeable user needs today and embodying expendability for the "future."

The term "Intelligent Gateway" has been used increasingly as a term referring to the generic integration of a range of specific gateway system and subsystem products together with a comprehensive control and management system. Such gateways can include modular expansion capabilities for the foreseeable future and a relatively easy to use operator interface that maximizes automation of otherwise repetitive or unnecessary human intervention. They maintain and update status information on available communications pathways and use this information when routing messaging and choosing virtual circuit connections for data streams and voice.

Almost every major communications product vendor now advertises one or more Intelligent Gateway solutions for conventional data, voice, and video communications. They combine specific gateway, router, and host software and hardware products in a multitiered architecture embodying in practice many gateways and routers between "standardized" subsystems, and interworking devices designed to provide specific interfaces to "non-standard" equipment or system elements.

2.1.2.1 *Architecture Considerations - Transport Media*

Available communications links are the principal limiting factor in any system design. With increasing availability of fiber for terrestrial interconnects, this concern is rapidly diminishing for all but the mobile user. The mobile user faces the problem of mobile data rate needs growing at a much faster pace than the availability of mobile communications spectrum. Virtually all mobile communication is via existing allocated radio spectrum, and both physics of propagation and available RF technology limit available RF spectrum. From a standardized perspective, anything below 9600 bps is considered extremely low speed and presents special problems for networked communications. The range from 9600 bps to 56 kbps is considered low speed, and network designs embody limited ITU-T X.25 standards for packet communications. The range from 56 kbps to the 1.544 Mbps or 2.048 Mbps rates are considered medium speed and utilize frame relay techniques; anything above this is considered high-speed data and is a candidate for both frame relay and forthcoming ATM standards.

2.1.2.2 *Architecture Considerations - Client/Server*

Although centralized processors and dumb terminals, variously termed mainframes and minis, are still widely used, any serious new Intelligent Gateway design must be based upon modern modular client/server architecture. This architecture matches the current world where processors and processing power are inexpensive and easily distributed. Most elements of the design can be, and usually are, hosted in separate microcomputers. Servers handle most centralized communications, database, and file storage. Client machines handle user interface needs and constitute the majority of end-user information sources and sinks. Interworking processes, providing modular interfaces, are either hosted on one or more shared processor platforms, or in stand-alone closed architecture hardware optimized for specific dedicated functions.

2.1.2.3 *Architecture Considerations - Host Configuration*

With the rapid convergence of microcomputer operating systems toward either true or pre-emptive multitasking, most gateway software processes may be run simultaneously on low-cost PCs. With the rapid increase of CPU power and relative low cost of workstations today, the same overall architecture is equally applicable to UNIX, Windows (3.1, NT, etc.), OS/2, and Macintosh. Since most development environments are multiplatform already or will be within the year, it is safe to assume that the use of a multitasking host or group of host machines will have a small impact, in terms of hardware and operating system cost, on an overall system cost component. Interfaces for TCP/IP, mobile IP, SNMP, and the various ITU-T standards are uniform across all these platforms. Performance is far more than adequate across all these platforms.

2.1.3 <u>Intelligent Gateway Workshop</u>

SEMCOR, Inc. hosted COMMSYS 2010 Workshop #2 on 19-20 Dec 1994 for representatives of the Coast Guard R&D Center, Coast Guard Headquarters, COMLANTAREA, COMPACAREA, TISCOM, and Ogden Government Services. The purpose of the workshop was to acquire a more specific definition of requirements for the design of the Coast Guard Intelligent Gateway, noting that the specific design of the Gateway would not be performed until after this workshop was concluded.

The workshop gave Coast Guard participants an orderly presentation of preparatory information, each section of which built upon the prior section, so that by the end of the workshop each participant had formulated those requirements most important in that participant's area of interest. Recommendations for requirements were then discussed and tabulated at the end of the workshop in real-time.

As the workshop progressed, the participants generated a sheet of candidate requirements, line-by-line, until the last section of the workbook was covered. During the last day, this list of candidate requirements was discussed in detail and prioritized in paragraph 2.1.4 below.

2.1.4 Further Requirements from Workshop

The following fifteen areas of requirements are further amplification of Intelligent Gateway requirements agreed upon by Coast Guard attendees present at workshop #2. The workshop requirements add to the initial requirements included in the section 2.1.1. Where those requirements conflict the following requirements supersede those requirements listed in section 2.1.1 as they represent the latest task directions from the C.O.T.R. and other responsible Coast Guard representatives attending the workshop.

In journalistic fashion, what follows is the exact text of the written guidance from the workshop, and as such it is abbreviated. A full text interpretation is found in this document in section 2.3 as derived requirements.

The following are the prioritized list of Intelligent Gateway (IG) requirements validated by workshop #2:

- Transactions
  - — The IG must log all transactions, including all transmitted messages, and received messages.

- Alarming
  - — The IG must provide exception ALARMS when a transaction cannot be completed, based on RULE-BASED intelligence. Requires maintaining a DB of:
    - -- unit profile example: transmission path inoperative
    - -- media profile example: transmitter inoperative, crypto won't synch, landline inoperative

- Unit database profile
  - — mobile - includes location, equipment DB
  - — shore - includes HF transmitter, HF receiver, SATCOM DB

- Check for duplicates and notify operator if found
  - — same DTG (date and time group)
  - — same originator
  - — same subject line
  - — same SSIC (except ZDK, ZFD, ZFG, ZEL, ZDS)
  - — finally, do a File Compare (an ASCII code comparison)

- Notify operator if flash traffic (Z). Alarm if not delivered (within 10 minutes).

- Notify operator if emergency traffic (Y) (flash override) or flash (Z)

- Automatic OPS NORMAL capability from aircraft. Fixed wing must report OPS NORMAL each 30 minutes; position each 60 minutes. Helos must report OPS NORMAL each 15 minutes; positions each 30 minutes.
  - — must be secure-capable (85 percent of workload)
  - — for helo:
    - -- 1 minute late (Yellow screen/alarm): recontact procedures; call A/C immediately.
    - -- 3 minutes late/no contact (Red Screen/alarm): Notify Air Station - (provide last position). Use recontact procedures. Provide emergency situation (alarm handling).

- Solve High Frequency Data Link (HFDL) problem of monitoring backlog and clearing of messages to small units, e.g., WPB (110-foot patrol boats) and WLB (buoy tenders):
  - — generate alarm if queue backs up past a <TBD> depth
  - — route messages via an alternate means

- Network Control requirements - include the following:
  - — status of equipments, via an equipment matrix with alarms for downed paths
  - — status of terrestrial nets, such as FTS 2000 control, line states, remote key lines
  - — alternate message route initiation
  - — tasking for estimated link and equipment setup
  - — routing database update
  - — automated “best frequency, best transmitter location” system, an automated Prophet or chirp sounder method calculation
  - — automate the setup for OTAR, OTAT messages - which location, transmitter, path
  - — alarm clock that prompts operator for OTAR, OTAT (but actual rekeying is done outside the IG)

- Phone Patch (unclassified) - not done in Prototype IG; IG built modularly to accommodate voice in future.

- Phone Patch (classified) - not done in IG; IG built modularly to accommodate voice in future.

- Secure Voice Network - not done in IG; IG built modularly to accommodate voice in future.

- Manual Intervention
  - — all automated processes have a manual override
  - — list chronologically all automatic processes
  - — in transaction log, include hours usage on each transmitter by frequency for HF transmitters, to lengthen life of final PA tubes. Keep this info in media profile for use in selection process of best frequencies and best transmitter site.

- Satellite RATT requirements (CAMSLANT is NECOS)
  - — need alarm and window for remote operator to initiate a TTY contact
  - — terminal-to-terminal window
  - — message receive mode
  - — message send mode
  - — format and spellcheck, perform PLAD check (have an “add” function in dictionary), provide operator with selective on/off of spell checking by media or msg-by-msg
  - — force always checking of PLADs and format
  - — all messages are archived by IG for 30 days
  - — have an operator-to-operator buffer
  - — parallel processing - good messages can move on while bad messages are separately shunted aside for bad message handling manually
  - — automatic parsing of individual messages from a group of messages (process 1 file with multiple messages to separate messages)
  - — recognize each individual message (make 1 file per 1 message)
  - — name message files automatically with DTG and more as needed to be unique

- No voice or video is to be included in IG design

2.2 ARCHITECTURAL CONSIDERATIONS

2.2.1 Client/Server

Most modern applications which have a many-to-one correspondence between event-generating processes and an event-processing element use the client-server paradigm. Usually this is implemented as physically separate computers for each of the many clients and the single (or a few) server computer(s). The primary advantage is in selecting the optimum hardware and operating system for each function. Additionally, there may be physically separated clients.

The most commonly encountered client-server applications are the database and file servers. In both of these the clients are workstations, and the events which are processed by the server are ultimately stimulated by the workstation’s human user. The Intelligent Gateway (IG) should use the same paradigm, but the client events and the server processes are specific to its function. In the IG case, the clients are incoming messages or media changing-status events. The messages originate in separate gateways, according to the communications medium. The server process runs in the communications controller, and has several functions, such as queuing, switching, and archiving. One additional advantage of the client-server paradigm for the IG is that it enables the use of redundant communications controllers without requiring the gateways to be redundant. The purpose of this is to avoid a single point of failure for all messages.

The following paragraphs outline the architectural considerations for the Coast Guard IG.

2.2.2 Open Architecture and OSI Standards

To ensure an enduring, reliable, and sound fiscal investment, an open architecture philosophy will be exercised. This will further enable the benefits espoused in section 2.2.1. Specifically, open architecture will empower multiple vendor selection, thereby promoting optimal cost/performance, allowing system evolution (incremental changes with contained impact), and minimizing interfacing and interconnect problems.

Accordingly, all Intelligent Gateway internal interfaces will use Open Architecture hardware and software to facilitate modularity, upgradeability, and object-oriented design.

Hardware and software interfaces and protocols will be examined to ensure the Intelligent Gateway internal interfaces are open architecture implementations. The following are examples of the various aspects to be considered.

- Communications protocols, e.g., Ethernet (IEEE 802.3), TCP/IP, X.400
- GUI Application Interfaces, e.g., MOTIF, Windows SDK
- Hardware Interfaces, e.g., 10-base-T, RS-232, VME bus

2.2.3 Minimization of Proprietary Components

The modular distributed processing client/server architecture outlined in section 2.2.1 and the open architecture outlined in section 2.2.2 facilitate partitioning elements that have COTS sources. For instance, gateways are mainly available as COTS, but lack required quality of service capabilities. This and other IG-related services are provided by the communications controllers. The open architecture will also facilitate the availability of COTS software, e.g., protocol stacks, libraries, Remote Procedure Calls (RPCs), and Terminate and Stay Resident (TSR) processes.

The open architecture approach is best implemented by a common Local Area Network (LAN), using the same protocol for all units. If a desired COTS interface gateway unit is not available with the selected LAN interface, it may be interfaced via a COTS protocol converter.

2.2.4 Database-driven Structured Design

A database-driven structured design will reduce software development costs by reading required routing parameters from databases. This paradigm will decouple the implementation from the design by avoiding changes to the communications controller source code when upgrading the hardware. Also, use of databases will allow the separation of the following functions: acquisition of status data for the operator; interface; communications control; and updating status data from facilities/media management.

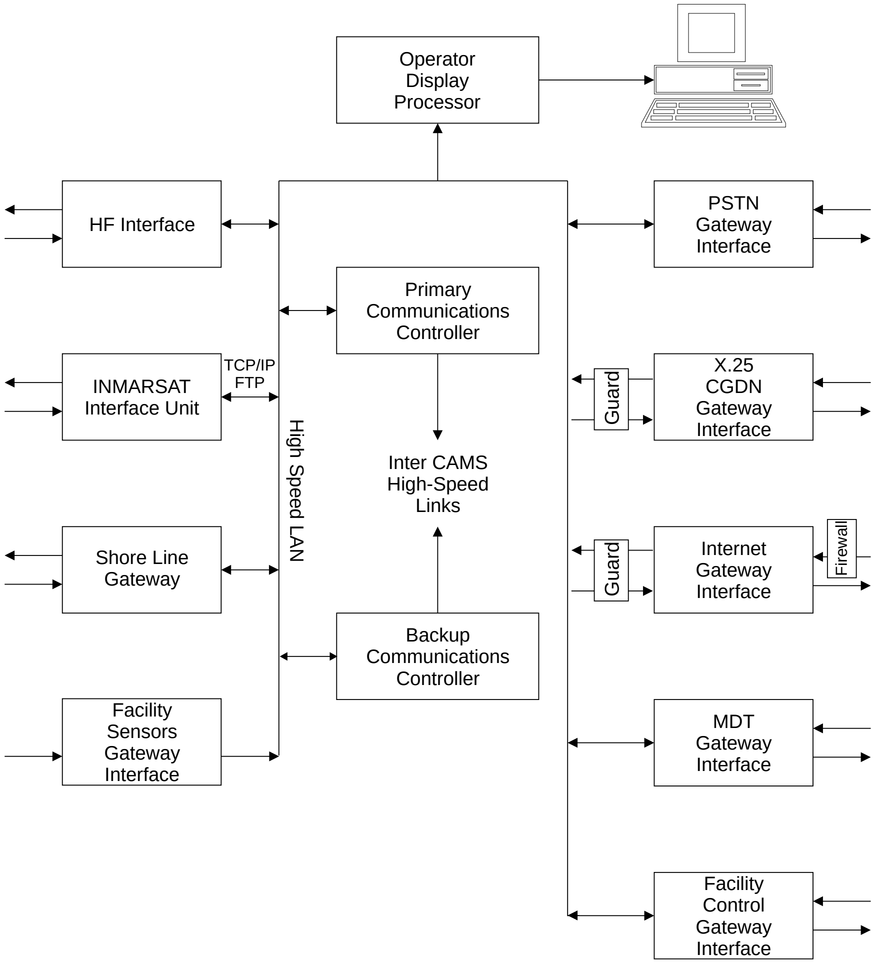
The different relative types of databases include configuration, status, and message statistics. Configuration databases are relatively static and only change if hardware changes. Status databases are relatively dynamic and are used to track media changes, user changes, equipment, and channel availability. Message statistics databases track numbers of messages, originators, etc., in daily and monthly periods.

A different type of information which may be amenable to codification as a database concerns the rule-based criteria for intelligent routing. In addition to routing decisions based upon available channels, a rule-based approach may implement routing decisions based upon cost or policy. When a rule is implemented as a database parameter, rather than a hard coding, it may be changed at run time according to circumstances beyond the capabilities of an automatic system.

Appropriate database implementations will be considered and implemented, e.g., stand-alone application on a database server computer, with the communications controller as client; separate task, process or thread in a multitasking communications controller; static or dynamic class or structure objects in the communications controller software.

2.3 SUMMARY OF DERIVED DESIGN GUIDANCE

The following is an indexed summation of requirements from the IG workshop and as was described in section 2.1. Please refer to figure 2.3-1 which illustrates the logical arrangement of the Intelligent Gateway components.



Operator Display Processor
HF Interface
INMARSAT Interface Unit
TCP/IP FTP
Shore Line Gateway
Facility Sensors Gateway Interface
High Speed LAN
Primary Communications Controller
Inter CAMS High-Speed Links
Backup Communications Controller
PSTN Gateway Interface
Guard
X.25 CGDN Gateway Interface
Guard
Internet Gateway Interface
Firewall
MDT Gateway Interface
Facility Control Gateway Interface

Figure 2.3-1. Intelligent Gateway Logical Diagram

2.3.1 Gateway Interface Functions

The IG shall provide interface devices, generically termed gateways, for mobile units, fixed stations, and inter-CAMS communications. These interfaces shall be modular units with standard, open architecture internal interfaces to the communications controllers and the media. Generally, each interface gateway unit shall provide ports for multiple channels of a common media. It shall provide support for the unique external protocols indigenous to the media and a limited amount of FIFO buffering.

Input and output channels would be used for remote control and status sensing of physical resources. This would be for devices that require individual signals, rather than a RS-232 digital signal, or packets embedded into a communications channel, such as SNMP packets. In some cases a communications interface may provide signals for its associated attached devices, and would not need the capabilities of a separate interface unit.

2.3.1.1 *Mobile Unit Interfaces*

The following classes of interfaces shall be provided for communications with mobile units:

2.3.1.1.1 High Frequency

The HF interface gateway unit shall provide control and status capability for remotely situated transmitter and receiver sites. Automatic Link Establishment (ALE) shall be supported with communication controller assistance. This unit shall accommodate HFDL/IHFDL and High Speed Fleet Broadcast (HSFB). The HSFB shall provide serial broadcast, which is configurable to meet dynamically changing afloat user requirements. The interface shall provide, or be connected to, high-speed HF modems for ship/shore/ship tactical requirements.

2.3.1.1.2 Air-to-Ground (A/G)

Aircraft may be equipped with an INMARSAT-C terminal together with a GPS receiver for automated A/G OPS NORMAL reporting. If this is implemented then an interface shall be provided to the INMARSAT ground station, which shall receive these messages and automate logging and alarming according to established criteria.

2.3.1.1.3 INMARSAT

An interface shall be provided to connect with the INMARSAT ground terminal. The interface shall accommodate both RATT and voice-band data (using a modem). Data shall include single (immediate) messages, multiple-queued messages, and interactive (virtual circuit). Full duplex shall be exploited in non-interactive mode to provide concurrent transmission of independent data messages in both directions.

2.3.1.1.4 Voice Communications

The IG shall accommodate voice and facsimile communications switching using an existing COTS PABX system. An interface shall be provided to connect with this system for parametric control and status reporting.

2.3.1.1.5 Additional SATCOM Systems

The IG design shall accommodate the addition of modular interfaces for SATCOM systems not currently implemented for CG use.

2.3.1.1.6 Shore Connections

Interfaces shall be provided for in-port use via PSTN/PSDN.

2.3.1.2 *Fixed Interfaces*

The following classes of interfaces shall be provided for communications with landlines:

2.3.1.2.1 MDT/PARS

AUTODIN service shall be accommodated by an MDT interface.

2.3.1.2.2 CGDN

An X.25 interface shall be provided to the CGDN.

2.3.1.2.3 PSTN

An interface shall be provided to the PSTN. Modular, multiple, and alternative interface types shall be accommodated as required, including 2-wire dialup. 4-wire leased, Fractional T1, DSS, or ISDN.

2.3.1.2.4 DISN

A data interface shall be provided to the FTS 2000 network in the event that the Coast Guard has a requirement to use the FTS 2000 instead of, or in addition to, the CGDN.

2.3.1.2.5 STU-III

An interface shall be provided to multiple dial-up STU-IIIs.

2.3.1.2.6 Sensing and Control

This interface provides external analog and digital input and output channels for remote control and status sensing of physical resources. This would be for devices that require individual signals, rather than a RS-232 digital signal, or packets embedded into a communications channel, such as SNMP packets. In some cases a communications interface may provide signals for its associated devices, and would not need the capabilities of a separate interface unit.

2.3.2 <u>Communications Controllers</u>

Communications controllers provide message handling, intelligent message routing, message queuing and archiving, database services, monitoring, and control.

2.3.2.1 *Fault Tolerance*

Two redundant communications controllers shall be used to minimize the possibility of losing complete functionality of a CAMS. The failure of one controller shall not result in the loss of or mishandling/routing of any message. Recovery shall not require manual intervention or significant delay in transmission. Each controller shall be able to access up-to-date system status information. Each controller shall have its own copy of the message queues. Precautions shall minimize the probability of message duplication during normal operation.

2.3.2.2 *Additional Message Processing*

The communications controllers shall provide any necessary processing required in the interface for a specific message class. An example is the provision of channel cost minimization (for an INMARSAT-type output interface) as describe in paragraph 2.9.4, with cost benefits illustrated in figure 2.9-6. This processing shall apply to both incoming and outgoing messages.

2.3.2.3 *Intelligent Routing*

The heart of the IG is the "intelligent router," which routes messages based upon parameters available from the content of the message, the communications link the message arrives on, and the destination of the message.

Documented required functions of the intelligent router provide for rule-based routing of messages based upon a list of user parameters. These parameters include the following:

- Classification (security required)
- Type (position reports, E-mail, standard message, etc.)
- Recipient comms capabilities
- Message format (digital voice, data, real-time video, etc.)
- Location of mobile unit
- Error rate of channel/quality of service
- LPI/LPD considerations
- Message priority
- Circuit availability
- Message length
- Reliability
- Cost
- ACK/NAK requirement.

Appropriate modes of operation may be provided to modify the application of the rules manually by operator selection, or according to system status such as queue lengths.

2.3.2.4 *Message Handling*

The incoming messages may be directly routed between the interfaces involved, or pass through the communications controllers. If the nature of the communication is a permanent or virtual circuit, then the routing is direct. Typically, this would be an interactive application. The function of the communications controller for this case is to set up and disconnect the circuit, including the path internal to the IG and external circuit setup via the required interfaces, as necessary. All other messages are internally routed via the communications controllers.

2.3.2.5 *Message Queuing*

The interfaces typically provide internal queuing of messages of their own class for the purpose of minimizing the probability of data loss resulting from the application of hardware or software flow control on either the external or internal interfaces. The use of queuing at the interfaces shall be minimized to this function since such queuing is not aware of the global communications situation.

The communications controllers shall maintain separate incoming message queues for each priority, with additional queues if necessary to implement the routing rules. Each output channel shall have a separate message queue to prevent blocking of all channels if one channel is down. These shall also be separated by priority. These queues shall be of such capacity as to minimize the probability that they will be filled during peak traffic periods. Expansion of queue capacities by hardware enhancement shall be facilitated in the software.

The communications controllers shall periodically monitor the reserve capacity of each message queue. If the reserve is too low, and there are many uncompleted messages which cannot be archived, then an event shall be generated. If appropriate, such as the case of backlogged HFDL messages to small units, rule changes may be automatically invoked to route the backlogged messages via alternate, more expeditious, means.

2.3.2.6 *Message Archiving*

Messages which are routed via the communications controllers and which have been transmitted to the external destination shall be efficiently stored on permanent media at intervals which minimize the probability of filling message queues. Purging of these stores, or transfer to off-line media, shall be based on policy rules, which may be manually overridden by an operator. The communications controllers, upon operator demand, shall be capable of recovering specific on-line or off-line archives for retransmittal, viewing, transfer to off-line media, or printout. The communications controllers, upon operator demand, shall be capable of transferring specific on-line archives to off-line media.

2.3.2.7 *Inter-CAMS Link*

Each communications controller shall have a direct and (physically and logically) independent communications channel to the alternate CAMS IG for message transfer and database synchronization.

2.3.2.8 *Databases*

The communications controllers shall have access to, or incorporate, database elements that codify all non-intrinsic numerical parameters. For example, the databases shall include all hardware configuration parameters which could change according to unit complement, source selection, connection allocation, setup selections, or upgrade status.

If any given routing rule (such as a rule to perform minimum-cost routing) can be numerically parameterized, and is subject to change by policy or operator command, it shall be implemented as a database element.

Additional databases shall contain dynamic information which shall be updated promptly as values change. Included shall be local and remote hardware and communication channel status, message handling, queuing, archiving, and routing parameters, and modes and parameters of operation, whether selected according to rules or by operator command.

The division of information into tables or other forms of storage shall be optimized with respect to content, correspondence to physical or logical entities, speed of access, and implementation convenience. To the maximum extent possible, database content shall be loaded at boot time. Changes to dynamic information shall be checkpointed into permanent storage periodically, and transmitted to the alternate CAMS via the inter-CAMS link.

2.3.2.9 *Operator Interface*

Each communications controller shall provide a logical interface to one or more operator stations. Through a standard protocol, this logical channel shall provide access to database information and messages. Changes to database values shall be made via this interface only as permitted by an authorized access list, that identifies items and operator groups. This interface shall also permit the operator to archive and restore message queues and to manipulate archived records of messages, in accordance with security criteria. The operator may also have read-only access to the live message queues as limited by security criteria. The design of the communications controller shall preclude the loss of any message due to operator action.

2.3.2.10 *Message Logging*

A log of all message transactions shall be maintained. Transaction logs shall be permanently archived periodically. Each entry shall include header information, time stamps, message classification, type, length, and disposition. The entry shall be initiated when the message is received, and updated when forwarded or otherwise handled. At the time of reception the message type shall be checked for special logging. Flash messages shall be additionally entered into a special Flash message log, which is checked at least once per minute for excessive delay. Upon completion, the entry is deleted from the special Flash message log (not from the transaction log).

All aircraft OPS NORMAL and position reports shall be additionally entered into a special log. This log is checked periodically for excessive time since the most recent entry for each active flight. At the successful conclusion of a flight, the entries for that flight shall be transferred to a separate archive.

2.3.2.11 *Event Handling*

The communications controllers shall automatically log events and forward them to each operator station. Events generally shall include alarms which should result in manual intervention. Events shall be time stamped. Specifically included are:

- Hardware faults
- Alarm clock that prompts operator for OTAR, OTAT (but actual rekeying is done outside the IG)
- Downed channels
- Overdue aircraft OPS NORMAL reports
- Flash messages and delayed flash messages.

Modes of operation may provide for several grades of event criticality which may be selected by the operator within limits. The operator shall be provided with the capability of generating event messages of arbitrary format and length.

2.3.2.12 *Duplicate Detection*

Each message transaction logged shall be compared with previous entries in the log file. If an identical entry is found, an event shall be generated for operator review.

2.3.2.13 *Automated HF Link Optimization*

The communications controllers shall automate a “best frequency, best transmitter location” system, and an automated Advanced Classic Prophet or Chirp Sounder method calculation. They shall also automate the setup for OTAR and OTAT messages as to location, transmitter, and path. Execution of the setup shall use the HF interface, or the sensing and control interface, whichever is the most economical. The HF transmitter setup shall be cognizant of hours usage on each transmitter by frequency for HF. This information shall be kept in a media profile for use in selecting the best frequency and the best transmitter site.

2.3.2.14 *RATT Requirements (CAMSLANT is NECOS)*

The controller shall buffer RATT signals. Order wire and net control communications shall be diverted to a window on the operator workstation. Facilities to be provided to the operator shall include:

- Alarm on contact initiation
- Terminal-to-terminal communications
- Message receive mode
- Message send mode.

The controller shall provide the following additional functions for RATT messages:

- Perform format check
- Perform PLAD check
- Divert bad messages to the operator
- Automatic parsing of individual messages from a group of messages.

2.3.3 Operator Consoles

The IG shall be equipped with physically or logically independent operator interface processing units or processes. These shall be modular to facilitate expansion. Each operator interface shall be logically interfaced using a standard interface to the communications controllers. The operator may select either of two controllers, or view and control both concurrently in a windowed environment. In this latter case, selection of the communications controller shall be by focus.

2.3.4 Unit Interconnection Medium

The media interface units, the operator interface units, and the communications controllers shall be interconnected by a common standard medium using standard protocols. Generally, this common medium shall be used for all types of digital data. If in specific cases, a unit cannot be economically procured with the common interface, this unit may be directly connected to the communications controllers using an alternative standard point-to-point interfacing method.

The common medium shall not have a sinlge point of failure and shall be capable of direct transmissions between any two connected units. Redundancy shall be provided as required to maintain a high level of IG availability. The capability of the medium shall be sufficient for current peak message loading, with substantial reserve or upgrade capability, without significant design changes to any unit.

2.4 CONSTRAINTS ON DESIGN

The following constraints govern practical implementation of the IG:

2.4.1 Interface Gateway Unit Selection

The interface types must be limited to those which are expected to be used by the CG for the foreseeable future. It is expected that a COTS source will be available for each selected interface gateway. If the cost to implement a developmental interface to the IG for a particular type is excessive, and the CG currently uses a reasonably satisfactory implementation, then continued use of the present system for that type is indicated for the near future.

2.4.2 Communications Controller Platform

A computer type for the communications controller will be selected using criteria including:

- GFE availability
- Desired operating system ported to the computer
- Desired development environment and LAN library ported to the computer
- Required LAN adapters available for the computer
- Computer type upgrade to substantial increases in message traffic.

2.4.3 User Interface Platform

The computer used for the demonstrating the operator interface will be selected for compatibility with a GUI development system which provides rapid prototyping. This will provide quick and economical revisions to accommodate CG recommendations. The operator interface may be implemented using a more capable and upgradeable computer type. To the maximum extent possible within these constraints, the demonstration implementation effort will be transferable to the implemented system.

2.4.4 Interconnection Medium

A LAN implementation that is compatible with the connected units will be selected. It will be expandable and have an upgrade path for substantial increases in message traffic.

2.4.5 Voice or Video

Patching voice and video signals, whether in analog or digitized form, will be switched by COTS units external to the IG. The IG will interface with these units to the extent necessary to provide appropriate operator displays and control. The extent of IG involvement is strongly dependent on the capabilities of the COTS switches.

2.5 ASSUMPTIONS FOR BASIS OF TECHNICAL DESIGN

2.5.1 Implementation Approach

The SOW requirements will be met by a combination of COTS and development status hardware and software.

2.5.2 Implementation Priorities

In addition to conformance with goals of open systems architecture, selection of the hardware and software elements will be made primarily by total initial procurement cost and reserve capacity and secondarily by development time.

2.6 TECHNICAL DESIGN

2.6.1 Throughput Considerations

While there are several technical issues crucial to successfully implementing an Intelligent Gateway, one aspect is throughput. Since there are several current types of communication protocols to be interfaced, and additional ones may be added in the future, full protocol stacks must be employed. Passing messages through a protocol stack is a heavy user of processor cycles. This design confines any proprietary protocols which accompany legacy external communications channels to individual interfaces. Since each of these units handles only one protocol, they can use a streamlined design which typically employs special-purpose processing elements. Typically, these will be COTS units that benefit from their manufacturer's accumulated experience in a specialized market. While this distributed approach does not avoid all throughput problems for the communications controllers (which must use general-purpose processors), it considerably lessens the impact.

2.6.2 High-Speed Transmission Modes

The Intelligent Gateway requires that practically all messages be passed through the communications controllers. These requirements include intelligent routing, transaction logging, concatenation of messages to reduce INMARSAT communication costs, tracking Flash and OPS NORMAL messages for delay alarms, and operator access. The processing power necessary to handle buffering of the message load is also a concern, but is not critical for current moderate transmission volumes. In general, the external transmission rate is not the main concern, since the messages are buffered in the interfaces. However, high-speed interactive communications are expected to be used in the future. These use virtual circuit instead of datagram protocols. For this mode, the communications controller is only involved during the circuit setup and hangup phases. This design approach, therefore, permits virtual circuit packets to bypass the communications controllers, passing directly between the selected interfaces, thus avoiding what would be an overwhelming load on the communications controllers.

2.6.3 Operator Interfaces

The operator interfaces are the main viewport to the message transaction operations, as well as the status and control of the internal and external resources. It is to be expected that a considerable portion of the development effort will be in this area, and that there will be a period of refinement as experience is gained in the operational use of the Intelligent Gateway. The design uses logically and physically separate workstations to implement the operator interface function. The purpose is to decouple them from the communications control function. The operator interfaces mainly with the databases which drive the communications control function. This configuration has several advantages: changes to the operator interface software are not as likely to impact the communications control function, which may have been already validated; additional operator interface workstations may be added as modules without impacting the rest of the system. If, for any reason, a prototype operator interface has to be used initially in a production Intelligent Gateway, it may be supplemented or later replaced with an advanced model without impacting the rest of the system.

2.6.4 Internal Interface Medium

A Local Area Network (LAN) approach has been selected for the data transmission medium which interconnects the communications controllers, the media interface/circuit units, and the operator interface units. An alternative might be a combination of direct links and a matrix switch for the virtual circuit transmissions. The LAN approach is expected to be easier and cheaper to implement, easier to expand, and may more readily be made redundant. Common types such as 10 Mbps Ethernet and 16 Mbps token ring are adequate for current message loads, but may become inadequate for future high-speed interactive transmissions. However, speed upgrades to FDDI or FAST Ethernet may be easily implemented with minimal software impact.

2.6.5 Redundancy Considerations

The Coast Guard intends to establish two CAMS, one for each coast. If one is down, the other can pick up the load. To allow this, each IG will be updated frequently with the user status tables from the other. In practice, there will be limitations and therefore there are elements of redundancy in this design to minimize the probability of a single hardware failure or software abort from completely halting message flow. The design approach is to provide two redundant LAN media and adapters, and to use the two redundant communications controllers. One way to employ two communications controllers is for one to be a ready or "hot" spare. This would have its dynamic database tables periodically updated from the active communications controller, but would process no messages. The limitation of this approach is that a failure of the active controller will result in the loss of queued messages. The preferred approach is to use parallel or distributed operation. All incoming messages are passed to both controllers and processed, but only one sends the outgoing messages to the destination interface gateway. Both controllers receive the acknowledgments from the destination interface gateway and will maintain identical queues, transaction logs, and dynamic database tables. In order to determine the health and database status of the controllers, the operator workstations will periodically compare the message transaction log databases of the controllers. If the databases differ then the operator will be notified by an alarm.

2.7 INTELLIGENT GATEWAY SYSTEMS DESIGN OVERVIEW

The design described in the following sections satisfies the requirements listed in sections 2.1 and 2.3. The logical arrangement of the major units is illustrated in figure 2.7-1. This shows a Local Area Network that interconnects all major units:

- Media interface units
- Communications controllers
- Control and status interfaces
- Operator workstations.

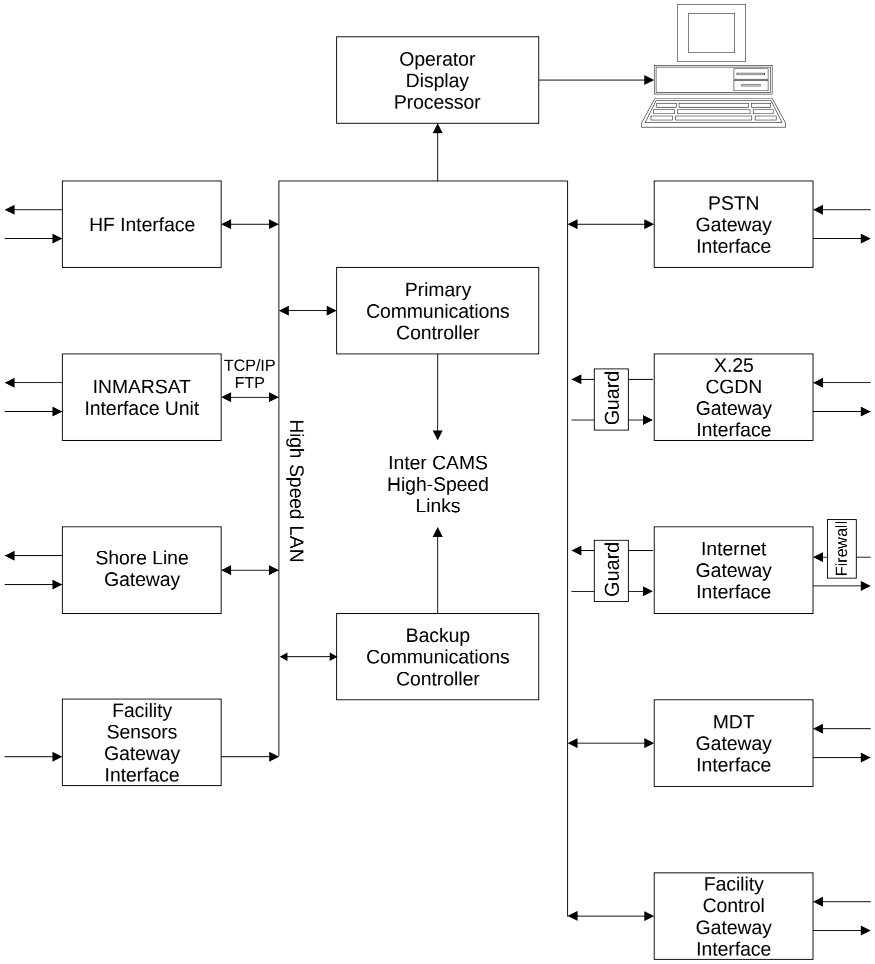


Figure 2.7-1. Intelligent Gateway Logical Diagram

The hardware implementation is described in section 2.11. The actual interface units vary considerably in capability and may consist of more than one physical unit. They are described in section 2.10.

In order to ensure that the LAN has no single point of failure, two redundant LAN media are used. There are also two redundant communications controllers running in parallel. These implement resource control and monitoring, which is covered in section 2.8, and message routing in section 2.9.

Only one operator workstation is shown, but as many as is necessary may be used. The workstations are identical: the operators may divide the workload. The user interface is detailed in section 2.13.

Refer to section 2.12 for software considerations for the Intelligent Gateway.

2.8 CONTROL AND MANAGEMENT SUBSYSTEM

Proper performance of the Intelligent Gateway requires a comprehensive, overall controller function. The controller function is usually distributed, but is summarized on at least one display terminal. For this IG design, this function will reside on the main CAMS operator display screen. However, any desired number of backup control terminals may exist at the user's option, provided a user with control authorization desires to log into a suitably-equipped remote user terminal for remote control and management.

The controller operator interface allows user management of element functions by providing maximal automation of repetitive tasks and alarm notifications, thus freeing the user to control and configure the system quickly and correctly.

2.8.1 Communications Control and Management

The control and management segment, which is the nucleus of the Intelligent Gateway, may be divided logically into five functional elements: Network Planning and Engineering, Spectrum Management, Security Management, Network Management, and Network Administration. These areas are consistent with overall Communications Support Subsystem (CSS) plans within DoD, FAA ATC systems development within DoT, general commercial industrial practice, and they are key to automating the gateway controller.

While the availability of standard interfaces and status databases are necessary to ensure a complete table-based set of status indications to the controller operator, adequate interworking elements may replace the function of standard interfaces for legacy controllable assets not yet equipped with standard interfaces. SNMP is the lowest common denominator for such control. A conceptual definition for each functional element is given below. The design of the intelligent gateway will incorporate each element in detail.

2.8.2 Network Planning and Engineering

Network planning and engineering specifies the set of capabilities to plan and engineer initial, contingency, and follow-on network deployment and operations. It includes non real-time aspects of configuration management including: the operational constructs of communications management domains (the CAMSLANT or CAMSPAC domains, for example), virtual networks, and COMMPLANs. The communications management domain provides the capability for a single platform to manage communications on a set of platforms in an integrated manner. The virtual network provides communications services to users without the user having to be concerned with the physical transmission media used to support the service. Communications planning provides the capability to plan networks and define allowable connectivity among users and allows flexible reconfiguration as often as needed.

The user of the communications service is concerned with the grade or quality of service required, rather than which transmission resource is selected to satisfy the service. Virtual networks are functional and operational information exchange paths that share access to one or more bearer services, the user of a communications service is provided bandwidth from one or more transmission media resources.

2.8.3 Spectrum Management

Spectrum management specifies the set of capabilities to systematically plan, manage, engineer, and coordinate electromagnetic radiation in a manner that supports effective frequency use of the radio spectrum. Some aspects of spectrum management are common regardless of media, and others are media-specific (e.g., aspects of RF propagation and path prediction are frequency-dependent).

Regardless of the platform or media contemplated, example necessary parametric data include platform locations and their projected movement, connectivity and grade of service requirements, preferred RF band usage, available RF components (tx, rx, ant, etc.), frequency range (both generally allocated and specifically available), and any considerations for protection from jammers and direction finders.

Automatic routines will be exercised for spectrum management, particularly frequency selection and antenna/path selection for HF and basic satellite link calculations for setting up paths via satellite as needed. Since existing communication and control routines perform most of the spectrum management functions listed here, those routines would directly integrate into the IG communications controller architecture.

2.8.4 Security Management

Security management specifies the set of capabilities that addresses security essential to using and protecting communications services along with the operating environment. Although automatic in nature, security management defines security-related events to be logged or reported to a manual operator, detecting security breaches, protecting information and devices, supporting security levels, key management and distribution interface, and accessing control requirements.

One example candidate operating system, Windows NT 3.5, embodies powerful multilevel conditional security features. Windows NT utilizes NSA-approved crytptographic devices for in-stream bulk encryption, STU-III devices for dial-up connections, and RSA-key DES software such as Secret Agent, in its message processor.

2.8.5 Network Management

Network management specifies the set of capabilities to control, monitor, and maintain communications services. Network management encompasses fault, performance, accounting, and the near real-time aspects of configuration management. It includes systems communications control, reconfiguration, monitoring, remote operations, alarm handling, logging, near real-time communications service activation, maintenance, and adaption parameter handling requirements. The specific ability to satisfy network management requirements is dependent upon the capabilities of the external interfacing system or interworking device.

Additionally, the selection of a network management product will be based on its functional comprehensiveness. The ease and completeness in implementing the following functions, as described by Harry Newton in Newton's Telecomm Dictionary (1993), is the criterion upon which functional comprehensiveness will be based.

“Network management generally falls into five areas:

1. CONFIGURATION MANAGEMENT deals with installing, initializing, "boot" loading, modifying and tracking the configuration parameters of network hardware and software.

2. FAULT LOCATION and REPAIR MANAGEMENT tools let you find out what's going wrong with what equipment or lines and give you the ability to fix those resources -- by re-routing traffic on different lines or reporting problems to the carrier, or suggesting to whoever that certain equipments should be replaced. Fault location and management tools have strong error and alarm characteristics.

3. SECURITY MANAGEMENT tools allow the network manager to restrict access to various resources in the network. There are devices such as password protection schemes, giving users different levels of access to different network resources.

4. PERFORMANCE MANAGEMENT tools provide real-time and historical statistical information about the network's operation. Such tools show, for example, how many packets are being transmitted at any given moment, the number of users logged into a specific server and use of network lines.

5. ACCOUNTING MANAGEMENT applications help users allocate the costs of the various network resources -- from lines to PBXs, from access to a mainframe to time used on printers.”

2.8.6 Network Administration

Network administration specifies the set of capabilities to define the physical communications equipment environment, the supported communications services, and the means to configure the communications equipment in order to satisfy mission requirements. This includes the capabilities to store and manage network and communications equipment configuration and user service profile information and to generate configuration reports. This configuration information forms the basis for the Intelligent Router decision-making capabilities and the ability to centralize and automate the communications planning process. An editing capability will be provided to build and maintain the configuration tables for the network element components required for operation.

2.9 INTEGRATED ROUTER FUNCTIONS

Most messages which are passed through the Intelligent Gateway technically correspond to datagrams in ISO communications standard terminology. Each message is complete in itself, and includes addressing information. These messages are passed through the communications controllers, which use this addressing information, together with source logical channel information and resource database information, to perform intelligent routing.

Messages are initially processed to demultiplex, as required, parse to extract addressing information, check for validity, and create a transaction. These processes are described in section 2.9.1. The actual intelligent routing is described in section 2.9.2.

Messages are queued on arrival to accommodate peak message loads. This process is described in 2.9.3. When a message transaction is complete, its content is transferred to permanent storage for off-line review and on-line retransmittal in case it was lost after leaving the Intelligent Gateway. This operation is described in 2.9.4. Figures 2.9-1 through 2.9-5 illustrate the logical design of the router.

2.9.1 Message Processing

Messages require processing at several stages. The first step checks for validity. Incoming messages will be demultiplexed if rule-comparison indicates the packet may contain multiple messages. Normally, demultiplexing is performed in the interface units but could be a communications controller function.

After demultiplexing, the individual messages are initially parsed to determine their classification and priority. Different priorities are separately queued, which may also take into account the type of message, the channel it arrived from, and the source and sink identification, according to operational mode and rules. At this time a transaction record is created that includes the following:

- Header information
- Source interface channel
- Current time timestamp
- Message length
- Queue identification
- Message type
- Destination interface channel
- Priority
- Classification

Identification of the record's location in the current transaction database is attached to the message before queuing.

Messages are extracted from the several input queues generally according to their priority, but this process could be modified by considering how long it has been since a message has been extracted from a lower priority queue. At this time the message header is parsed, according to type, to extract information necessary to perform intelligent routing in conjunction with status information. The message is then passed to the output queue indicated by the routing function. The transaction log is timestamped with the delivery timestamp, closed, and logged. Parameters influencing the routing function that may be extracted from the parsed header include:

- Precedence
- Message type (ACK, OPS NORMAL, and Datagram)
- Classification
- Format
- Destination

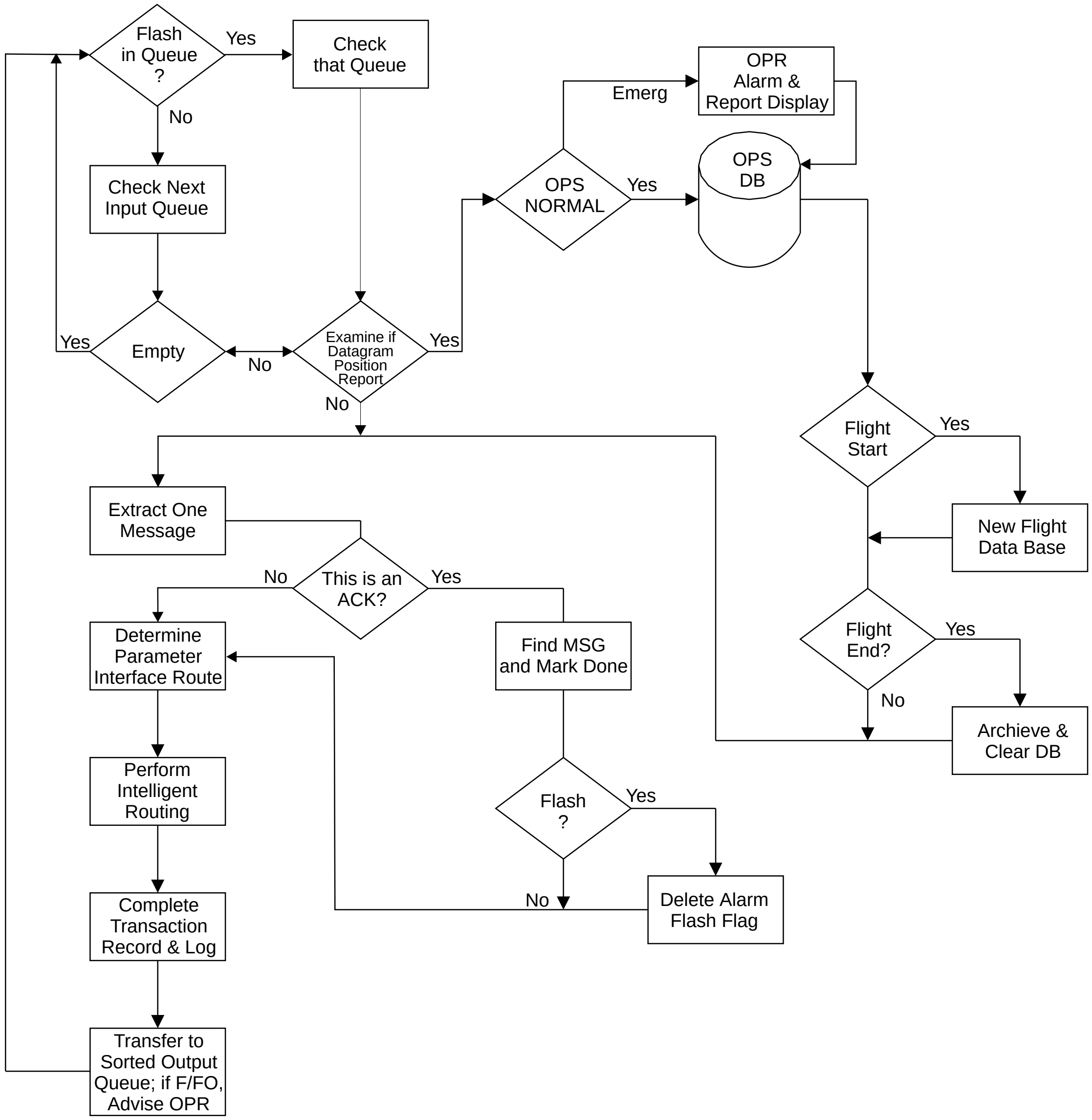


Figure 2.9-1. Routing Task

2.9.2 Message Routing

2.9.2.1 *User Profile Tables*

User profile tables will contain configuration and status data elements for mobile units and electronic devices interfaced to the shore-side gateways. The tables will include all necessary parametric data which could conceivably change according to unit complement, source selection, connection allocation, setup selections, or upgrade status. If any given routing rule can be numerically parameterized, and may be subjected to change by policy or operator command, then it shall be included in the configuration table. Example parameters include: recipient communications capabilities (RF components [tx, rx, ant, etc.]), name/platform ID, unit type, communication links available, connectivity, grade of service requirements, platform location and projected movement for mobile units, RF band usage available, circuit availability, remote hardware status, modes, and parameters of operation.

2.9.2.2 *Media Profile Tables*

Media profile tables will contain configuration and status information that shall be updated promptly as values change. Included information shall be data rates of each channel, connection allocation, setup selections, source selection, cost, reliability, allocated radio spectrum, availability of mobile communications spectrum, and error rate of channel, etc.

To the maximum possible extent, database information shall be loaded at boot time. Changes to dynamic information shall be checkpointed into permanent storage periodically and to the alternate location via the CAMS link.

The table will be appropriately optimized regarding speed of access, reliability, and implementation convenience.

2.9.3 Message Queuing

Message queuing refers to the temporary storage of messages in transit through the Intelligent Gateway. In general, the queues consist of arrays or linked lists of messages. Generally, the queues are in the computer’s dynamic memory, although in a virtual memory operating system, such as UNIX, data in DRAM is automatically paged to disk if there is insufficient DRAM. The purpose of the queuing is to accommodate differences in transmission rate between input and output channels, and to give the processor extra time during peak periods. A properly configured system will have nearly empty queues most of the time. Output queues are established for each combination of priority and classification. Output queues use the First-In, First-Out (FIFO) paradigm. An input queue is established for each input interface unit. Input queues also use the FIFO paradigm. Queues are polled in sequence by the communications controller with the exception that a queue containing a Flash message will be processed next.

Most of the interfaces will also have buffers which allow for access time to the interconnecting LAN. These need not be deep, since the LAN is in general much faster than any of the communications channels. These buffers may be byte serial, rather than message serial.

The communications controller uses a multitasking operating system and multitasking or threaded programming. One task, called the Message Input Task (figure 2.9-2), manages the incoming messages from the interface units. This task continually polls each of the interface units for data. If the interface has data, it sends all available bytes to the controller, which stores them in a single buffer specific to that interface unit. Other methods my be applicable to particular interface units, such as File Transfer Mode (FTM) for a unit which supports TCP/IP. Otherwise the interface unit sends a negative reply, and the communications controller polls the next interface unit in logical order. If the data sent results in a completed

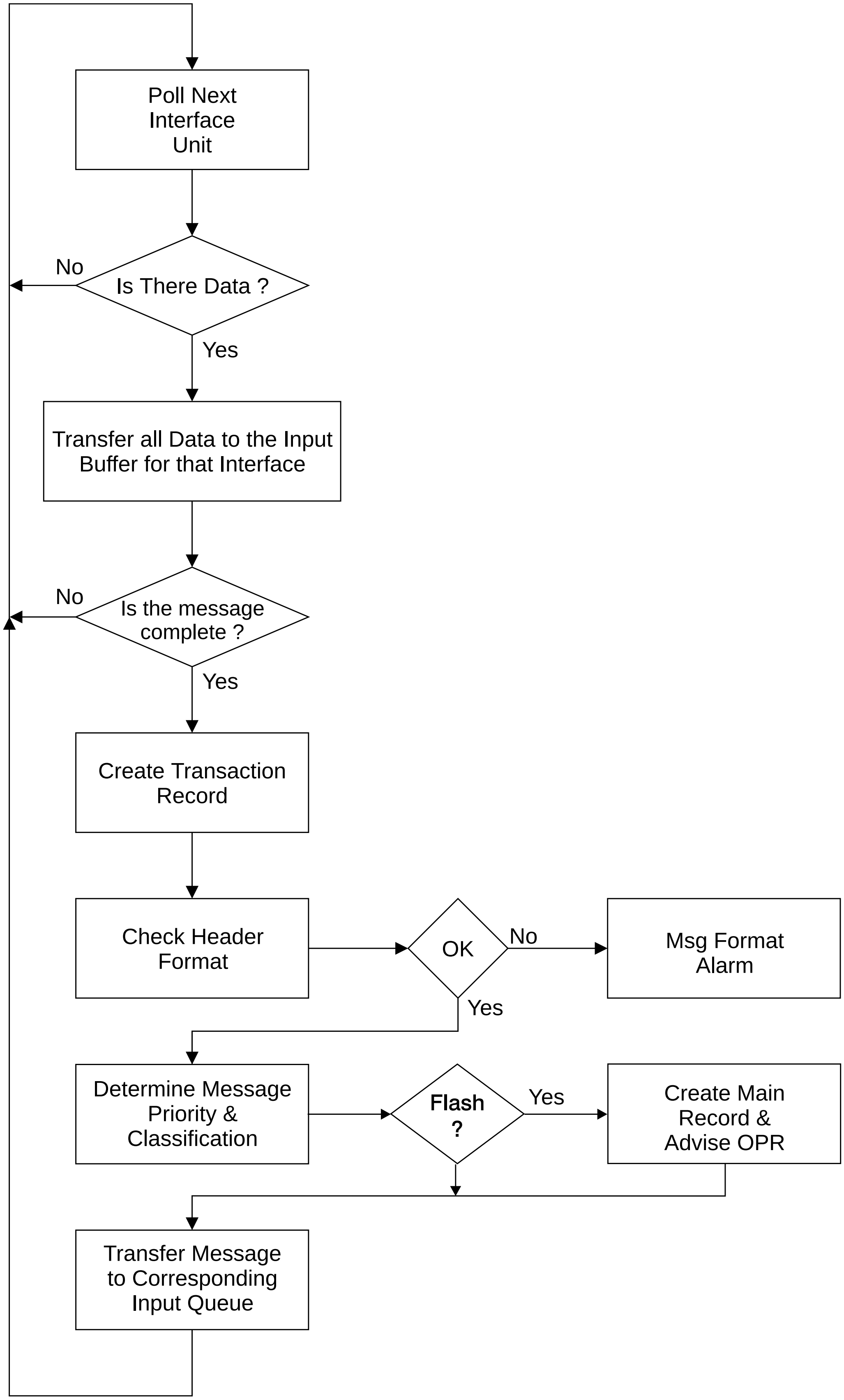
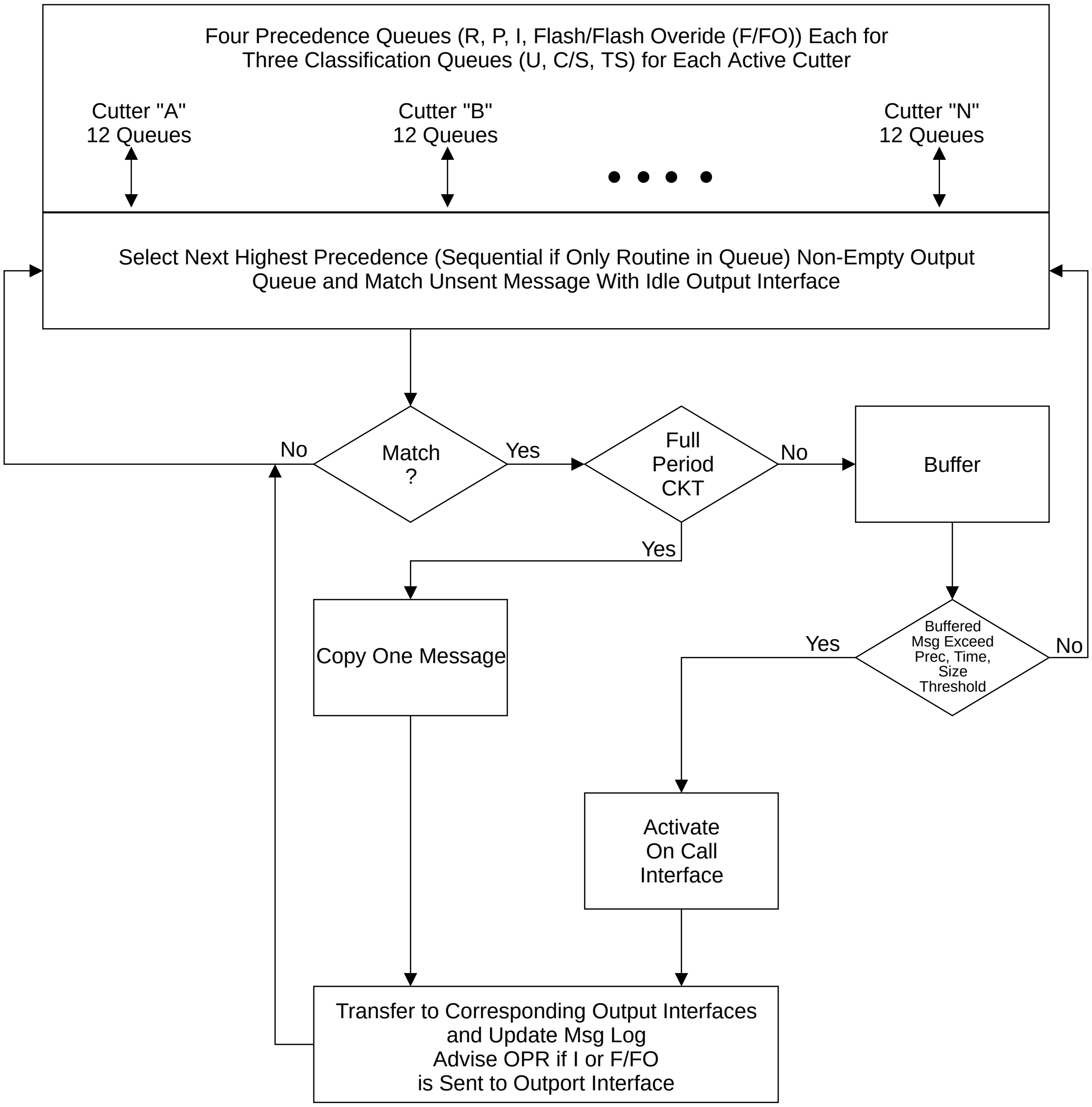

Poll Next Interface Unit
Is There Data ?
No
Yes
Transfer all Data to the Input Buffer for that Interface
Is the message complete ?
No
Yes
Create Transaction Record
Check Header Format
OK
No
Msg Format Alarm
Yes
Determine Message Priority & Classification
Flash ?
Yes
Create Main Record & Advise OPR
Transfer Message to Corresponding Input Queue

Figure 2.9-2. Communications Controller Message Input Task



Four Precedence Queues (R, P, I, Flash/Flash Overide (F/FO)) Each for Three Classification Queues (U, C/S, TS) for Each Active Cutter
Cutter "A" 12 Queues
Cutter "B" 12 Queues
• • • •
Cutter "N" 12 Queues
Select Next Highest Precedence (Sequential if Only Routine in Queue) Non-Empty Output Queue and Match Unsent Message With Idle Output Interface
No
Match ?
Yes
Full Period CKT
No
Buffer
Yes
Copy One Message
Yes
Buffered Msg Exceed Prec, Time, Size Threshold
No
Activate On Call Interface
Transfer to Corresponding Output Interfaces and Update Msg Log Advise OPR if I or F/FO is Sent to Outport Interface

Figure 2.9-3. Message Output Task

message, the communications controller performs the initial message processing described above in 2.9.1, and transfers the message to the appropriate queue. This task also identifies classification and priority, and if a Flash message, sets up the proper accountability records and notifies the operator interface.

Another task, called the Message Routing Task (figure 2.9-1). continually polls the input queues and extracts one message from the highest priority queue, if there is any. It then performs the header parsing processing described above in 2.9.1, followed by the intelligent routing of 2.9.2. The message is then transferred to the output queue identified by the intelligent router. This task also checks for OPS NORMAL datagrams and ACK replies, and updates the corresponding logs.

A third task, called the Message Output Task (Figure 2.9-3), polls the output interface units for output buffer status. If it can match up a free interface unit with a non-empty output queue, it transfers the oldest message in the highest priority output queue to the interface unit. This may take several steps if the interface unit cannot accept a whole message at LAN speeds. During the intervals other interface units may be served.

An independent task monitors all queues for buffer utilization. It has the options of increasing or decreasing buffer size based on percent of buffer in use over a sampling period, archiving to hard disk (ref. 2.9.4), sending an alarm to the operator, or sometimes transferring the messages to a faster output channel.

Another independent task, called Delay Monitor Task (figure 2.9-4), checks flash, OPS NORMAL, and output queue delays, and performs the associated operator notifications.

Within the IG communications controller, each direction of a full-duplex channel is used independently for processing and establishing associated queues and also including checks for the communication statistics.

2.9.4 Message Archiving

Message archiving refers to the permanent storage of messages on a hard disk, for record-keeping, review, printing, or retransmission. Unless prompted by an operator action or loss of facility power, only messages which have been completed, including acknowledgment from the ultimate destination, if implemented, are archived. Archived messages are transferred from the several queues.

A separate task of the multitasking communications controller, called the Archiving Task (figure 2.9-5), performs the archiving function. It continually examines the queues to determine if any contain a sufficient number of completed messages so that their total length exceeds a threshold, which is intended to use the hard disk medium efficiently, and to minimize the impact of the hard disk operation on the message processing and routing functions. This length is such that, in conjunction with the queue reserve monitor task, queue overflow is prevented.

There are additional procedures which operate on hard disk files:

- Retransmission
- Viewing
- Transfer to offline storage
- Printing
- Recovery after power failure or re-booting

Another function which may be implemented using output queues is channel cost minimization. This applies if the output channel is not used full period, and there is a connection overhead or per-minute rounded up to the even minute. In this case costs may be substantially reduced by grouping messages and filling up each minute without exceeding the last minute. Figure 2.9-6 illustrates this cost reduction routing function.

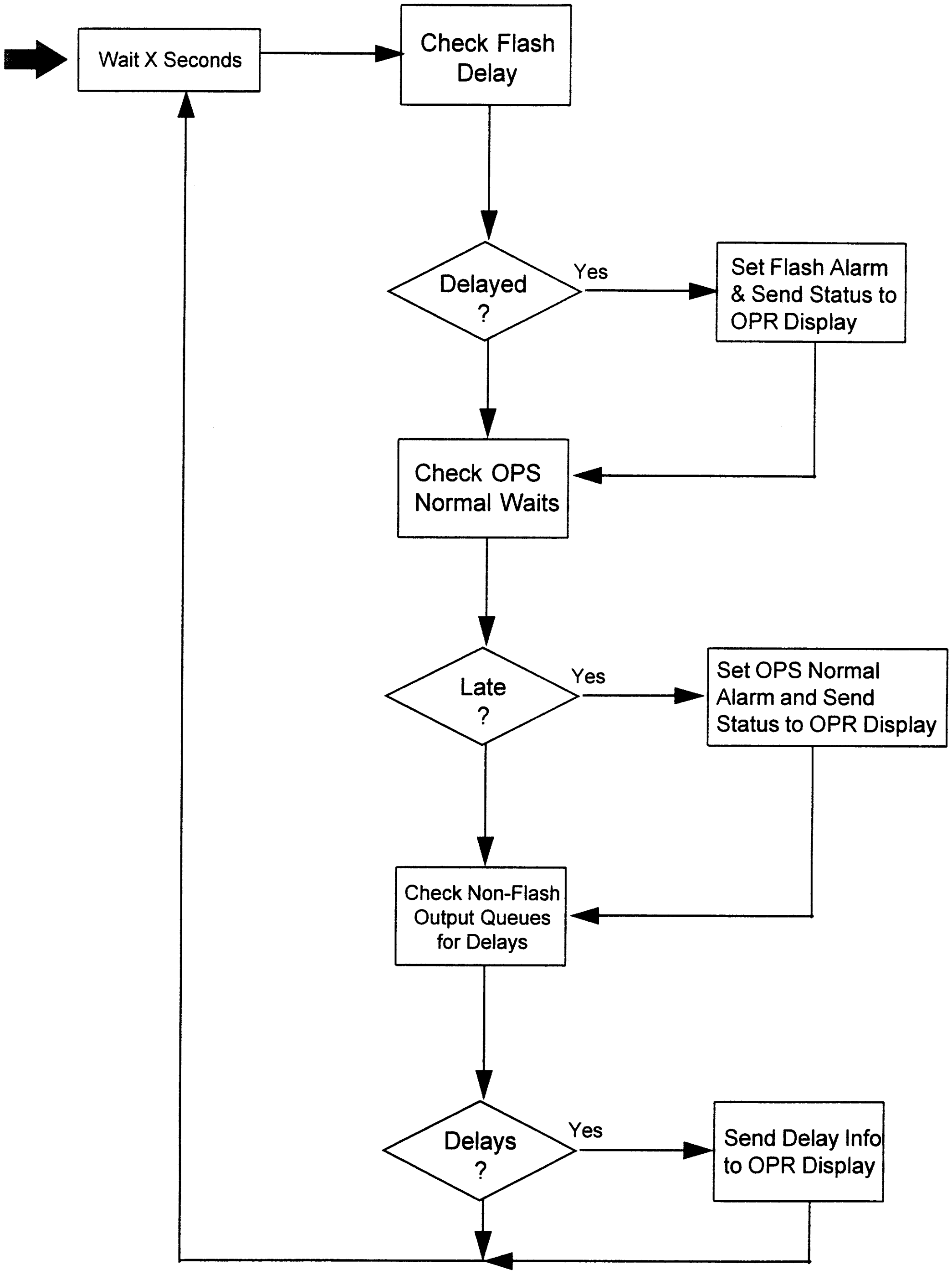

Wait X Seconds
Check Flash Delay
Delayed ?
Yes
Set Flash Alarm & Send Status to OPR Display
Check OPS Normal Waits
Late ?
Yes
Set OPS Normal Alarm and Send Status to OPR Display
Check Non-Flash Output Queues for Delays
Delays ?
Yes
Send Delay Info to OPR Display

Figure 2.9-4. Delay Monitor Task

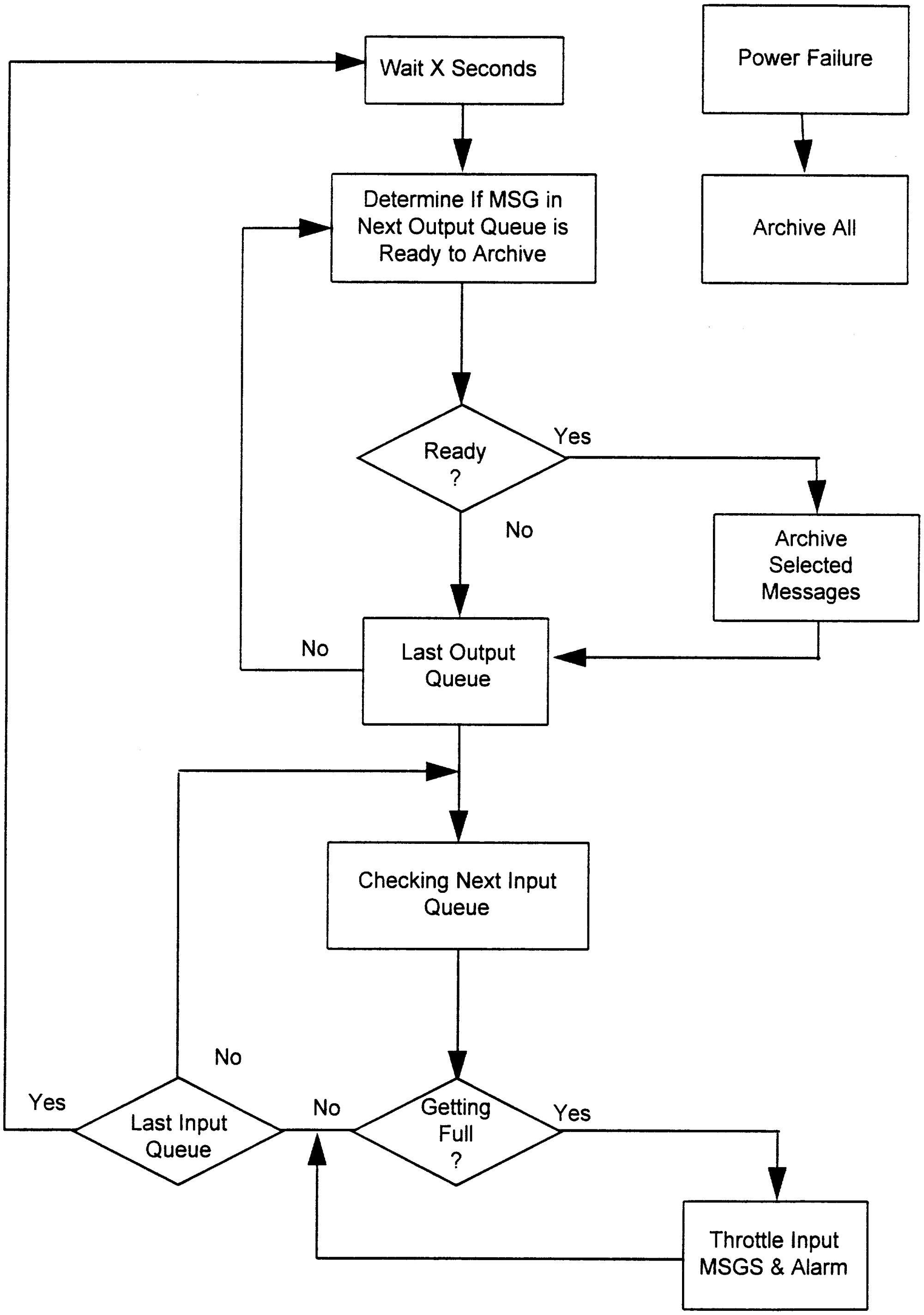
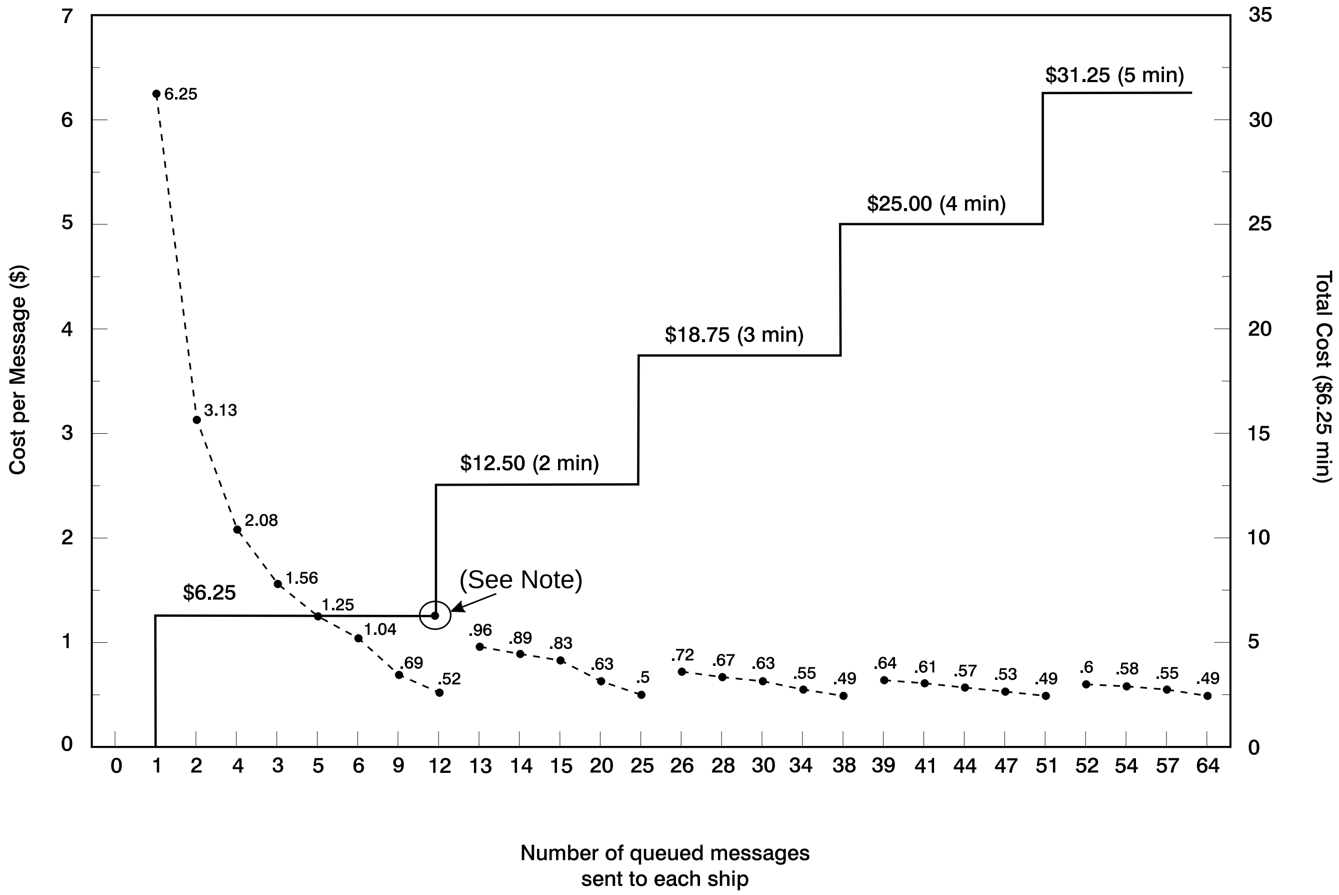

Wait X Seconds
Power Failure
Determine If MSG in Next Output Queue is Ready to Archive
Archive All
Ready ?
Yes
No
Archive Selected Messages
No
Last Output Queue
Checking Next Input Queue
No
Yes
Last Input Queue
No
Getting Full ?
Yes
Throttle Input MSGS & Alarm

Figure 2.9-5. Archive Task



Note: It takes 4.66 secs to transmit 2 pages of text @ 12.2 kbps throughput.
At this rate, the maximum number of 2-page messages which can be sent in 1 minute is 12.

Figure 2.9-6. Message Delivery Cost Reduction Analysis

2.10 INTERFACES TO MEDIA

For maximum flexibility in interfacing with existing legacy systems which may not have standard interfaces, we have included interworking functions in the IG design. These interworking functions handle the I/O translations to match the protocols and timing of routed input and output from the IG host to existing communications media. There is a wide variety of media, and it will be possible to connect to many media with standard terrestrial informations system data communications market products, while most RF media will necessitate a custom interworking function hosted in both software and in hardware. RF media will be connected via serial ports to the gateway while terrestrial media will be connected via the IEEE 802.3 LAN adapter in the gateway.

2.10.1 Interworking Functions to Media

2.10.1.1 *Bulk Encryption*

To maintain adequate security from intentional reception and interpretation of data communications by unauthorized parties, the gateway design incorporates bulk encryption of data prior to modulation throughout, utilizing the approved DES-based devices designed for such use. For current HF communications, existing KG-84C cryptos will be retained. For satellite communications, KG-84C units will bulk-encrypt data prior to transmission to the modulating satellite terminal gateway. For UHF or cellular communications, a KG-84C or KYV-7 coder-decoder will encrypt all message traffic. STU-III units will handle voice and dial-out modem data communications from the CAMS. The gateway will incorporate in its interworking functions the necessary logic to dialout in the clear and then rely upon the default programming in the STU-III products currently on the market to automatically go secure prior to allowing the gateway to transmit.

2.10.1.2 *Protocol Conversion*

Primary conversion from a vendor-specific or service-specific protocol to an industry-standard protocol will be performed by interworking devices. These will range from COTS NDI items such as multiprotocol hub adapters for the Ethernet LAN to custom software modules running as client processes on the gateway hardware host. As described above, this may be the conversion of one messaging format to a native file under Windows NT, or the conversion of the Newcomb AV-2 satellite transceiver signal format to a TCP/IP packet format, or the control commands to set up an INMARSAT link or a cellular dialup service before sending a bulk-encrypted data stream. The initial interworking devices will interface current messaging sources in the CAMS to the gateway, and will interface the gateway to the CGDN, a bank of dial asynchronous modems, the HF and INMARSAT services, and the local LAN within CAMS. Conversion will not be readily available to the older CGSW BTOS computers since they use a proprietary protocol. Interface to the existing CGSW CTOS machines is possible over the Ethernet LAN supplied with the gateway server.

2.10.1.3 *Control and Status Interfaces*

The gateway will use SNMP agents for control and status of remote sites and will utilize a software product that provides a display and alarming at the control terminal. Status and control of serial ports and virtual interworking device ports will be reflected on the customizable OpenView display screens, and the interworking devices will receive status and exert control over the interworked legacy Coast Guard systems to the extent they are controllable. For example, a remote HF site equipped with RCS will feature a true SNMP agent providing keying, frequency selection, and antenna setup, as well as reflecting status and the health of the controlled site. For an uncontrollable site, the gateway will compute necessary parameters for site or media setup, then present the operator with this information on an appropriate display to get the uncontrollable site setup as needed. For example, an operator would be given the information needed to talk to a remote person over the phone or over a radio link to request certain setup, but to the maximum extent the system would select the data needed by that operator so that the operator does not have to calculate repetitive information such as frequency to tune to, settings for antennae, or power levels. Where status is not automatically reported by a non-controllable communications resource, the operator will be given entry screens for manually entering necessary status information (such as a transmitter is down, or a block of frequencies is unusable for a period of time).

2.10.2 RF Media

Despite the disparity in data rates between conventional HF and the newer satellite communication media, cost versus minimum quality of service is the basis upon which the gateway will select media for transmitting data messaging. Based upon the precedence and priority of a particular message, together with its destination, the gateway will select the lowest cost RF media which will ensure error-free messages. Information entered into the media tables will be automatically updated as often as possible, and the operator can view and update table information where such information is not available to the gateway for automatic update. In general, RF media will interface to the gateway host hardware via serial ports supporting the RS-232C format.

2.10.2.1 *HF Transceivers*

The primary method of interoperable, universal message transmission will remain HF, and the gateway will process messages with less priority or less required time-to-delivery for transfer over HF if available. It will maintain queues of messages and feed them over IHFDL/HFDL links through an HFDL interworking device. All messages intended for transmission over such links will be automatically encrypted prior to storage in files, unless that HF medium is covered by a bulk encryption device such as a KG-84C. The file name will contain enough information to allow the recovery and sequencing of messages into the appropriate interworking device for translation to IHFDL/HFDL. A similar process will be followed for reception and processing of SSAMPS traffic intended for passage to HF transmitters.

2.10.2.2 *SATCOM Transceivers*

Whether the medium is INMARSAT, SHF DSCS, or commercial domestic satellite, the gateway will add the additional necessary controls and encryption necessary to write and read data communicated through SATCOM resources. The router selects messages with high priority or very short time-to-delivery requirements, and pushes them into the interworking device for that medium. For example, to dial up an INMARSAT-equipped ship the gateway will maintain on its tables of media and user profiles the information needed to open that link, pass the traffic, and close the link. The time spent on the link will be updated into the journal log along with a rough cost projection assigned to that message in the log together with other necessary info such as dialed number and status of response. An interworking device, such as a dial-up modem, will handle the dialing and signal synchronization for modulation and connection. Interworking devices will also use the required protocol commands to open and maintain the link while the router selects and sequences the files to push across the link. Such an architecture allows for the addition of future interworking devices such as LEO satellite services. The gateway will gracefully accept additions to its list of media in the media profile table and an additional interworking device would be written in software to handle the vendor-specific controls and status functions necessary for a new service.

2.10.2.3 *Other RF Media*

Since the gateway architecture allows for the addition of new interworking devices at a later date, as each new RF service becomes available the operator can update the list of available media in the media profile table. Where necessary, an additional interworking device would be written in software to handle the vendor-specific controls and status functions necessary for each new RF media. A new UHF cellular service, or a locally-available broadcast RF service, would be accommodated in this fashion. The media profile table will have enough entries to allow configuration of almost any RF medium desired, and an interworking device written as a software driver or protocol translator will accommodate medium-specific control and translation.

2.10.3 Terrestrial Communications Media

The intelligent gateway's WAN backbone is comprised of existing terrestrial sites linked by terrestrial wireline, fiber, virtual CGDN circuits, and leased connectivity or dial-up services through PSTN and FTS. Similar to the above RF media, each terrestrial communications medium will have media profile table entries characterizing services and connectivity, together with relative cost and quality of service such that the gateway can make routing decisions based on least cost where two or more alternate routes exist to push data messages. In general, terrestrial communications media will be lower in cost per message due to the high data rates enjoyed by non-RF wireline and fiber and the relative predictable performance of these circuits. However, many more alternate routes will exist for terrestrial media than for RF media, and interworking devices will generally consist of pure COTS NDI hardware and firmware products.

2.10.3.1 *CGDN*

Access to the CGDN is provided by an X.25 COTS router unit hosted in stand-alone hardware and firmware which connects to the gateway IEEE 802.3 Ethernet LAN, and routes packets addressed to destinations out on the CGDN via TCP/IP embedded addresses. The CGDN is an existing WAN with a Channel Service Unit/ Data Service Unit (CDU/DSU) synchronous modem and router already in place at the CAMS. Media tables within the gateway will characterize the connection and routes available through the CGDN.

2.10.3.2 *Leased-line*

Leased-line services, where necessary to augment CGDN connectivity, will be supplied by the customer apart from the gateway itself, but the gateway will provide interface via the IEEE 802.3 LAN through a customer-premises COTS CSU/DSU and router. Leased-lines will also be used to connect to the backup CAMS. Media tables within the gateway will characterize the connection and routes available through leased-lines provided by the customer.

2.10.3.3 *Dial-up PSTN*

Connection to the PSTN will be via the bank of dial-up modems which are connected to the gateway PC host via addressable serial ports. A communications client application included with the gateway provides dial-out services based upon matching the requested destination address on message files to media services listed in the gateway's media profile tables. The user table entry of a PSTN phone number matching that user is read, and supplies the client application with a dialing sequence to set up the connection. The client monitors time used, and after the call is completed and torn down, the client writes the elapsed call duration and call number to the journal log for the user, and to the overall server database for archiving and billing history.

2.10.3.4 *Other Terrestrial Media*

Almost any form of terrestrial media can be added in a modular fashion, such as special-purpose fiber via a fiber-to-Ethernet transceiver. Conventional special services, such as dockside wireline tethers for use while a ship is in port, are examples of incidental terrestrial media. While a ship is in port, the gateway would be notified of this by the operator or by a special message sent to the gateway. Until further notice of the user leaving port, messages would be re-routed through this wireline, rather than passing across RF media otherwise used routinely to communicate when underway.

2.11 HARDWARE IMPLEMENTATION

The exact layout of the Intelligent Gateway will depend on the configuration of the COTS interfaces, and the computers selected for the communications controller and operator interface workstations. In general, the units will be rack or console mounted, have positive internal cooling air pressure with filtered incoming fans, adequate operating temperature range, and enclosures which provide excellent electro-magnetic compatibility (EMC) protection. An Uninterruptible Power Supply (UPS) is necessary for the communications controller system units, as a minimum. Details of the hardware-related portion of the gateway design are documented in this section.

2.11.1 Host Hardware Platform

The communications controller is required to be compatible with the selected operating system (ref. 2.12.2.1). Although the preferred approach is first to select the most suitable software, if GFE TAC-3 tactical computers are made available, then a POSIX-compliant real-time operating system ported to that computer type will be selected. This will be a UNIX-type environment. The computer used will of course be fast, but it is more important to select a type for which an upgrade path can be foreseen. The communications controller needs to have enough DRAM after the operating system and operating program have been loaded to maintain queues of at least 30 minutes of peak message flow. The hard disk should hold the run-time portions of the operating system, the operating program, and a week's messages. A native tape or optical disk backup unit is also required.

The display of the communications controller is a console display. During operation it would normally continuously show dynamic system status, or actual messages scrolling, along with the queue status and message flow. A character-based display is preferable, since it uses less of the computer's resources in updating. Other screens would be used for setup and diagnostic purposes. All system data would also be available at each operator's console, but updated less frequently.

The selection considerations for the operator's workstation are different. Its main consideration is a large high-resolution color display, which is supported by a GUI development system. In this case also, a TAC-3 workstation running the supplied operating system is acceptable, although X-Windows/Motif has a steep learning curve and the ease of modifications is poor. Point and click GUI development environments are available for PC-based operating systems such as Windows and OS/2.

2.11.2 Physical Port Interfaces

In addition to the standard interrupt-driven parallel and serial ports present on all PCs, the communications controller will contain additional addressable serial ports through the use of bus adapter cards with fan-outs of multiple RS-232C ports. The number of ports available from some vendor products is up to 256 with optional purchased fan-out patch bays which exceeds the number of ports expected to be required by the CAMs over the life of this gateway. These interfaces will be used for attachments to asynchronous modems, serial bulk in-stream encryption devices, STU-III products, and any other local devices required to be serviced by a serial port connection. Since serial port cable run are limited to 50 feet or less, optional line-driver adapters are available which will convert from the serial format into RS-422 or even RS-485 format for very long cable runs of hundreds or even thousands of feet. These adapters are modular and universally available for long runs of cable at the CAMS.

There will also be a physical LAN interface for connection to the operator interface and all of the interface units which can be procured or adapted COTS with a LAN internal interface.

This approach is both modular and expandable, and expansion is transparent to the gateway design implementation itself. Expanding the gateway at a later date by attaching a second client operator display workstation is possible without disturbing the physical or logical setup of the basic server machine and first client machine.

The operator's workstation requires only a LAN adapter.

2.11.3 Communications Devices

Individual modems, LAN adapters, digital multiplexer ports, and CSU/DSU devices are representative of the communications devices by which the IG will connect to transmission links and shoreside networks. Dial-up access through the Public Switched Telephone Network (PSTN) will be accessed through standard modems operating at 2.4 - 14.4 Kbps. Compression algorithms allow data rates in excess of 28.8 Kbps. Synchronous digital data services at rates from 2.4 - 56 Kbps are possible through direct DCE/DTE interface with digital multiplex port interfaces or, if individual channels, through CSU/DSU devices. CGDN, Internet, and MDT communications will be provided via LAN interface adapters. Inter-CAMS high speed links will be provided via leased 56 Kbps digital service via CSU/DSU interface.

2.11.4 Interworking Devices

Where required to interface non-standard or proprietary transmission devices to the IG, hardware and/or software "interworking devices" will be used. Such devices translate between dissimilar protocols such as RS-232 to RS-422 converters, parallel to serial data port conversion, or parallel data to Ethernet conversion.

2.11.5 External Off-site Hardware

It is envisioned that CCS would be separate from the IG and connected to the same LAN system that the media are connected to. The IG will interface with off-site equipment for purposes of remote control of transmission resources or for providing equipment status. Communications and interworking devices described in 2.12.3 and 2.12.4 will provide access to and from the remote control and/or sensor equipments at off-site locations.

2.12 SOFTWARE IMPLEMENTATION

Software implementation will depend on the physical layout of the Intelligent Gateway, configuration of the COTS interfaces, computers selected for the communications controller and operator interface workstations. Details of the software-related portion of the gateway design are documented in this section.

2.12.1 Host Software Platform

The selection considerations for the communications controller and the operator's workstation are different. The operators workstation main consideration is available GUI development capabilities. The communications controller main consideration is true or pre-emptive multitasking and memory management. Additional details of the host software platform are documented in the following sections.

2.12.2 Host-Resident Software

2.12.2.1 *Operating System Considerations*

As explained in section 2.11.1, the preferred approach is first to select the most suitable software. However, if GFE (e.g. TAC-3 tactical computers) computers are made available, then a POSIX-compliant real-time operating system ported to that computer type will be selected. In either case, demo and production operating system platforms will be selected based on various factors: cost, POSIX compliance, reliability, proven relevant implementations, software development costs, built-in communications capabilities, deadlock handling, security capabilities (e.g. mandatory access control, file protection, etc.), concurrent processing capabilities and scheduling mechanisms/policies, primary and secondary storage management, and other performance/capabilities characteristics. Other non-performance factors will influence the selection of the operating system such as commonality with the predominant file server environment used in the Operational Information System Project, air-ground automation, and other applications host environments present in the COMMSTAs. The communications controller(s) will act as servers freeing applications from much of their machine-dependence. A cross-platform server environment like Windows NT will pass files with security intact along a file transfer path which may contain two or more differing hardware platforms. Only the host platform containing the actual host-resident software modules is restricted to a platform CPU which must match the compiler used. This paradigm is illustrated in the following example implementation.

In the case of the Gateway, an 80x86 family and an executable compiler for the 80x86 family would be used. Having files transported across a common pathway, such as messages from the OIS/2 airborne LAN environment through the satcom link to the shore, and thence into the Gateway, could solve many security and addressing problems before they occur.

The operator display and control client PC would run Windows NT Workstation, taking full advantage of the server's Windows NT file and communications support services environment. The principal advantage of separating the functions into two physical PCs is one of unloading all of the operator's client display and control functions from the server PC's CPU, while retaining access to local databases contained within the server.

Control and status windows would reside on the client PC, but will retain access to the important databases within the server on demand.

The benefits to system performance and flexibility of this approach will have to be weighed against the additional initial hardware cost of such a two PC gateway system.

2.12.2.2 *Database Backend*

The choice of a Database Management System (DBMS) over a traditional file processing system is indicated by numerous advantages. The principle advantages are that data maintained by a DBMS can be integrated, more secure and less redundant. DBMS also have increased integrity and programs that access data without any file format dependency. The following paragraphs will detail each of the principle advantages mentioned above.

> Integrated Data - in the DBMS paradigm all of a systems data is maintained by the DBMS. Application programs are able to request single data items or complex mixtures of data without requiring knowledge of the specific detail of how to combine the data. This combining of data is handled by the DBMS and alleviates the complex algorithms from the application programs.
>
> Data Security - is enhanced by the use of a DBMS which provides mechanisms that allow only authorized user the ability to view and perform operations on specific data items. The DBMS provides authorization rules used by the security mechanisms, which are administered by the Database Administrator (DBA) such as access controls on Views, Fields, and Tables.
>
> Data Redundancy - is decreased because the data is stored and maintained by the DBMS, making the requirement to store data in multiple files obsolete. With the data stored in only one place in the DBMS, updates and modifications to the data are only required once, which greatly reduces CPU usage and the manipulation of data, which reduces the possibility of introducing data errors.
>
> Data Integrity - is the assurance that data does not become corrupt during typical operations such as updates, changes, deletions, and multiple user activities. The DBMS provides increased data integrity by having all actions performed against a data set managed by the DBMS.
>
> Program and Data Independence - is provided on DBMSs because data formats and locations are managed and maintained by the DBMS in lieu of the application programs. Programs need not include the file format, block structure, or record format of the data they request. Application programs need only include a definition of the data being requested from the DBMS. This procedure decreases maintenance costs of the application program, especially when the format of the data changes.

The disadvantages of a DBMS are that the development is more complex than that of a file processing system. This complexity increases the cost of development because developers, engineers, and programmers must be more knowledgeable in the development of DBMSs. Overheads are increased in the areas of index processing, I/O, disk space, and memory. Response time can be slower than the traditional file processing systems as well. All of the hardware and performance issues can be overcome with the use of more powerful processors and increases in mass storage devices as well as random access memory (RAM).

In order to provide complete query functionality the DBMS must utilize a relationaly complete language. The Structured Query Language (SQL) is relationaly complete, and is additionally an ANSI standard. These factors indicate the use of an SQL DBMS backend.

Therefore, commonality factors discussed above, as well as availability constraints will be considered in the selection of an SQL Server database backend providing identical services for managing queries among server-based database files.

2.12.2.3 *Common Applications/Utilities Library*

Network management procedures, software, equipment and operations designed to keep a network operating near maximum efficiency will be used for distributed gateway communications network. A Network Management product such as IBM's NetView, HP's OpenView, Sun's SunNet Manager or Novell's NMS will be used. The selection of the network management product will be based on various factors including interoperability with selected hardware and choice of network management protocols such as SNMP, CMIP and DME. Additionally, the selection of a network management product will be based on the five functional areas defined in section 2.8.5.

2.12.3 Specific Software Modules

2.12.3.1 *Logical Message Processor*

Perhaps the most important initial function is the ability to segment, order, and examine logical files containing streams of ASCII characters. Following this examination, the Message Processor function compares key character sequences to entries in a reference table to determine how to handle a particular stream of characters. Based upon these stored parameters, the process separates message streams into separate logical files, each file containing one and only one message. Storage of files where information is embedded into the filename allows subsequent processing and routing of the message without the need to reexamine the contents of the file. This will allow the contents of the file to be encrypted while still allowing routing in the clear by filename.

Encryption filters within the message processor, realized as in-line linked code modules such as Secret Agent DES RSA-key encryption software, will ensure that no data is sent unencrypted - whether there is a companion serial bulk encryption interworking device on the media interface or not.

2.12.3.2 *Custom Protocol Adapter*

A custom protocol adapter will be necessary for the OIS Phase II function of automating the periodic and labor-intensive Operations Normal status messages routinely received from airborne platforms (and perhaps some afloat platforms eventually). In particular, the interworking device for the HH60J satellite transceiver is a custom protocol adapter, since the vendor cannot support TCP/IP addressing. Such addressing is necessary for the remainder of the shore communications network, and the adapter will provide necessary translation services.

2.12.3.3 *Custom Interworking Services*

For COTS/GOTS gateway interfaces that do not have standard internal interface and where there are no COTS/GOTS interworking devices, custom interworking services will be developed to interconnect these devices to the LAN or directly to the communications controller.

2.12.4 Logical Interfaces to External Software Processes

2.12.4.1 Interface to MDC Gateway Protocol Adapter

As explained in section 2.12.3.2, OPS NORMAL reporting, via the Newcomb AV2-Mobile Data Comm (MDC) gateway, requires interfacing to a custom "base" protocol adaptor, which converts between TCP/IP and the proprietary Simple Transport Protocol (STP) (a CCITT X.25 derivative) that is used by the Newcomb AV2. The intelligent gateway will be either directly connected to the MDC gateway with a separate (from the District Command Center) version of the protocol adaptor, or connected to the District Command Center via a TCP/IP protocol communications link.

2.12.4.2 *Remote Control of External Devices*

It is envisioned that the CCS would be separate from the IG and connected to the same LAN system LAN that the media are connected to. The remote control standard family of SNMP agents will be used to provide “hooks” to external remote control features of controllable hardware located at remote sites, such as unattended HF transmitter sites where there are available control systems in use. Monitoring status information will be returned through the “send status” command hook of SNMP. The Navy’s RCS is such an example. Both control commands and remote telemetered status are available to the gateway in an autonomous framework for continual automatic update of media status profile databases.

2.13 USER INTERFACE

The operator of the IG responds to alarms, event-generated operator intervention demands. The IG also monitors and reviews generated reports. The user interface can be either attached directly to the gateway or a remote terminal attached to the network. It will use a dashboard concept, presenting only critical information with intuitive graphical displays. Bar gauges and status lights to indicate readiness or level of effort underway on the IG is envisioned. A keyboard, a pointing device, and voice recognition could be used to select an area of interest and to investigate the details of a particular system. The operator's control terminal will offload dedicated windowing, status display, and control entry functions from the server by being hosted in a separate client PC.

2.13.1 Local Operator Console

The design will utilize a Windows (possibly X-Windows) interface with the Motif look and feel. The screens contained in Appendix B are representative of the prototype code, are intended to stimulate discussion. A discussion of the screen operation is provided with each screen.

2.13.1.1 *Input and Control Devices*

A standard enhanced keyboard, pointing device and ergonomic work station furniture will be required for each machine.

2.13.1.2 *Alert and Alarm Features*

Alarms will be configurable both in terms of initialization parameters and computer response. Visual, aural and e-mail/pager information are planned. As the severity of alarm increases, the programmed response will increase. Normal information goes to the screen while warnings become audible. Casualties or fatal errors will also generate audible and visual alarms to notify the responsible person.

2.13.2 Remote Operator Terminal Access

Remote operator terminal access will be virtually the same as local operator console. All functions that can be performed from the local terminal may be performed at the remote terminal. For example any warnings that require physical action to the IG will either alarm in appropriate format or an additional code can be added to accomplish a hardware reset. A remote operator will be able to communicate directly to the local console operator and with other remote operators.

2.13.2.1 *Windowed Display Screens*

The screens have the same look and feel as the local console.

2.13.2.2 *Input and Control Devices*

If possible, the remote console could be made keyboardless, with only a pointing device required.

2.13.2.3 *Alert and Alarm Features*

Has the same features as the local terminal.

2.13.2.4 *Terminal Communications Support Link*

The network established to support the IG will also support the remote terminals, using industry standards and COTS products.

Appendices

Appendix A

Acronyms

Appendix A
Acronyms

AATS	Automated Amplifier Test Set
ABS	Automated Broadcast System
ACK	Acknowledge
AERO-C	Aeronautical INMARSAT-C Terminal
AFCEA	Armed Forces Communications and Electronics Association
AFLX	Air Force Logistic Center
A/G	Air/Ground
ALE	Automatic Link Establishment
ALEM/C	Automatic Link Establishment Modem/Controller
AM	Amplification Modulation
AMP	Automated Message Preparation
AMSC	American Mobile Satellite Corporation
AMVER	Automated Mutual-Assistance Vessel Rescue System
ANCC	Automated Network Control Center
ANDVT	Advanced Narrowband Digital Voice Terminal
ANSI	American National Standards Institute
ARQ	Automatic Repeat Request
ASC	Autodin Switching Center
ATM	Asynchronous Transfer Mode
AUTODIN	Automated Digital Information Network
BCS	Broadcast Control Station
BCST	Broadcast
BER	Bit Error Rate
BG/ARG	Battle Group/Amphibious Ready Group
BIT	Built-in Test
BKS	Broadcast Keying Station
BPS	Bits per Second
BTOS	Burroughs Technology Operation System
C4I	Command, Control, Communications, Computers and Intelligence
C4IFTW	C4I for the Warrior
CAMS	Communications Area Master Station
CAMSLANT	Communications Area Master Station Atlantic
CAMSPAC	Communications Area Master Station Pacific
CCITT	International Telephone and Telegraph Communications Committee
CCS	Communication Control System Communication Station Controller System
CDA	Communication Decision Aids
CDC	Call Directory Code
CG	Coast Guard
CGDN	Coast Guard Data Network
CGSWS	Coast Guard Standard Workstation
CINC	Commander-in-Chief
CJCS	Commander, Joint Chiefs of Staff

CJTF	Commander, Joint Task Force
CKT	Circuit
CMU	Control Modem Unit
CNO	Chief of Naval Operations
COMMDET	Communications Detachments
COMMSTA	Communications Stations
COMMSYS	Communications System
COMNAVCOMTELCOM	Commander, Naval Computer and Telecommunications Command
COMSPAWARSYSCOM	Commander, Space and Naval Systems Command
COMSTATREP	Communications Status Report
CONUS	Continental United States
COTS	Commercial Off-the-Shelf
CSU/DSU	Channel Service Unit/Data Service Unit
CTOS	Convergent Technolgy Operation System
CUDIXS	Common User Digital Information Exchange Subsystem
CW	Continuous Wave (Morse Code)

DAMA	Demand Assigned Multiple Access
DBA	Database Administration
DBMA	Database Management System
DBS	Direct Broadcast Satellite
DCS	Defense Communications System
DES	Digital Encryption Standard
DHSD	Duplex High Speed Data
DISA	Defense Information Services Agency
DISN	Defense Information Switched Network
DITCO	Defense Information Technology Contracting Office
DOD	Department of Defense
DPSK	Differential Phase Shift Keying
DPUS	Distributed PLA Verification System
DRAM	Dynamic Random Access Memory
DSC	Digital Selective Calling
DSCS	Defense Satellite Communications System
DSN	Digital Switched Network
DTG	Date Time Group
DTMF	Dial Tone Multiple Frequency

ECCM	Electronic Counter-Countermeasure
ECM	Electronic Countermeasure
ECO	Engineering Change Order
ECS	Exterior Communications System
EHF	Extremely High Frequency
ELF	Encrypted Link Filter
E-Mail	Electronic Mail
EMI	Electromagnetic Interference
EMP	Electromagnetic Pulses
ET	Electronic Technician

FAST	Fly-Away Satellite Terminal
FAX	Facsimile

FDDI	Fiber Distributed Data Interface
FEC	Forward Error Correction
FIFO	First In First Out
F/FO	Flash/Flash Override
FLTBCST	Fleet Broadcast
FLTCINC	Fleet Commander-in-Chief
FLTSAT	Fleet Satellite
FM	Frequency Modulation
FMS	Foreign Military Sales
FRTT	Fleet Radio Teletype
FSK	Frequency Shift Key
FSS	Fixed Satellite Services
FTM	File Transfer Mode
FTS	Federal Telephone System
GFE	Government-Furnished Equipment
GFI	Government-Furnished Information
GMDSS	Global Maritime Distress Safety System
GMF	Ground Mobile Forces
GOTS	Government Off-the-Shelf
GPS	Global Positioning System
GUI	Graphical User Interface
HF	High Frequency
HFAARS	High Frequency Adaptive Antenna Receiving System
HFCM	High Frequency Communications Manager
HFCW	High Frequency Continuous Wave
HFDL	High Frequency Data Link
HFDS	High Frequency Data System
HFNCS	High Frequency Narrowband Communications System
HFRATT	High Frequency Radio Teletype
HFRG	High Frequency Radio Group
HFRWI	High Frequency Radio Wireline Interface
HSFB	High Speed Fleet Broadcast
ICW	Interrupted Continuous Wave
IDE	Indoor Equipment
IEEE	Institute of Electrical and Electronic Engineers
IG	Intelligent Gateway
IHFDL	Integrated High Frequency Data Link
IMO	International Maritime Office International Maritime Organization
IMM	Interactive Message Manager
INMARSAT	International Maritime Satellite
INTEL	Intelligence
IP	Internet Protocol
ISA	Industry Standard Architecture
ISO	International Standards Organization
ITDS	Information Transfer and Distribution System
ITU-T	International Telecommunications Union - Telecommunications

JITC	Joint Interoperability Testing Command
JTF	Joint Task Force
KDD	INMARSAT Earth Station at Yamaguci, Japan
kHz	Kilohertz
Ku	Ku Satellite Band
LAN	Local Area Network
LANTAREA	Atlantic Area
LANTCOMMSYS	Atlantic Area Communications System
LEASAT	Leased Satellite
LEIS	Law Enforcement Information Systems
LEO	Low Earth Orbiting
LES	Land Earth Stations
LF	Low Frequency
LHD	Landing Ship Helicopter Dock
LOG	Log Server
LPD	Low Probability of Detection
LPI	Low Probability of Intercept
LQA	Link Quality Assessment
LR	Long Range
LRI	Limited Range Intercept
LRU	Lowest Replaceable Unit
LSB	Lower Side Band
MARDEZ	Maritime Defense Zone
MARISAT	Maritime Satellite
MBC	Meteor Burst Communications
MCU	Microprogrammer Control Unit
MDT	Message Distribution Terminal
MEP	Marine Environmental Protection
MF	Medium Frequency
MHz	Megahertz
MILSATCOM	Military Satellite Communication
MIPR	Military Inter-Department Procurement Request
MLE	Maritime Law Enforcement
MO	Military Operations
MOP	Memorandum of Policy
MSC	Military Sealift Command Multiple Services Contract
MSG	Message
MSS	Mobile Satellite Services
MT	Mobile Terminal
MTDS	Message Transfer and Distribution System
NAK	Negative Acknowledgement
NATO	North Atlantic Treaty Organization
NAVCAMS	Naval Communications Area Master Station
NAVCENT	Naval Forces Central Command
NAVCOMPARS	Naval Communications Processing and Routing System
NAVMACS	Naval Modular Automated Communications System

NAVTEX	Navigational Warning System
NBDP	Narrowband Direct Printing
NCTAMS	Naval Computer and Telecommunications Area Master Station
NDI	Non-developmental Item
NECOS	Network Operating Control
NISE	Naval In-Service Engineering Group
NM	Nautical Mile
NOAA	National Oceanographic & Atmospheric Administration
NOSC	Naval Ocean Systems Center (San Diego)
NRaD	Naval Command, Control and Ocean Surveillance Center Research, Development, Test, and Evaluation Division
NSA	National Security Administration
NTCC	Naval Telecommunications Center
NVIS	Near Vertical Incident Skywaves
O&M	Operations and Maintenance
OPCEN	Operational Center
OPNAV	Office of the Chief of Naval Operations
OPNAVINST	Chief of Naval Operations Instruction
OSC	Operations System Center Orbital Science Corporation
OTAR	Over-the-Air Rekeying
OTAT	Over-the-Air Transfer
PABX	Private Automatic Branch Exchange
PACAREA	Pacific Area
PC	Personal Computer
PDU	Portable Dama Units
POC	Point of Contact
POSREP	Position Report
PoST	Portable Satellite Terminal
POTS	Plain Old Telephone System
PRIN	Portable RF Integrated Network
PRS	Pocket Radio Software
PSDN	Public Switched Data Network
PSK	Phase Shift Keying
PSTN	Public Switched Telephone Network
QC	Quality Checks
QDPSK	Quadrature Differential Phase Shift Keying
Q/R	Query/Response
R&D	Research and Development
RAM	Remote Antenna Matrix
RATT	Radio Teletype
RCC	Rescue Coordination Centers
RCP	Resource Change Proposal
RCS	Remote Control System
RCVD	Received
RF	Radio Frequency

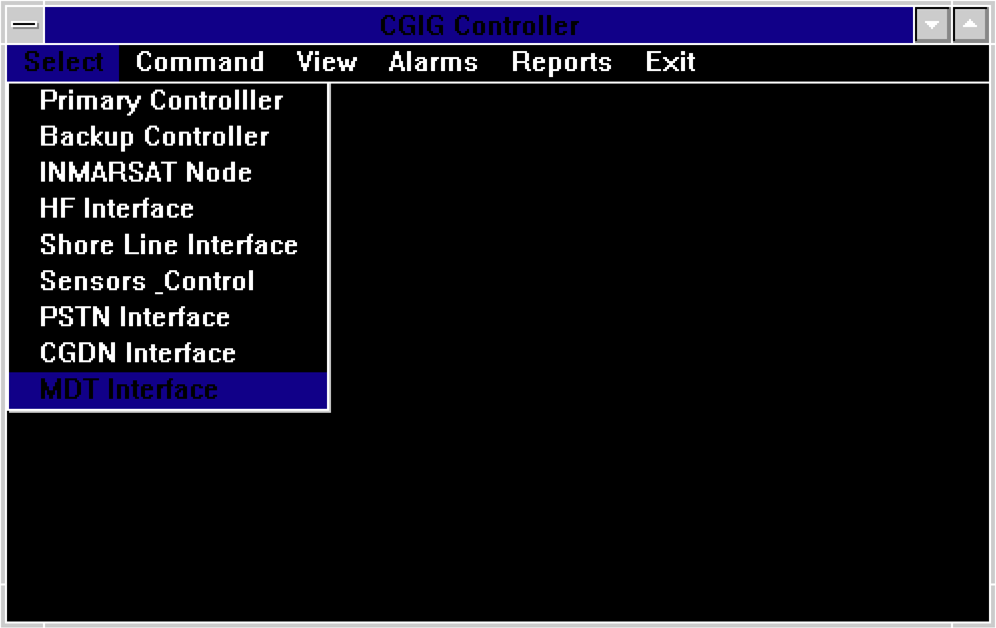
RFAu	Radio Frequency Antenna Unit
RI	Routing Indicator
ROI	Return on Investment
RSA	Rivest-Shamir-Adleman algorithm
RTE	Radio Terminal Emulator
RWI	Radio Wireline Interface
SAR	Search and Rescue
SATCOM	Satellite Communications
SATCOMMFACS	Satellite Communications Facilities
SCCN	Secure Command and Control Network
SCN	System Coordination Network
SDK	Software Development Kit
SDN	Secure Data Network
SHF	Super High Frequency
SHSD	Simplex High Speed Data
SINCGARS	Single-Channel Ground and Airborne Radio Systems
SITOR	Simplex Teletype Over Radio
SNMP	Simple Network Management Protocol
SOLAS	Safety of Life at Sea
SPAWAR	Space and Naval Warfare Systems Command
SQL	Structured Query Language
SRCS	Shore Remote Control System
SSACCS	Surface Ship Automated Communications Control System
SSAMPS	Standard Semi-Automated Processing System
SSB	Single Sideband
STEP	Site Telecommunications and Engineering Plan
STM	Serial-Tone Modems
STU-III	Secure Telephone Unit (Third Generation)
SVN	Secure Voice Network
SWS	Standard Work Station
TACTERM	Tactical Terminal
TADIL	Tactical Digital Information Link
TAGOS	Towing Auxiliary General Ocean Surveillance Ship
TAO (USN)	USN Oiler
TBD	To Be Determined
TCC	Transportable Communications Center
TCIC	Telecommunications Chief-In-Charge
TCM	Tactical Command Management
TCP/IP	Transmission Control Protocol/Internet Protocol
TELECORS	Telecommunications Requirements
TELEX	Teletype Exchange
TFSI	Timeplex Federal Systems, Inc.
TISCOM	Telecommunications and Information Systems Command
TOR	Time of Receipt
TTY	Teletype
TWPL	TeletypeWriter Private Line
UFO	Ultra High Frequency Follow-on

UHF	Ultra High Frequency
UMIB	Urgent Marine Information Broadcast
UNCLAS	Unclassified
USAF	United States Air Force
USB	Upper Side Band
USCG	United States Coast Guard
USMFT	United States Message Text Format
USN	Unites States Navy
VFCT	Voice Frequency Control Terminal
VME	Versabus Modular Eurocard
VOBRA	Voice Broadcast Automation
VSAT	Very Small Aperture Terminal
VVFD	Voice, Video, Facsimile, and Data
WAGB	Ice Breaker
WAN	Wide Area Network
WHEC	High Endurance Cutter
WLB	Buoy Tender, Oceangoing
WMEC	Medium Endurance Cutter
WIX	Trainer, USCG Barque Eagle
WPB	Patrol Boat
WX	Weather
XMIT	Transmit

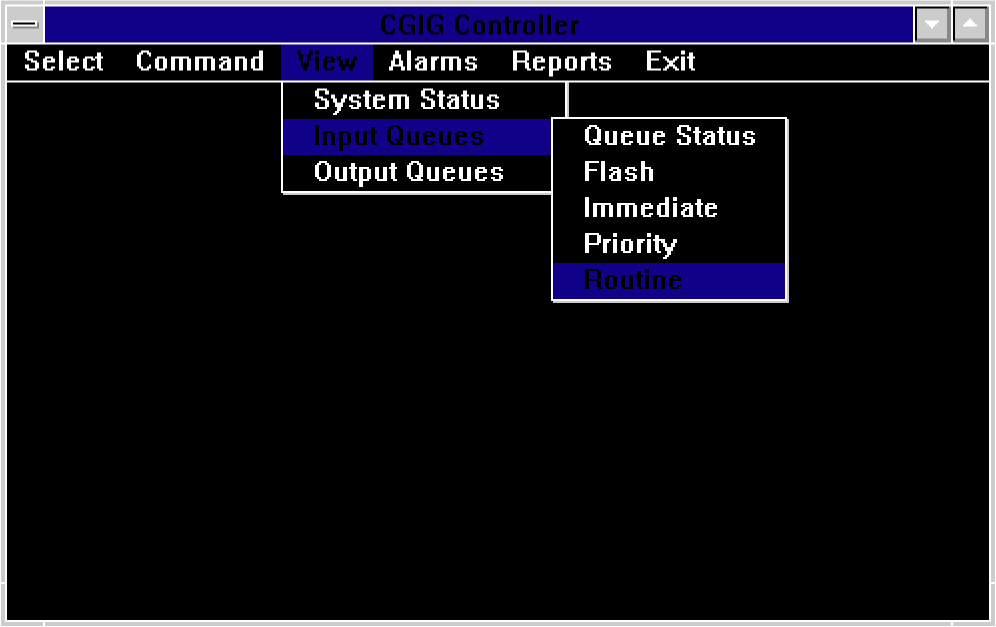
Appendix B

User Interface Sample Screen Views

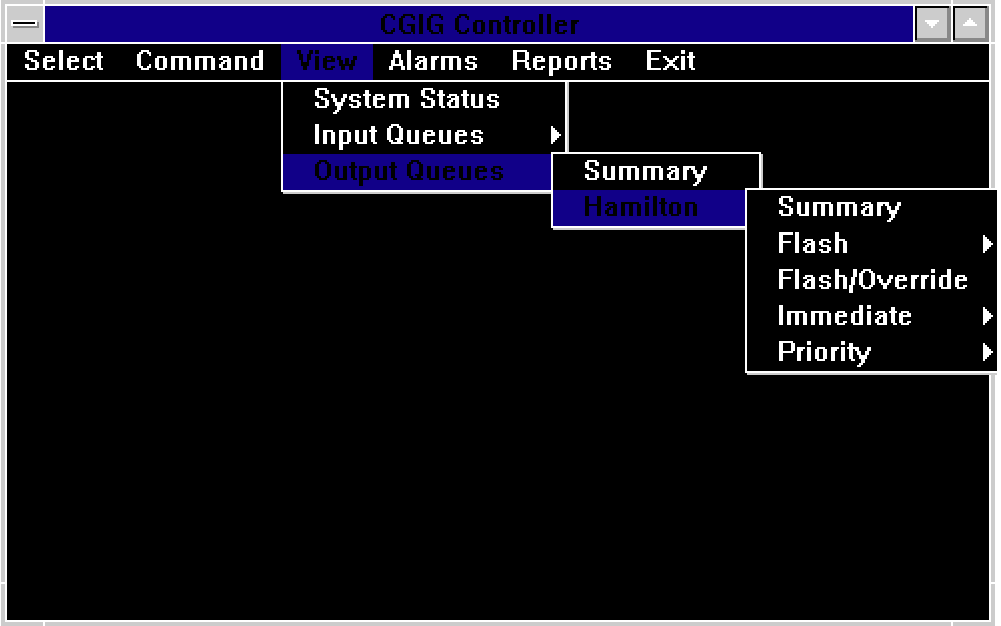
User Interface Sample Screens



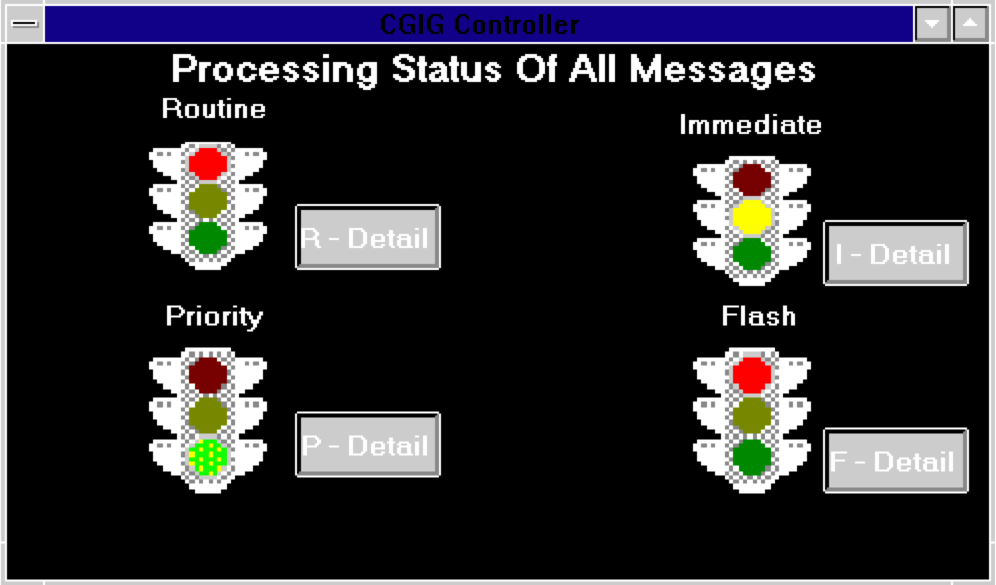
Main Control Screen: This menu provides the operator with all the basic commands required to operate the Coast Guard Intelligent Gateway (CGIG) Controller. The Select menu provides the operator with various system selectable controls and access to detailed interface control information.



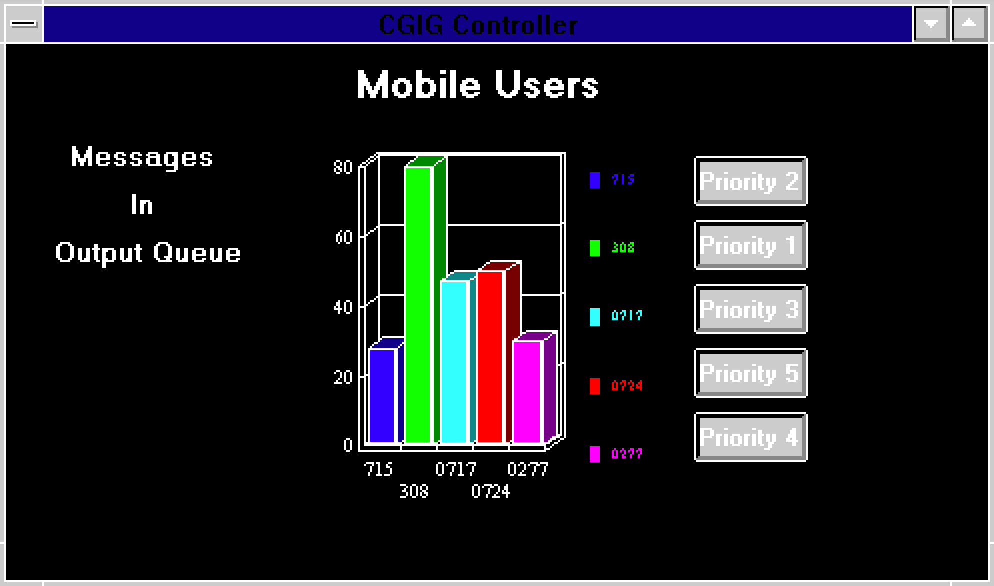
Main Control Screen 2: This menu provides the operator with access to various Graphical Information views. Each view is designed based on selections previously made in the Select and Command pull down menus.



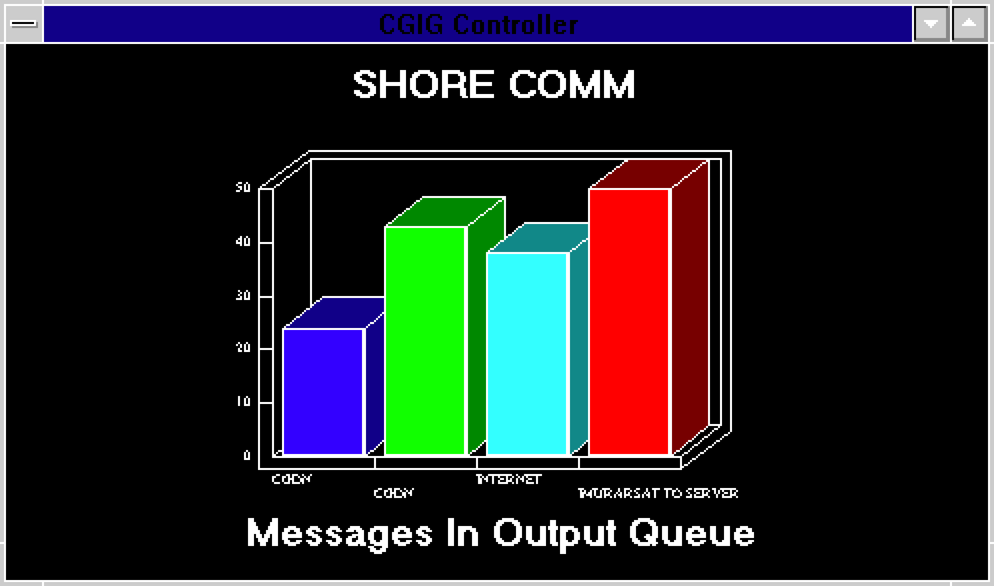
Main Control Screen 3: This menu provides the operator with additional access to various graphical information views. Each view is designed based on selections previously made in the Select and Command pull down menus.



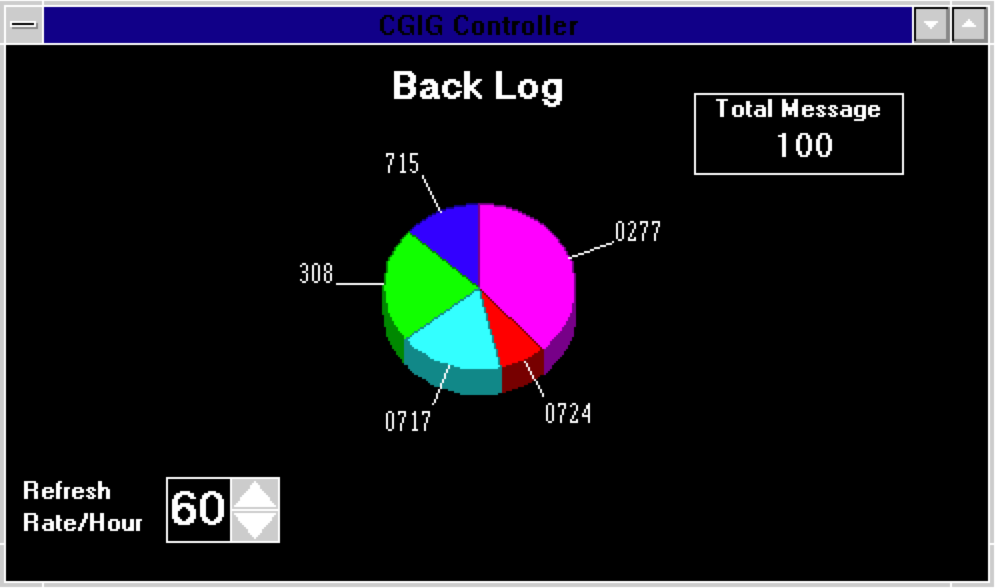
Processing Status of all Messages view: This view indicates the presence or absence of a backlog for each of the message priorities. Green indicates all messages in the queue are expected to be delivered on time. Yellow indicates a potential for a backlog exists or the number of messages in queue is greater than the warning limit set by the operator. Red indicates the queue is in a backlog status as established by the operator.



Mobile User Messages in the Output Queue view: This view indicates the number of messages in the queue for the guarded mobile platform and allows the operator to adjust the priority of delivery based on the platform. The scales are operator selectable to maintain perspective on the overall status of the IG.



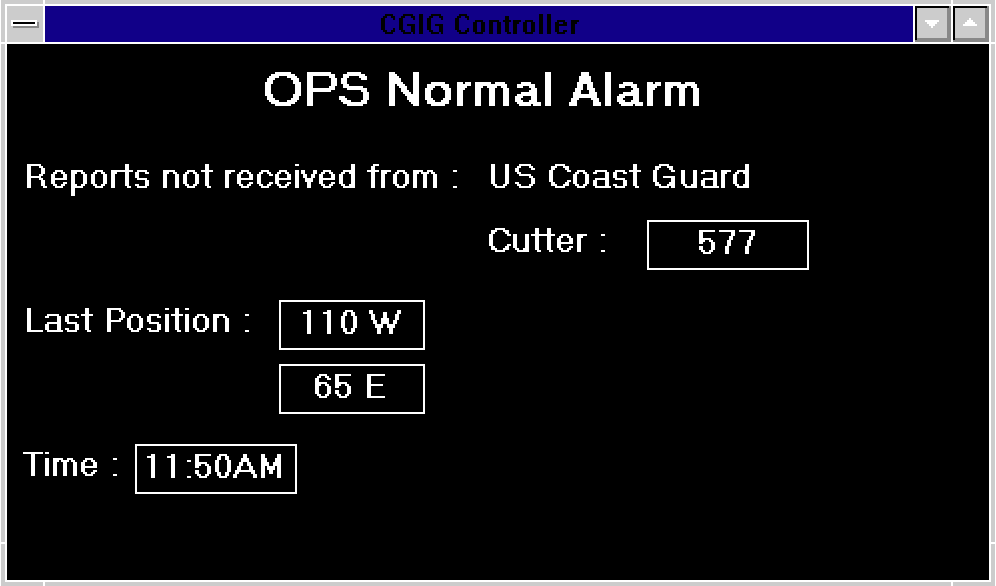
Shore Communications Links Messages in the Output Queue view: This view indicates the number of messages in the queue for the various outbound circuits supported by the IG. The scales are operator selectable to maintain perspective on the overall status of the IG.



Total Message
100

Refresh Rate/Hour 60

Back Log view: This view indicates the total number of messages in the mobile outgoing queues displayed as a percentage of the total for each mobile users. The refresh rate is operator selectable to maintain perspective on the overall status of the IG without committing computer central processing unit cycles to the maintenance of the display. If the requirement for timely reporting increases or decreases the rate can be changed without returning to the main menu.



OPS Normal Alarm

Reports not received from : US Coast Guard

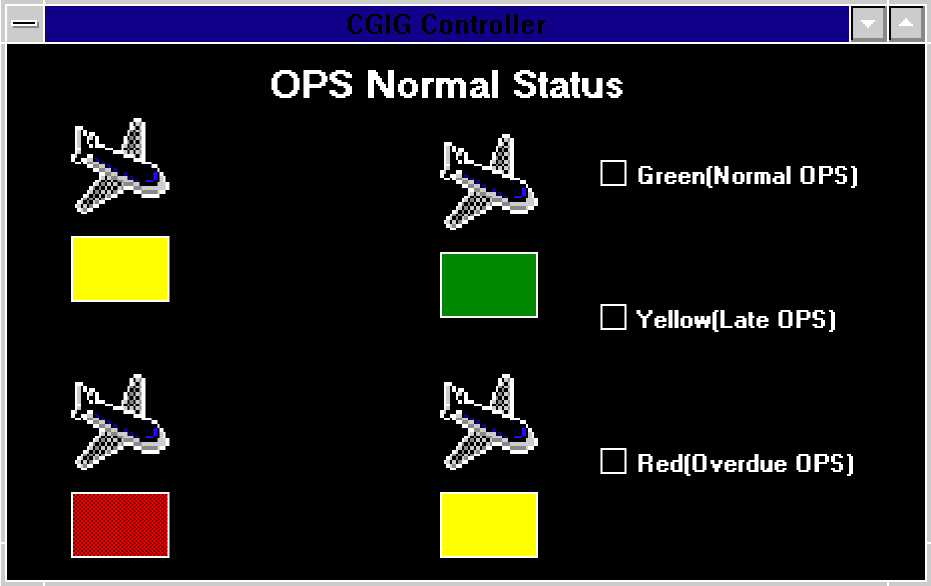
Cutter : 577

Last Position : 110 W

65 E

Time : 11:50AM

OPS Normal Alarm view: This view is automatically presented when an operations normal report is overdue from any of the mobile users which require them. The time from the last report until the alarm is actuated can be set permanently within the system or made adjustable by the operator.



OPS Normal Status

□ Green(Normal OPS)

□ Yellow(Late OPS)

□ Red(Overdue OPS)

OPS Normal Status view: This view indicates the status of all operations normal reports from mobile users which require them. The time from the last report until the alarm is actuated can be set permanently within the system or made adjustable by the operator.