CHAPTER 1

CENTER OPERATIONS

Upon completing this chapter, you should be able to do the following:

- *Identify the procedures for transmitting messages via automated systems and manual circuits.*
- *Identify the procedures for monitoring and reporting of circuit backlogs.*
- *Identify the steps to verify broadcast number continuity.*
- *Determine the procedures for preparing, updating, and verifying the command guard list (CGL) and the master station log (MSL).*
- *Identify the procedures to verify STU-III systems parameters for remote/dial-in users and explain the need to set up and operate the STU-III terminals with remote/dial-in users.*
- *Determine the procedures for the preparation of the communications plan.*
- *Identify the steps to reset communications systems to RADAY.*
- *Determine communications protocols applied to circuit set up/restorations.*
- *List the steps to activate, deactivate, and place communications circuits in standby, set up, or restoration.*
- *Identify the procedures to transmit or receive cryptographic keying material via OTAT/OTAR.*
- *Define the steps to analyze network capacity and reliability.*

Telecommunications capabilities are continually advancing as technology improves. Because of advances in technology, we are seeing great improvements in the quality and speed of communications, and an increase in our information transfer capabilities. The Navy's modern automated systems greatly reduce writer-to-reader times in message handling, and the volume of messages that can be processed is steadily increasing.

ASHORE AUTOMATED TELECOMMUNICATIONS SYSTEMS

Two new shore command systems that are coming on-line in the 1990s are the Navy Standard Teleprinter Ashore (NSTA) and the Manual Relay Center Modernization Program (MARCEMP). We will discuss these two new systems as well as the other in-place automated shore systems and their interface components.

NAVY STANDARD TELEPRINTER ASHORE

With the introduction of the Navy Standard Teleprinter (NST) at afloat commands, there was a need to replace antiquated communications systems ashore with a system compatible with the NSTs. To meet this need, the Navy has developed the Navy Standard Teleprinter Ashore (NSTA) program.

The heart of the NSTA program is the Personal Computer Message Terminal (PCMT) and its

associated software. The PCMT (shown in figure l-l) is a PC-based microcomputer. The PCMT is a major step toward modernizing the entire Naval Telecommunications System.

Personal Computer Message Terminal

The Personal Computer Message Terminal (PCMT) is a remarkable military message-processing software package that runs on a combination of IBM-compatible PC- or AT-class desktop microcomputers and input/output devices called bus interface units (BIUs). The PCMT has the following advantages:

- For sites having a message relay requirement, the PCMT system eliminates handling torn paper tape.
- For small naval telecommunications centers (NTCs), the PCMT provides a sophisticated, easy-to-use automated message-handling system.
- For Local Digital Message Exchange (LDMX) or Naval Communications Processing and Routing System (NAVCOMPARS) subscribers that must be served remotely, the PCMT can provide an excellent, low-cost remote terminal capability. Received traffic can be reviewed at a terminal and selected messages shifted to a printer when a hardcopy is needed. The system will allow the operator to compose and save any number of partially completed pro forma messages. Subsequently, these messages can quickly and easily be retrieved, completed, and sent whenever needed.
- The PCMT allows messages to be exchanged via diskette media. For users who wish to exchange AUTODIN message traffic with their own PC-based systems, the PCMT provides an excellent vehicle for doing so.

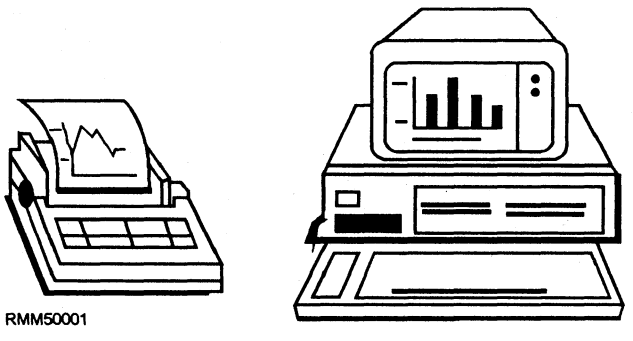

Figure 1-1.—Personal Computer Message Terminal (PCMT) with printer.

PCMT System

The PCMT message-processing system is a store-and-forward system that provides full accountability for all messages transmitted and received. The PCMT consists of a microcomputer configured with an 84-key keyboard, monitor, hard disk, and one or two floppy diskette drives. The PCMT also includes a medium-speed printer for printing message logs and hard-copy messages when required. Bus interface units (BIUs) are required to interface between the PCMT and the automated shore systems.

The PCMT microprocessor has 640K (minimum) of random-access memory (RAM) and uses the Microsoft® Disk Operating System (MS/DOS). The PCMT has a 5 1/4- and 3 l/2-inch disk drive capability. The minimum hard disk has a capacity of 10 million bytes. The hard disk varies based on software and user storage requirements. The PCMT may have either a nonremovable or removable drive, depending upon the user's security requirements.

The MS/DOS software is designed for a single workstation operation with operator-entered commands controlling the workstation. Powerful, easy-to-use message edit software will help the operator correct errors in input data from diskettes and generate messages. The monitors are monochrome except where the software has been coded to display pertinent information in color. In the next paragraphs, we will describe some of the capabilities of the PCMT.

The PCMT system assigns a message accountability number (MAN) to each complete or partial message processed. Once a MAN is assigned, the system reports each step in the processing of that message. This is done by automatically generated and on-demand log entries and on-demand message accountability reports. Message accountability reports identify all processing activity completed or pending for each message processed by the system.

The system also generates a log entry each time a complete or partial message is received, transmitted, or canceled. All messages received from or delivered to a diskette are further identified in the log entries and message accountability reports by the appropriate diskette volume identification.

The PCMT can be used to recall a specific message from the hard disk, which can be printed on an output

device. The operator can recall a message by providing a message accountability number (MAN), a component identification number (CIN), or a channel service number (CSN). The operator can also recall a message with an originating station routing indicator (OSRI), station serial number (SSN), or time of file (TOF).

The PCMT also provides significant paper reduction since information on receipt and delivery of message traffic is recorded on diskettes instead of paper. The PCMT stores messages on the hard disk until the operator requests delivery. The PCMT then outputs messages to a diskette, thereby reducing manual processing steps.

The PCMT system is setup so that narrative and data pattern (card image) traffic received from the serving LDMX and NAVCOMPARS can be delivered to the printer and/or diskettes. Data pattern traffic is usually delivered only to diskettes. Messages delivered to diskettes are segregated by routing indicators so that message centers receive only those messages addressed to them.

An operator can use the PCMT to enter a narrative or card image message, or create anew message using a simple keyboard/display screen editor. The terminal allows the operator to save a partially completed message on a diskette, recall it, and continue to edit it. At some communications centers, the operator can enter narrative or card image data pattern traffic prepared elsewhere.

Simple PC-based application programs that can be used in an office environment to review and prepare both narrative and card image messages are being developed. Once a day, the PCMT system will generate a summary report that identifies all traffic processed by the terminal during the previous 24-hour period.

The PCMT is the outgrowth of a program begun by COMNAVTELCOM (now COMNAVCOMTEL-COM) in 1982 to provide automation support for fleet message relay centers. The Navy had a continuing requirement to exchange message traffic over HF radio channels terminated at a relay site. Unfortunately, such channels impressed transmission garbles on any message they carried.

Since NAVCOMPARS required that message data presented by a TTY circuit be letter-perfect, NAVCOMPARS could not terminate such circuits directly. In the past, a message received on these circuits had to be punched out onto paper tape and printed simultaneously. The fleet center operator would then examine the printed copy and, if there were no errors, feed the paper tape into a reader that was on-line to NAVCOMPARS. If there was an error, either the ship would have to resend the message or the operator would have to recut the message's paper tape on a Model 28 TTY.

The process was slow, manpower intensive, and error prone. The system built in response to this need is now what we call the Manual Relay Center Modernization Program (MARCEMP).

MANUAL RELAY CENTER MODERNIZATION PROGRAM

The Manual Relay Center Modernization Program (MARCEMP) was first certified for operational use in 1988 as part of the NSTA program. However, even before certification, it was recognized that the system could serve as the basis for a much more generalized low-cost message-processing system. The typical MARCEMP system is a PCMT configuration.

The MARCEMP provides significant automation support for all aspects of HF message relay operations within the fleet. Since all HF fill-period termination and primary ship-shore traffic circuits have been terminated directly into a state-of-the-art computer-based system, the need to handle tom paper tape has been completely eliminated.

The MARCEMP system automatically checks formal messages for errors and sends them on when no errors are found. The system also makes available to a fleet center operator an advanced, full-screen computer terminal editor. The operator can use the terminal editor to correct format errors in the message that occur due to transmission garbles. The terminal editor can also be used to carry on an operator-to-operator dialogue with afloat communications personnel to coordinate corrective action.

The system provides a complete message audit trail and detailed accountability reports, which help ensure that all traiffic is properly handled. Its modular and flexible design permits it to be easily tailored to meet the varying individual needs of the large or small fleet center. MARCEMP can handle up to 24 send and 24 receive circuits simultaneously. MARCEMP can also process approximately 3,500 narrative or operator-to-operator dialogue messages daily.

A number of significant enhancements have been added to the MARCEMP version 1.0 baseline system. These enhancements have resulted in the PCMT version 2.0 as another configuration of the NSTA

program. This version is configured as a single workstation. Version 3.0 can be configured as a multiple workstation or single workstation PCMT system to replace both the earlier version 1.0 MARCEMP and version 2.0 PCMT. The PCMT version 3.0 can do everything MARCEMP and PCMT version 2.0 can do—and much more.

GATEGUARD SUBSYSTEM

The GateGuard subsystem is an Automatic Digital Network (AUTODIN) Interface Terminal (AIT) that provides user office automation systems (OASs) a gateway to the AUTODIN system. (AUTODIN is discussed later.) GateGuard also acts as a security guard device; hence, the name GateGuard. The GateGuard subsystem will eventually allow commands (subscribers) to interface directly with the AUTODIN system. This direct interface eliminates the manual handling of messages by the servicing telecommunications center (TCC).

Currently, a servicing TCC processes (transmit and receive) message traffic from the AUTODIN system for its subscribers. The GateGuard subsystem will eventually eliminate the need for TCCs because subscribers will be able to process their own messages through GateGuard. Subscribers will also be able to route messages via their local area networks (LANs) using desktop computers.

The GateGuard system is comprised of three elements:

- An AUTODIN Gateway Terminal (AGT),
- A gateway communications link to an Automated Information System (AIS), and
- A Guard Device (GD).

The AGT functions as a RIXT look-alike send-and-receive terminal connected to one of the AUTODIN subscriber terminals, such as the LDMX, NAVCOMPARS, or PCMT. The AGT serves as the primary AUTODIN interface point for a single organization.

The AGT has software that will operate on microcomputer systems designed to be operated by organization admin personnel. For example, in a small command, the AGT is located in the commanding officer's outer office and is operated by the Yeoman or secretary.

The communications link connecting the AUTODIN Subscriber Terminal (AST) with the AGT passes through the Guard Device (GD). The main purpose of the GD is to assist in enforcing system security policy. Specifically, the GD serves to isolate sensitive data in the serving AST from data processed by the AGT. It does so by ensuring that each message processed has been properly encapsulated and assigned a security code that the AGT is cleared to process.

The serving AST provides long-term archive storage for all messages sent to or received from the AGT. When the AGT is served by an LDMX, an operator at the AGT is able to recall messages from that system automatically. The operator is also able to identify the desired message by its originator and date-time group, originating station routing indicator, station serial number, time of file, or by the processing sequence number assigned to the message by that system.

The following is a simplified description of how the GateGuard subsystem works:

Various offices in a command have desktop computers that are interconnected by the command's LAN. Messages drafted on any computer in the system can be stored in a central computer. These messages can be accessed by any computer in the LAN. The messages can then be reviewed and checked for accuracy in format and content. When a message is released, the command sends it to the AUTODIN system via the GateGuard subsystem. At no time does the message leave the computer channels.

When messages are sent to subscribers via the AUTODIN system, the GateGuard subsystem will be able to identify messages for the various subscribers by plain language addresses (PLAs) or routing indicators (RIs). In some cases, GateGuard will use a key word or phrase in the message text to identify the subscriber for which the message is intended.

GateGuard will examine each message for which it accepts delivery responsibility, determine message completeness, and determine if it contains internally consistent security labels. If GateGuard detects any discrepancies, the software will not allow the message to be forwarded or delivered to a diskette. However, the message can still be routed to a local printer connected to the GateGuard subsystem.

AUTOMATIC DIGITAL NETWORK

The Automatic Digital Network (AUTODIN) is a worldwide computerized communications system. AUTODIN provides for the transmission of narrative and data pattern traffic on a store-and-forward basis.

AUTODIN provides reliable, secure, and efficient communications. AUTODIN also incorporates error detection and contains the highest speed transmission equipment currently available. AUTODIN is part of the Defense Communications System (DCS) and is managed by the Defense Communications Agency (DCA).

Interface equipments translate all AUTODIN inputs into common machine language, making AUTODIN compatible with many computer codes, speeds, and media, such as cards and tapes. Because of this, communications equipment within the NTS can be integrated into the AUTODIN system.

AUTODIN Switching Centers

The backbone of the AUTODIN system is the Automatic Switching Center (ASC). There are eight ASCs in the continental United States and five ASCs overseas (Europe and the Pacific).

The ASCs are interconnected into a digital network by trunk lines. Each center has local lines that link it to each subscriber (communications center) terminal. Messages entering the AUTODIN system at any of the subscriber terminals are forwarded through their respective switching centers. The ASCs accept messages from subscribers, determine the classifications and precedence of the messages, and relay the messages to the addressed subscribers.

AUTODIN Operational Modes

There are five AUTODIN system operational modes. These modes provide variation of speed and operation capabilities based on the equipment configurations of the message center subscribers. The following paragraphs describe each mode:

- **Mode I** —A duplex operation with automatic error and channel controls. Mode I operation allows independent and simultaneous two-way operation between two stations. The channel control characters acknowledge receipt of valid line blocks and messages or allow return of error information to the subscriber. The terminal (switching center) responds automatically to these characters by continuing or stopping transmission and displaying action information to the operator. A magnetic tape terminal is an example of terminal equipment using mode I.

- **Mode II** —A duplex operation normally associated with TTY or teleprinter equipments with independent and simultaneous two-way operation capability. There are no automatic error and charnel controls in mode II operation. Message accountability is maintained through channel sequence numbers and service message actions.

- **Mode III** —A duplex operation with automatic error and channel controls but only one-way transmission capability. The return is used only for error control and channel coordination response. The mode III channel is reversible on a message basis. Control characters are used in the same manner as in mode I.

- **Mode IV** —A unidirectional operation (send only or receive only) without error control and channel coordination. The mode IV channel is nonreversible and is equivalent to half-duplex operation of mode II.

- **Mode V** —A duplex operation, normally associated with TTY or teleprinter equipment, with independent and simultaneous two-way transmission. Control characters acknowledge receipt of messages and display limited information to the operator. Message accountability is maintained through the use of channel sequence numbers.

Input and output (I/O) devices, such as teleprinters, provide the central AUTODIN computer with the necessary means to communicate with the user. Output devices provide the means for changing the computer-processed data into a form specified by or intelligible to the users. The selection of I/O devices depends on the specific use for which a computer is intended.

Generally, I/O devices must meet several basic requirements. First, they must be able to modify all data so that it is acceptable to the computer during the input phase of the operation. The devices must also be able to present data in usable form during the output phase and operate quickly and efficiently with the computer.

I/O devices use coded languages. These languages are:

- **ASCII Code** —American Standard Code for Information Interchange, eight-level paper tape; and
- **ITA #2 Code** —American version of international TTY alphabet, five-level paper tape.

Message Header Programming

At the beginning of each AUTODIN message is a header (format line 2) containing pertinent information on the destination of the message. The originator can address a message either to a single addressee or to multiple addresses. This system saves time and requires fewer communications facilities, since only one message is prepared by the originator and sent to the switching center.

The timing system contained in AUTODIN equipment briefly connects a switching center to each subscriber terminal in turn. Computer memories act as reservoirs for the incoming messages of each subscriber terminal. The computer is programmed to connect each terminal in turn during a cycle. Messages received in their entirety are scheduled for output to the addressees' charnels as their turns arrive in the cycle.

AUTODIN has built-in safeguards that can detect almost any type of hardware or format error. Additionally, a complete (reference) copy of all relayed messages is kept on AUTODIN computer tape. A separate (journal) copy is made of only the addressee(s). Using this journal copy as an index enables the system to locate the reference copy of any message.

AUTODIN Tape Messages

The AUTODIN system is programmed to accept properly cut tapes and route them through the various switching centers and terminals en route to their ultimate destination. The system is then able to produce a tape and hardcopy for the designated addressee(s).

When preparing a message tape for the AUTODIN system, you must adhere to certain tape-cutting procedures. For example, format lines 1, 2, and 4 must not deviate; otherwise, the ASC will reject the message. The next paragraphs discuss the most important points on proper preparation of tape messages for transmission in the AUTODIN system.

ROUTING INDICATORS. —Within the AUTODIN network, a message tape is routed through the AUTODIN system to the addressee(s) by a routing indicator. Routing indicators are combinations of not less than four nor more than seven letters.

A routing indicator begins with the letter R or Q. The letter R indicates that the routing indicator is part of the worldwide tape relay system. The letter Q indicates that the routing indicator is within a self-contained network within a command or theater.

The second letter of the routing indicator identifies the nation or international alliance to which the indicator belongs. For example, the letter U refers to the United States. Therefore, RU indicates that the message tape is part of the worldwide network and is destined to a station in the United States.

The third letter of the routing indicator identifies the geographical area in which a particular station is located or from which it is served. This is necessary for relay purposes because the second letter may indicate a large nation within which there are a number of subdivisions or stations. For example, many stations in the United States are designated by the third letter C. Therefore, the first three letters of "RUC" indicate that the tape is part of the worldwide network, destined for the United States, and to a certain geographical area within the United States.

The fourth and subsequent letters of a routing indicator designate relay and tributary stations within the tape relay network. Like the first three letters, the fourth and subsequent letters may vary, depending upon location, area, and other factors.

TRANSMISSION IDENTIFICATION (FORMAT LINE 1). —As a means of maintaining traffic continuity, TTY terminals (modes II, IV, and V) must prefix each message header with a message transmission identification (TI). The ASC validates the elements in the TI. Modes I and III do not require format line 1. The TI is constructed without spaces and must be accurately prepared without corrections. For example, a correctly prepared TI might appear as follows:

VZCZCJTA (FIGS) 123 (LTRS) (2CR 1LF)

The elements of the TI and their meanings are as follows:

- **V** —Ensures that the first character of intelligence is not lost or garbled;
- **ZCZ** —Indicates the start of the message;

- **JTA** —Station/channel designator letters;
- **xxx** —Three-digit number indicating the sequential number of transmissions.

The station/channel designators vary for each channel and are determined by the status of the originating station. For example, if a minor relay or tributary station originates a TI to a major relay station, the first two characters consist of the fifth and sixth letters of the station routing indicator. The third character identifies the channel. Channel designators start with the letter A, progress alphabetically, and are assigned to all connected channels. For example, a tributary station having the routing indicator RUWTABA would use the designator "ABA" for the first outgoing channel and "ABB," "ABC," and so on, for additional outgoing channels.

MESSAGE HEADER (FORMAT LINE 2). —The message header is a basic 43-position header (figure 1-2). The message header is the starting point for the operator who is preparing the message tape. When preparing the header, the operator must remember that it must be letter-perfect.

The following paragraphs describe each position of the header:

Position 1 (Precedence) —The prosign Z (FLASH), O (IMMEDIATE), P (PRIORITY), or R

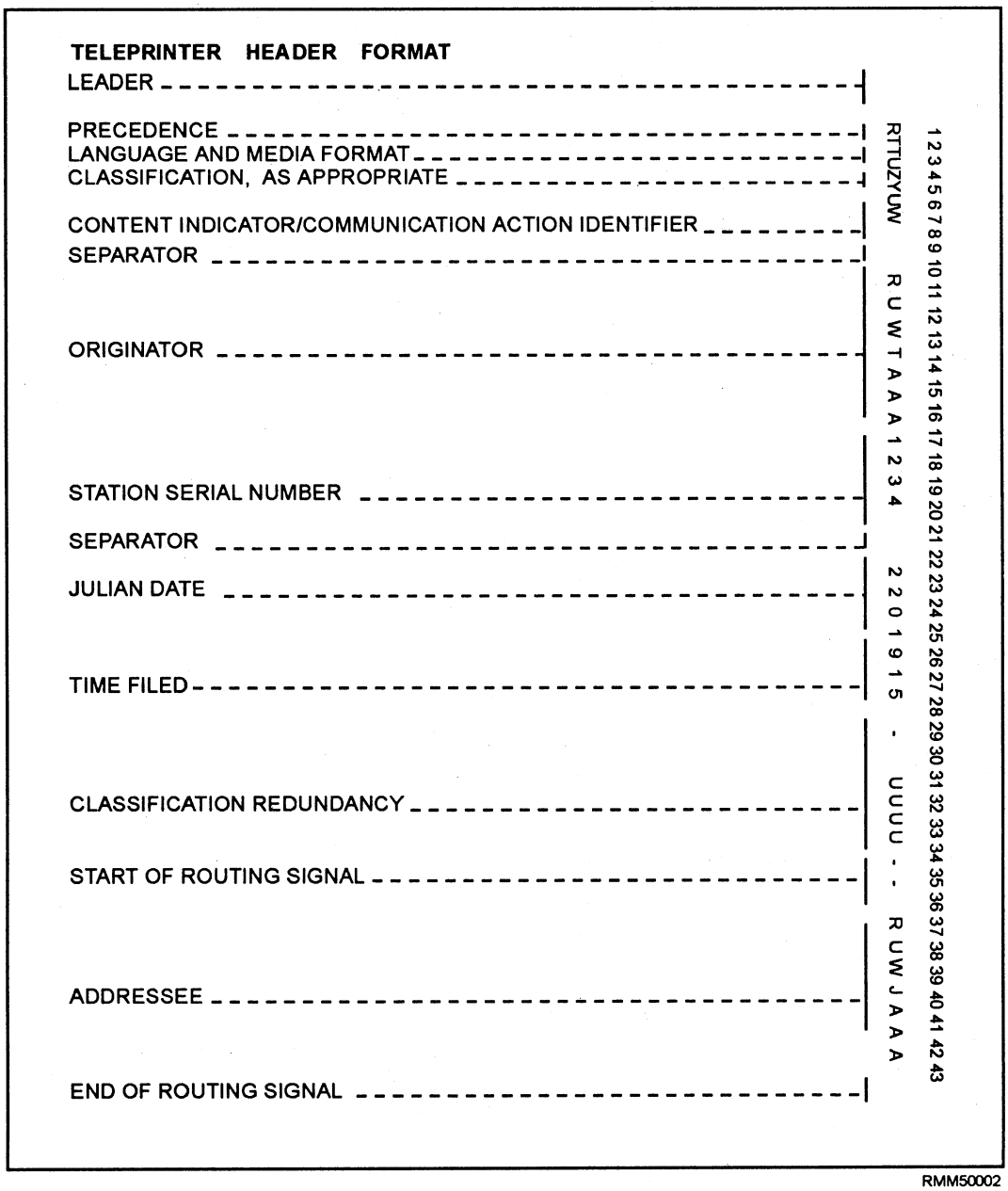

Figure 1-2.—Message header (format line 2).

(ROUTINE) is the first element. The prosign Y (YANKEE) is an emergency command precedence (ECP) and is assigned to emergency action messages (EAMs). The prosign Y indicates that a message has FLASH preemption capability. EAMs are processed ahead of all other traffic and interrupt lower precedence traffic already in processing within the AUTODIN system.

Positions 2 and 3 (Language and Media Format) —The language and media format (LMF) consists of two alphabetical characters. The LMF is the mode used to insert a message into the AUTODIN system. The LMF of the originating station is placed in position 2, and the LMF of the preferred output device of the addressee is placed in position 3. For example, in figure 1-2, positions 2 and 3 have the character T. The character Tin position 2 indicates that the originator's transmitting mode is paper tape (TTY/teleprinter) (five-level ITA2 code). The character T in position 3 indicates that the output device at the receiving end will be paper tape (TTY) (five-level ITA2 code). If the character C was used in position 3, this would indicate that the message was prepared and transmitted on paper tape and the output device at the receiving message center would be magnetic tape. *Automated Digital Network (AUTODIN) Operating Procedures,* JANAP 128, lists the LMFs used in the AUTODIN system.

Position 4 (Classification) —The letters authorized to indicate the message classification or special handling in this position are:

A	Special Category (SPECAT)
T	Top Secret
S	Secret
C	Confidential
E	Unclassified EFTO
U	Unclassified

Positions 5 through 8 (Content Indicator Code [CIC]/Communication Action Identifier [CAI]) —These positions of the header are a combination of either four letters or three letters and one number. These combinations are used to indicate message content and to provide identification for communications handling. For example, in figure 1-2, the CAI in positions 5 through 8 is ZYUW. This identifies the message as a narrative message. A CAI of ZFH2 would mean that the message is being forwarded to the addressee for information only. A CAI of ZYVW would indicate that the message is a service message. A complete listing of these codes is found in JANAP 128.

Position 9 (Separator) —At this point in the header, the operator must press the space bar to insert the TTYcode equivalent for space on the message tape.

Positions 10 through 16 (Originator) —The appropriate routing indicator of the originating station is placed in these positions.

Positions 17 through 20 (Station Serial Number) —The station serial number (SSN) of the sending station is inserted here. The SSN serves two specific purposes. First, when used in combination with the originator's routing indicator, it provides positive identification for each transmission. Second, in the end of message (EOM) validation (discussed later in this section), the SSN appearing in format line 15 provides a means by which the ASCs can check for the existence of straggler messages.

The SSN is expressed in four numeric characters, beginning with 0001 and continuing consecutively through 9999. A new series begins when the number 9999 is reached. Operating stations may use SSNs to identify local activities, channels, or positions within a station by assigning each activity a specific block of numbers. For example, one station may be assigned numbers 0001 to 2000; the next station 2001 to 4000, and so on.

Position 21 (Separator) —This position requires the same information as that for position 9.

Positions 22 through 24 (Julian Date) —The Julian date is the date that the message was received from the originator for transmission by the communications center. The first day of the calendar year is Julian 001, and each day is numbered consecutively thereafter.

Positions 25 through 28 (Time Filed) —The time filed is the time that the message was received from the originator by the communications center for transmission. Each filing time is expressed in Greenwich mean time (GMT) and must contain four numerical characters.

Positions 29 through 33 (Classification Redundancy) —For security reasons, the classification designator used in position 4 is repeated here. Position 29 is filled with a hyphen as a sentinel. The classification designator in position 4 is repeated in positions 30 through 33.

Position 34 through end-of-routing signal (start-of-routing signal and addressees) —The positions reserved for routing are made up of two sections: start-of-routing signal and the addressees' routing indicators. The start-of-routing signal consists of two consecutive hyphens and will always precede the first addressee routing indicator. Addressee routing indicators are listed immediately following the start-of-routing signal. A message can have a maximum of 500 routing indicators in these positions. If a message contains 501 or more routing indicators, the message will require two separate transmission. In this case, all routing indicators that have the same first four letters should be in one transmission

End-of-Routing Signal —The end-of-routing signal consists of a period (.) and is inserted in the position immediately following the last addressee routing indicator.

SECURITY WARNING (FORMAT LINE 4). —A security warning is the first component of format line 4. The appropriate operating signal (ZNR or ZNY) will always be followed by a classification character repeated five times. The operating signal and classification characters are as follows:

ZNR UUUUU —For off-line encrypted messages and classified messages transmitted in the clear;

ZNY EEEEE —For unclassified EFTO messages; and

ZNY, followed by CCCCC, SSSSS, or TTTTT —For Confidential, Secret, or Top Secret messages, respectively.

For SPECAT and SPECAT SIOP-ESI messages, the five redundant security characters are followed by an oblique (/) AAAAA for SIOP-ESI or BBBBB for all other SPECAT messages. For example, format line 4 for a Top Secret SPECAT message would be:

ZNY TTTTT/AAAAA(2CR, 1LF)

END OF MESSAGE (EOM) (FORMAT LINES 15 AND 16). —Format line 15 is the EOM validation line that is used to inhibit suspected straggler messages. Format line 15 consists of the SSN in format line 2 preceded by the number sign (#). Format line 16 consists of the EOM functions. The EOM functions consist of normal teleprinter ending procedure when five-level Baudot code is used (2CR, 8LF, 4Ns, 12LTRS). However, for ASCII, 12 delete functions are used (12DEL). The EOM for the message with format line 2 shown in figure 1-2 would be as follows:

TEXT	(2CR, 1LF)
BT	(2CR, 1LF)
(1FIGS)#1234(1LTRS)	
(2CR, 8LF)NNNN(12LTRS)	

Format lines 1, 2, 4, and 5 must all be accurately prepared. Backspacing, lettering out, double-spacing, or using two or more FIGURES and LETTERS functions in sequence will cause the ASC to reject the message during attempted transmission from the originating station. The EOM validation appearing in format line 15 and the EOM function in format line 16 must be prepared in uninterrupted sequence, be letter-perfect, and be without corrections.

General Teleprinter Rules

A leader must precede the header to ensure acceptance and transmission of the first character of the message header. The leader for the five-level Baudot code (most common) consists of at least six blanks and six letter functions. The leader for the ASCII (eight-level Baudot code) consists of at least six nulls and six delete functions. This will ensure acceptance and transmission of the first character of the message header.

When a message is assigned dual precedence, the higher precedence is shown in format line 2 (position 1). Both precedences are shown in format line 5.

Communications personnel of tributary stations must ensure that a record is made of the time of file (TOF) and the time available for delivery (TAD). These times are used to determine message-processing times.

Message Lengths

Messages cannot exceed more than 20 lines of heading and text, beginning with format line 5. Messages that exceed the 20-line limit must be divided into pages for transmission. The second and succeeding pages of a message are identified by the page number, the routing indicator of the station of origin, and the SSN. The security classification of classified messages follows the page identification. After the first letter of the classification, you must separate each letter by one space from the previous letter. For example:

PAGE 2 RUEDABA0123 C O N F I D E N T I A L (2CR, 1LF)

On unclassified messages, "UNCLAS" is placed after the page identification with no spaces separating the letters.

When a message exceeds five textual pages, the message must be divided into transmission sections. The message should be separated at a convenient point on the last permissible page of a transmission section. This normally will be at the end of a sentence or cryptopart. Each section must be numbered in plain language at the beginning of the text following the classification or abbreviation "UNCLAS." For example:

UNCLAS SECTION 1 OF 2

In long encrypted messages, when a transmission section starts with a new cryptopart, the designation of the cryptopart follows the designation of the transmission section. Also, when a numerical group count is associated with an off-line encrypted message and is indicated in format line 10, the count must indicate the number of groups in the textual section being transmitted— not the number in the complete message. Cryptopart identification is included in the group count; the page identification and transmission section are not.

Statistical and meteorological messages can have up to 100 lines of text without paging when the inclusion of paging information would disrupt processing by the user. However, you should divide these types of messages into transmission sections if they exceed 100 lines of text.

Misrouted and Missent Messages

A misrouted message is one that contains an incorrect routing instruction. This normally occurs when the originating communications center assigns an incorrect routing indicator during message header preparation. Misrouted messages are usually not discovered until they reach the communications center of the called routing indicator. Communications personnel of a tributary station in receipt of a misrouted message must take the following actions:

- Obtain the correct routing indicator, if possible;
- Apply a header change to the misrouted message and retransmit it to the correct routing indicator; and
- Originate a service message to the originating station advising of the reroute action and the correct routing indicator.

A missent message is one that contains a correct routing indicator but is transmitted to a station other than the one represented by the routing indicator. Missent messages can be caused by an equipment malfunction, incorrect switching, or operator error. Communications personnel of a tributary station in receipt of a missent message must take the following actions:

- Reintroduce the message into the AUTODIN system as a suspected duplicate (SUSDUPE) after applying a header change; and
- Forward a routine service message to the connected ASC citing the complete header and time of receipt (TOR) and advising that the message has been protected.

Suspected Duplicates

When a station suspects that a message may have been previously transmitted, but definite proof or prior transmission cannot be determined, the message should be forwarded as a suspected duplicate (SUSDUPE) by applying a header change. However, if a station receives a message that is already marked "SUSDUPE," the station should file the message if the message was previously received and delivered to the addressee. If there is no indication that the message was previously received and delivered, it should be forwarded.

Stations receiving unmarked duplicate transmissions should immediately forward a routine service message to the originating station. This service message should cite the complete header format of the duplicated message, including the TOR of the original and duplicate transmissions. If the initial copy was delivered to the addressee, the station should file the message.

Upon receipt of service messages concerning duplicates, communications personnel at the originating station must take the following actions:

- Check transmission records to determine the validity of the duplication report;
- Ensure that in-station procedures are adequate to guide operating personnel in the retransmission of SUSDUPE messages;
- Have maintenance personnel perform equipment checks if an equipment malfunction is suspected to be the cause of duplication; and

- Advise the connected ASC by routine service message if only one transmission can be accounted for.

An ASC receiving notification of a duplicate transmission should search its records to determine if the message was received in duplicate. If the message was not received in duplicate, it must be traced on a station-to-station basis to determine the point of duplication.

Magnetic Tape Messages

Magnetic tape is one of the principal media used in electronic data processing equipments (EDPEs). Magnetic tape terminal stations (MTTSs) in the AUTODIN provide for the rapid exchange of large volumes of data in a relatively short period of time. The basic mode of MTTS operation with other AUTODIN tributary stations is either full duplex or on a store-and-forward basis.

In the continental United States, terminals that have compatible equipment and circuit speeds and are connected to the same ASC may communicate directly by Hybrid AUTODIN Red Patch Service (HARPS). HARPS provides a direct subscriber-to-subscriber encrypted circuit. HARPS uses the same circuit and equipment normally used in the message-switching component of the network. Communications centers not serviced by HARPS communicate by normal message switching, which automatically performs the necessary speed, format, and code conversions.

Operating Rules

All received tape reels must be periodically dismounted and made available for delivery as scheduled by a receiving activity and system manager. A magnetic tape reel accepted by a communications facility for transmission is screened and arranged for transmission according to majority message precedence levels contained on the reel. Establishment of transmission schedules is the responsibility of the commands concerned. Prior coordination is necessary to provide for efficient use of the equipment and circuit time. Schedules are limited to 30 minutes per period.

Most facilities establish their own procedures for maintaining reel accountability and ensuring that message transmission has been accomplished. Message header and EOT printouts are finished by the message originator with each reel of tape to be transmitted. If a message cannot be transmitted, the MTTS operator returns the reel to the originator, identifying the message (or messages) that could not be sent. The originator is also provided the reason for the nontransmission, if known.

Terminal equipment should not be used to change message media format for customer convenience; for example, changing from magnetic tape to narrative records.

Operating Precautions

Communications station master records, such as history tapes and journal records, remain with the communications facility until destroyed. History tapes are labeled to prevent them from being inadvertently delivered to addressees with live traffic tapes.

Recorded information is very close to the edge of the tape. Tape-edge indentations, caused by careless tape handling, will seriously affect the accuracy of magnetic tape recordings. You should be aware that tape splices are not permitted in reels of tape used for traffic.

Message Formats

Message formats used within the AUTODIN require that each message contain a message heading, text, and EOT record. The textual material on magnetic tapes may consist of a wide variety of information recorded in either structured or nonstructured formats, depending upon the type of system.

EOT is either a single N or four consecutive Ns. The header, text, and EOT cards of magnetic tape messages are always transmitted in the AUTODIN common language code (ASCII). This is accomplished by automatic code conversion logic provided in the magnetic tape terminal.

The text of magnetic tape messages can be prepared by the EDPE system in 80-character data images, series record images, or by variable-length record images. The length of data records to be transmitted by AUTODIN may vary according to user requirements. For general transmission of data throughout the system, computerized terminals must be capable of transmitting records that contain from 18 to 1,200 characters.

Subscribers desiring to transmit messages that contain fewer than 18 or more than 1,200 characters must ensure that the addressee is capable of receiving such records prior to transmission. Typical line formats of magnetic tape message records are described in JANAP 128.

Magnetic tape messages prepared for transmission are limited to a maximum of 40,000 characters (five hundred 80-character data records) that include the header, text, and EOT records. The preparation of magnetic tape messages, formats, routing, contents, and sequence on tape is the responsibility of the message originator.

Message and Tape Reel Accountability

Each tape reel given to the MTTS operator for transmission must bear a tape label containing the following information:

- Reel number;
- Number of messages recorded on tape;
- Highest precedence used;
- Highest security classification;
- Date and time filed;
- Tape density;
- LMF used;
- Beginning and ending SSNs; and
- Time delivered to the MTTS operator.

Each blank reel of tape furnished to the MTTS operator for mounting on the receive tape transport contains a tape label with the following information recorded in the sequence of handling:

- A statement that the reel is blank;
- Reel number;
- Highest classification ever recorded;
- Time the reel is mounted on the receive transport;
- Time the reel is removed from the receive transport;
- Time the reel is delivered to the addressee; and
- Number and types of message on the reel and other applicable reel information.

All originated tape reels must be retained for at least 10 days. The header and EOT printouts finished the MTTS operator for both originated and terminated traffic are maintained as a station communications record for at least 30 days. Other logs recommended for MTTS operation are the master station log and the reel delivery log.

The master station log reflects the current operation status of the terminal equipments and circuits. This log should also reflect equipment and circuit outages, causes of the outages, and the corrective actions initiated.

The reel delivery log should indicate the reel number and the time the reel was delivered to the transmitting operator or the addressee.

AUTODIN Security

Required security protection must be extended to all classified traffic transmitted through the AUTODIN. The ASC automatically checks and compares the security classification stated in the header of the message against the authorized security level of the incoming circuit. Transmission of a message with a higher security level than authorized will result in the message being rejected by the ASC.

In addition, an automatic system-generated service will be transmitted by the ASC to the originating station. The purpose of this service is to advise the originating station of possible security compromises. Also, the ASC automatically checks and compares the security classification contained in the header of each message against the security classification of each destination. A security mismatch occurs for each destination that does not indicate a matching security level.

In the event of a security mismatch, the ASC takes the following actions:

- In a single-address message, the ASC rejects the message and alarms appear at the originating terminal indicating that the message needs retransmission.
- In a multiple-address message with at least one deliverable destination, the ASC accepts the message and delivers it to all valid destinations. For invalid routing indicators, an automatically generated service retransmits the message to the originating routing indicator and advises that the message needs retransmission.

In-station operating procedures should be carefully planned and rigidly enforced to prevent inadvertent transmission of classified messages to unauthorized stations or agencies. Complete security precautions and operating rules are contained in JANAP 128.

NAVAL COMMUNICATIONS PROCESSING AND ROUTING SYSTEM

The Naval Communications Processing and Routing System (NAVCOMPARS) is an automated system that serves as the interface between AUTODIN or other networks ashore and operational units of the Navy. There are five NAVCOMPARS sites: NCTAMS EASTPAC, NCTAMS WESTPAC, NCTAMS MED, NCTAMS LANT, and NAVCOMMTELSTA Stockton, California. The primary purpose of NAVCOMPARS is to provide security, speed, and systems compatibility for the Naval Telecommunications System (NTS). The NAVCOMPARS system provides the following services:

- On-line communications with AUTODIN switching centers;
- On-line communications with tactical and dedicated circuits;
- Off-line communications interface capabilities;
- Processing of JANAP 128-formatted messages;
- Conversion of DD Form 173 messages to JANAP 128 format;
- Conversion of modified ACP 126-formatted messages to JANAP 128 format;
- Filing, retrieving, and accountability of messages;
- Local delivery analysis;
- Distribution assignment;
- Message store-and-forward capability to fleet units;
- Fleet support through broadcast management or full-period terminations and primary ship-shore circuits;
- Broadcast keying and screening;
- On-line communications with the Worldwide Military Command and Control System (WWMCCS); and
- On-line communications with Common User Digital Information Exchange System (CUDIXS) and Remote Information Exchange Terminals (RIXTs). (CUDIXS and RIXT systems are discussed later.)

Automation of these functions and services eliminates manual processing and minimizes related delays and errors. Automation also improves originator-to-addressee delivery time and allows the timely exchange of information critical to the command and control of forces afloat.

LOCAL DIGITAL MESSAGE EXCHANGE

The Local Digital Message Exchange (LDMX) provides automatic outgoing message routing and reformatting for Navy activities ashore. It simultaneously transmits and receives messages over the AUTODIN and other remote terminal circuits. The LDMX system provides high-speed processing, system reliability, secure communications, flexibility, statistical information, and accounting data.

High-Speed Processing

The LDMX system provides high-speed communications processing. On-line to AUTODIN and other circuits, the LDMX system automatically receives, identifies, and files traffic for processing and future reference. Incoming messages are automatically arranged by precedence; then processed, edited, and printed on reproducible mats for delivery.

Outgoing traffic is entered by magnetic or paper tape. The system formats the outgoing message, creates a header, and validates the message identifiers, precedence, and classification. The LDMX system also searches system files to assign the correct routing indicator and arranges the message by precedence for automatic transmission. Operating at full capacity, the system can process up to 7,500 messages per day.

System Reliability

Message-processing reliability has been greatly improved by automatic message identification and header preparation and by system look-up files instead of manual files. The elimination of most manual functions and validation of those remaining greatly reduce misroutes and nondeliveries. The system continues to operate in either a semiautomatic or manual mode if a major component becomes inoperable.

Secure Communications

All message security fields are validated. If a mismatch is detected in the LDMX system, the message will be displayed to an inrouter or an outrouter for

review and action. Depending on user requirements, video display terminal (VDT) operators may be prevented from displaying or recalling Top Secret and SPECAT messages. The purpose of this precaution is to reduce the possibility of a security violation.

Flexibility

The LDMX system eliminates most manual processing without imposing stringent limitations on the user. Tailored to meet the unique situations at each command, the LDMX can be responsive to individual command requirements and variances.

Statistical and Management Reports

A significant feature of the LDMX system is the natural accumulation of statistical information and accounting data. This provides accurate verification of the reliability and performance of the system. Message-processing data is summarized in a series of statistical analysis summaries that include the following:

- A bar chart providing an hourly volume of incoming or outgoing messages;
- A summary report showing the number and average length of incoming or outgoing messages, the number of messages delivered to a remote printer, and the number of classifications and precedences;
- A listing of service messages sent and received;
- A listing of duplicated, misrouted, and missent messages; and
- A speed-of-service report, giving maximum, average, and minimum processing times (by precedence, classification, or selected originator).

FLEET COMMUNICATIONS SYSTEMS

The systems for afloat units are compatible with those used ashore. Next, we will discuss the types of automated systems used afloat.

NAVAL MODULAR AUTOMATED COMMUNICATIONS SYSTEM

The Naval Modular Automated Communications System (NAVMACS) is a shipboard message-processing system developed to meet command missions. The NAVMACS provides accurate, secure, and expedient communications for various classes of ships and flagships. The hardware, software, and fictional capabilities of the NAVMACS are based on the needs of individual ships and commands.

The current versions of NAVMACS are (V)1, (V)2, (V)2-MPD (message-preparation device), (V)3, and (V)5/(V)5A. NAVMACS capabilities are augmented in a building-block manner from the most basic system, (V)1, through the most sophisticated system, (V)5/(V)5A.

NAVMACS (V)1

The NAVMACS (V)1 configuration provides automation for the receipt and processing of up to four channels of incoming broadcast message traffic. This configuration provides one channel of incoming and outgoing high-speed satellite link message traffic from and to the CUDIXS (discussed shortly). The system incorporates the equipments and computer program necessary to perform the automatic address screening and management functions required in the processing of incomming messages. It also incorporates the storage, formatting, and accountability functions used in the ship-to-shore delivery of messages transmitted via satellite and the shore-to-ship delivery of messages received via broadcast and satellite.

NAVMACS (V)2

The NAVMACS (V)2 configuration provides the same message processing and delivery functions used in the (V)1 configuration for up to four channels of incoming broadcast message traffic. It provides one channel of incoming and outgoing high-speed satellite link message traffic from and to CUDIXS. The NAVMACS (V)2 configuration upgrades the (V)l system in the following ways:

- Adds automatic MILSTRIP paper tape message processing;
- Adds message output to medium-speed printers instead of low-speed printers; and
- Uses magnetic tape program loading instead of paper tape loading.

NAVMACS (V)2-MPD

The NAVMACS (V)2-MPD configuration has the same capabilities as the NAVMACS (V)2 version but uses a different program for operator language and

system printouts. The MPD program provides an additional capability for on-line message composition and editing ability, and outgoing message error analysis (before transmission). It also provides a proof copy with paper tape for off-ship transmission. The (V)2-MPD system consists of the same equipments as the (V)2 system with the addition of MPD units, which are modified video displays.

NAVMACS (V)3

The NAVMACS (V)3 configuration automates certain processing functions required in the handling of narrative messages. It serves as an afloat terminal within those communications networks using broadcast and point-to-point modes of operation on both conventional and satellite transmission paths.

The (V)3 configuration interfaces with up to four channels of fleet broadcast, and up to four channels of full-period termination send-and-receive circuits. It also interfaces with one channel of incoming and outgoing high-speed satellite link message traffic to and from CUDIXS.

The (V)3 configuration also interfaces with off-line torn tape and manual transmit/receive circuits of any type. The (V)3 system provides the capability of on-line message composition and on-line message retrieval fom magnetic tape.

NAVMACS (V)5/(V)5A

The NAVMACS (V)5/(V)5A system is an automated communications processing system capable of interfacing a mix of input/output channels. This system is enhanced with the addition of remote terminals for message input. It includes up to four incoming broadcast channels and eight itinerant, netted, and fully dedicated communication network channels. It also includes one incoming/outgoing high-speed satellite link with CUDIXS and onboard peripheral devices.

The (V)5/(V)5A system includes a remote terminal capability for direct input/output of narrative and data pattern messages to high-volume onboard user areas. Remote terminals consist of a medium-speed printer, video display, and paper tape reader/punch, or a combination thereof, depending on the unique requirements of the various remote terminals.

COMMON USER DIGITAL INFORMATION EXCHANGE SYSTEM

The Common User Digital Information Exchange System (CUDIXS) provides a bidirectional, ship-to-shore-to-ship, high-speed digital data communications link between a ship and a NCTAMS or NAVCOMMTELSTA. Subscriber stations use the NAVMACS as their terminal. The link consists of a single Fleet Satellite Communications (FLTSATCOM) half-duplex channel. The link is dedicated to synchronous communications between the CUDIXS shore station (Net Control Station (NCS)) and the subscribers afloat. Each CUDIXS communications link can operate with up to 60 subscribers. There are two types of subscribers: special and primary.

Special subscribers are those ships that are assigned subscriber identification (SID) numbers 1 through 10. Special subscribers can send and receive narrative traffic to and from CUDIXS.

Primary subscribers are assigned SID numbers 11 through 60. Primary subscribers are restricted to a send capability only. They can receive their shore-to-ship message traffic via other means, such as the fleet broadcast or fill-period terminations. Both types of subscribers can send or receive operator-to-operator (order wire) messages.

CUDIXS/Subscriber Net Cycle

CUDIXS/subscriber communications are accomplished through a modified round robin network discipline. The basic round robin net operating concept transfers net control from one subscriber to the next on a prearranged basis, completing one net cycle when each participating subscriber has transmitted.

In the CUDIXS/subscriber modified round robin operating concept, transmission timing and scheduling are determined solely by the CUDIXS shore station designated the NCS. Each net cycle starts when the NCS transmits a Sequence Order List (SOL) along with narrative traffic and operator-to-operator messages. The SOL specifies the order in which each subscriber transmits during the next net cycle and the amount of time allocated each transmission slot. Each subscriber, in turn, will transmit at a time computed from information in the SOL.

A net cycle can range from 20 to 120 seconds, depending upon the amount of transmit time requested by the subscribers and the amount of data transferred.

System Performance/Message Accountability

CUDIXS provides a shore operator with several means of monitoring system performance and maintaining message accountability for all messages processed by the CUDIXS NCS. Specifically, the system assigns sequence numbers to all messages processed, provides link status, traffic statistics, and system summary information in system reports. The system also allows the operator to assign parameter values that control net operations and to generate various alerts concerning immediate communications difficulties.

System Interfaces

CUDIXS serves as an extension of AUTODIN by storing and forwarding messages, normally without need for human intervention. CUDIXS interfaces with AUTODIN via the NAVCOMPARS and processes narrative traffic for general fleet communications teleprinter messages.

In accomplishing its tasks, CUDIXS supplements the traffic responsibilities previously assumed by ship-to-shore and broadcast HF circuits. CUDIXS can recognize EMERGENCY COMMAND, FLASH, IMMEDIATE, PRIORITY, and ROUTINE messages on a first-in-first-out (FIFO) basis within precedence. Through system reports, the operator has the following capabilities:

- Detailed information on every message processed by CUDIXS;
- Overall statistics on the volume of message traffic processed over the link; and
- Information on the quality of link communications with each net subscriber.

COMMUNICATIONS DATA PROCESSING SYSTEM

The Communications Data Processing System (CDPS) provides the USS *Tarawa* (LHA-1) class ships with the necessary communications hardware and software to process narrative traffic and to ensure circuit reliability. CDPS is one of the most complex of the automated systems afloat and offers the following capabilities:

- Automatic broadcast screening;
- Frequency management;
- Automatic message logging;
- Automatic message continuity checks;
- On-line message preparation and storage;
- Backup control and operation;
- High-speed data interface;
- On-line operational readiness testing;
- Quality monitoring with computer aid;
- Message error analysis;
- Circuit status and record-keeping functions;
- Construction of communications circuits; and
- Ability to act as a CUDIXS special or primary subscriber.

As with many of the automated systems, the operator has the ability to modify system configuration from the control console. The operator must know how to properly use, operate, and perform system changes. Your job will involve setting up and operating input/output (I/O) devices. Some systems allow the operator to patch receivers, transmitters, modems, and antennas directly from the console.

As a Radioman, part of your routine duties will be to energize electronic equipment and monitor power levels. In the event of primary power failure, equipment must be brought up on emergency or back-up power systems. Many of the automated systems in use today have uninterrupted power sources (UPS) or battery backups to preclude a complete system failure.

For more information on power requirements for individual components, refer to the equipment technical or operator manuals. You should become familiar with emergency power requirements and procedures **prior** to an actual emergency.

SUBMARINE SATELLITE INFORMATION EXCHANGE SUBSYSTEM

The Submarine Satellite Information Exchange Subsystem (SSIXS) provides the commanding officers of SSN and SSBN submarines with an optional satellite path to complement existing VLF/LF/HF broadcasts. The subsystem provides a rapid exchange of teleprinter information between SSN and SSBN submarines and shore stations.

To use the SSIXS, the submarine must be in a line-of-sight position with a satellite. The submarine must also be in a tactical situation that permits exposure of its mast-mounted antenna.

The SSIXS provides access to a satellite path through a programmable mixture of query-response and broadcast-without-query functions. This type of access provides maximum operational flexibility to the submarine commander.

All transmissions on the SSIXS provide automatic, reliable, long-range, high-data-rate, and cryptographically secure UHF communications between submarines, and between submarines and shore stations.

AUTOMATED VOICE COMMUNICATIONS SYSTEMS

The telephone is and will continue to be a convenient and fast way to communicate. In this section, we will discuss the Secure Telephone Unit Third Generation and the Defense Switched Network (DSN), which is an updated version of the Automatic Voice Network (AUTOVON).

SECURE TELEPHONE UNIT THIRD GENERATION

The Secure Telephone Unit Third Generation (STU-III) is the newest communications system that meets the need for protecting vital and sensitive information over a telephone system. The STU-III is a compact, self-contained desktop unit capable of providing the user with clear and secure voice and data transmissions. The unit is fully TEMPEST protected and is certified by the National Security Agency for use up to and including Top Secret material.

The STU-III is unique in that it works as an ordinary telephone and as a secure telephone network to other STU-III terminals. For secure transmissions, the STU-III uses a unique keying system.

The three manufacturers of the STU-III terminals for the Navy are AT&T, Motorola, and General Electric. Figure 1-3 shows an AT&T STU-III terminal.

The STU-III is operated the same as any telephone. That is, you pick up the handset, wait for a dial tone, then dial the number of the person you want to call. All calls on the STU-III are always initiated in the clear voice mode. Once the party you have called has answered, you have the option of talking to that person in the clear voice mode, clear data mode, secure voice mode, or the secure data mode.

Terminal Setup

The STU-III terminal uses special keys with a designator of KSD-64A. The KSD-64A is a plastic device that resembles an ordinary key. Two types of keys are used with the STU-III, the seed key and the crypto-ignition key (CIK). The seed key is a special keying material used for the initial electronic setup of the terminal. The CIK key is used by the users to activate the secure mode.

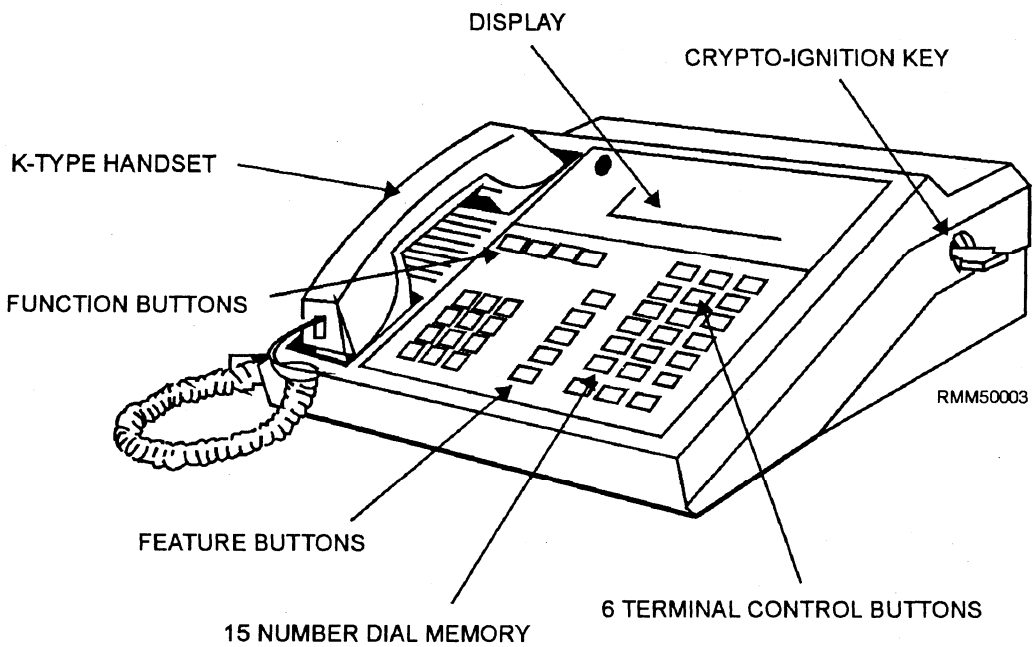

Figure 1-3.—AT&T STU-III terminal.

When the STU-III terminal is installed, the STU-III custodian sets up the terminal with the seed key. A seed key is issued to a particular terminal only. The seed key contains a microchip that is embedded electronically with identification information. This information includes the level of security authorized for that terminal.

Once the custodian inserts the seed key into the terminal, the information on the key is transferred to the internal memory of the terminal. At this point, the seed key no longer contains any information and is considered to be "empty."

The information in the terminal is electronically registered with the Key Management Center (KMC) located in Finksburg, Maryland. The KMC is the central authority responsible for controlling the key material and issuing reports of compromised keys. The user can discuss classified information up to the security level that has been keyed to the terminal.

The crypto-ignition keys (CIKs) can now be made for users to activate the secure mode. The CIKs are "empty" keys with no information embedded in the metal strip. When the empty keys are inserted into the terminal, some of the information that is now stored in the terminal from the seed key and other information in the memory is transferred onto the metal strips. This information becomes an electronic "password" on the CIKs for that particular terminal, making the CIKs unusable on other terminals. The terminal maintains a list of authorized CIKs for each key in its memory.

When using a STU-III with remote or dial-in, users parameters will be set according to the Secure Telephone Unit Third Generation (STU-III) COMSEC Material Management Manual (CMS 6) and locally generated instructions.

Levels of security classification, keying instructions, rekey instruction, CIK management will be decided by the user and the user's communications facility. All users must meet the minimum security clearance requirements.

Training on the STU-III will be documented in accordance with CMS 6 and local instructions.

Secure Mode

As we mentioned earlier, the secure mode of the STU-III is activated and deactivated using a CIK. When the CIK (figure 1-3) is inserted into the terminal, the STU-III can be used in the secure mode up to the classification of the keying material. Without the CIK, the STU-III operates as an ordinary telephone.

Calls are always initiated in the clear. To go from a clear to a secure voice transmission, either caller simply presses his or her SECURE VOICE button after the CIK is used to activate the secure mode.

Once a secure link has been initiated, the two STU-III terminals begin exchanging information. The information exchanged includes the identity of the CIK of the distant-end person, the list of compromised CIKS, and the common level of classified security information to which the two callers have access.

When two terminals communicate in the secure mode, each terminal automatically displays the authentication (identification) information of the distant terminal. This information is scrolled through the display window during secure call setup. The first line of the identification information and the classification are displayed for the duration of the secure call.

The information displayed indicates the approved classification level for the call, but does not authenticate the person using the terminal. Each terminal user is responsible for viewing this information to identify the distant party and the maximum security classification level authorized for the call.

STU-III Administration

The STU-III terminals and keys are COMSEC material. The terminals and keys may be administered either through the STU-III custodian or the CMS custodian. Both the terminals and keys are issued to users and must be signed for. Since the seed key is classified, it must be afforded protection for the level of classification in accordance with *Secure Telephone Unit Third Generation (STU-III) COMSEC Material Management Manual,* CMS 6.

Because CIKs permit the STU-III terminals to be used in the secure mode, the CIKs must be protected against unauthorized access and use. CIKs may be retained by the users who sign for them on local custody. Users must take precautions to prevent unauthorized access and must remember to remove the CIKs from the associated terminals.

When the terminals are unkeyed, they must be provided the same protection as any high-value government item, such as a personal computer. When the terminal is keyed, the terminal assumes the highest classification of the key stored within and must be protected in accordance with the classification of that key.

DEFENSE SWITCHED NETWORK

The Defense Communications System (DCS) Defense Switched Network (DSN) is a telecommunications telephone interconnected network. This system is found on most military and other Federal Government installations in the United States and overseas.

This system upgraded the Automatic Voice Network (AUTOVON) and will evolve into an all-digital network in the 1990s. The DSN incorporates capabilities that were not available in the AUTOVON system, such as automatic callback, call forwarding, call transfer, and call waiting.

Precedence of Calls

The precedence of a call indicates the degree of preference to be given a call relative to all other calls in progress. A preemption feature provides the ability to disconnect a call of lower precedence and seize the access line or interswitch trunk to complete a call of higher precedence. A unique aspect of the DSN is that switches have been programmed to determine what precedence treatment must be given each call.

The combined features of precedence and preemption used in DSN are called multilevel precedence and preemption (MLPP). The effectiveness of this system depends on the proper use of the precedence system by the users.

All users should be familiar with the system and the types of calls assigned to each precedence. Each user should ensure that his or her call is not assigned a precedence higher than that justified by the circumstance or information involved.

The DSN offers five types of call treatment. The precedences and their applications are listed below in relative order of priority in handling.

FLASH OVERRIDE (FO) —FO takes precedence over and preempts all calls on the DSN and is not preemptible. FO is reserved for the President of the United States, Secretary of Defense, Chairman of the Joint Chiefs of Staff, chiefs of military services, and others as specified by the President.

FLASH (F) —FLASH calls override lower precedence calls and can be preempted by FLASH OVERRIDE only. Some of the uses for FLASH are initial enemy contact, major strategic decisions of great urgency, and presidential action notices essential to national survival during attack or preattack conditions.

IMMEDIATE (1) —IMMEDIATE precedence preempts PRIORITY and ROUTINE calls and is reserved for calls pertaining to situations that gravely affect the security of the United States. Examples of IMMEDIATE calls are enemy contact, intelligence essential to national security, widespread civil disturbance, and vital information concerning aircraft, spacecraft, or missile operations.

PRIORITY (P) —PRIORITY precedence is for calls requiring expeditious action or furnishing essential information for the conduct of government operations. Examples of PRIORITY calls are intelligence; movement of naval, air, and ground forces; and important information concerning administrative military support functions.

ROUTINE (R) —ROUTINE precedence is for official government communications that require rapid transmission by telephone. These calls do not require preferential handling.

Security

Local command policy normally states that the DSN is to be used only for the most essential official calls. The DSN system must never be used to make personal or unofficial calls.

Telephone circuits, particularly those routed by high frequency and microwave, are susceptible to monitoring and interception. **The DSN is not a secure system!** Users must take care and use common sense to avoid divulging classified information. Giving hints or talking "around" a classified subject can lead to the compromise of classified information.

TRANSMIT MESSAGES VIA MANUAL CIRCUITS

In these days of super speed burst message transmission the use of manual relaying or transmitting of messages is not the norm. You should locate, identify, and use locally produced instructions, publications, and references.

ENEMY CONTACT REPORTING

Enemy contact reports are normally made only once when you are in direct communications with the officer in tactical command (OTC), a higher authority, or a shore radio station. Enemy contact reports are signaled using basic R/T procedures as modified by chapter 6 of ACP 125. Details of enemy contact

reporting are contained in *Allied Maritime Tactical Instructions and Procedures,* ATP 1, Volume I. There are two conditions under which enemy contact reports are to be made more than once:

- When DO NOT ANSWER procedures are used (texts are transmitted twice in this procedure).
- When the text consists of emergency alarm signals. In this case, the text is transmitted twice, separated by the proword I SAY AGAIN, with a time group in the ending.

When required, authentication is used in contact reports. Lack of proper authentication, however, should not prevent retransmission or relay of the message to higher authority.

There are two types of contact reports: initial and amplifying. As you would expect, initial reports are used to report initial contact or sightings. These reports should be sent as expeditiously as possible with immediate, pertinent information (type vessel, location, basic track, and so forth). The amplifying reports contain all necessary amplifying information to be fully analyzed by higher authority or command.

CODE AND CIPHER MESSAGES

Code words, such as VERDIN in the text EXECUTE PLAN VERDIN, are sent as plain language words. Encrypted groups, such as DRSRM, are spelled phonetically: DELTA, ROMEO, SIERRA, ROMEO, MIKE.

The phonetic alphabet is used for the names of signal flags as well as for spelling words, letter groups, and so on. Signal flags are combined into code groups that have meanings of their own. DELTA ROMEO ONE, for example, might mean "prepare to hover." Signal flag A is ALFA, flag B is BRAVO, and so on. Meanings of such code groups are given in appropriate signal publications.

Because flag signals are also sent by R/T, you must be able to differentiate between the two uses of the phonetic letters when you hear them. Here is the way—if the phonetic alphabet is used, the proword I SPELL precedes it and each phonetic letter is recorded as a letter. If you hear I SPELL, followed by DELTA OSCAR, write it as DO. On administrative nets, the proword SIGNALS, followed by DELTA OSCAR, means the groups have been taken from a signal book and should be recorded as such. Prowords are not used on nets used primarily for conveying signals. Therefore, you may assume that alphabet flags are intended.

The duties of an R/T operator require a knowledge of the special language developed for tactical maneuvering, air control, antiair warfare, naval gunfiie support, electronic countermeasures, antisubmarine warfare, and other specialized uses. Words, phrases, and abbreviations used in R/T for these specialized uses are called operational brevity codes. A complete list of operational brevity code words is found in *Operational Brevity Codes,* ACP 165.

You should understand that the words and phrases of the brevity code provide no communications security. The purposes of the codes are to:

- Standardize the vocabulary;
- Improve the accuracy of the transmission; and
- Shorten transmission time.

AUTHENTICATION

Authentication is a security measure designed to protect a communications system against fraudulent transmissions. There are specific times when you will have to use authentication procedures. Several types of authentication systems are in use, and the method of authentication will vary with the system that you are using. Authentication systems are accompanied by specific instructions outlining the method of use. You can find more information about the types of authentications and specific reasons when and why to use the authentication process in *Communications Instructions—Security (U),* ACP 122, and in NTP 5.

COMMUNICATIONS CENTER ADMINISTRATION

We will now show you some of the basic logs, command guard list (CGL), and changing call signs that deal with communications center administration. These short instructions are in no way a complete list of communications center operations. Each command has its own check-off lists or SOPs of how their command runs its center.

CIRCUIT BACKLOGS

Each circuit operator will notify the supervisor when the circuit status changes, when a backlog of traffic develops, when an outgoing transmission is delayed, or when any deviation from prescribed

procedures is recognized. Circuit operators will report the backlog or potential for backlogs (logged-out equipment, poor reception) to the supervisor, who will in turn pass the information up the chain of command to the CWO and will also log the information into the master station log (MSL).

When relieved, the circuit operator will pass on information pertaining to the circuit(s), when it is not covered in the circuit status standard operating procedures.

A broadcast form provides for the number of messages received, the classification of the message, and also provides a record of destruction for classified message traffic. A check-off sheet (stock number 0196-LF-301-2350) is available through the supply system for keeping a record of broadcast numbers received and transmitted.

COMMAND GUARD LISTS

Each command is responsible for maintaining an accurate list of all AIGS, CADS, general messages, and task organization assignments required to fulfill its mission, and to supply this guard list to a serving communications center.

The command guard list must be verified with the communication plan to ensure that it is accurate and any discrepancies are corrected prior to updating. This is normally done when a change in tasking, operating area, or mission occurs.

DAILY CALL SIGNS

FLTCINC communications operating plan will prescribe the specific form of call sign to be employed based on the network used and operating conditions.

Call signs are to be used when first establishing a net, when reporting into a previously established net, and in the transmission and address components when a message is required to be relayed to a station that is on a different net.

Daily call signs, by their very name, direct you to change the call signs daily, using various issued publications. Refer to local operating instructions for instructions on how to verify the type of daily call signs you are using for specific situations.

MASTER STATION LOG (MSL)

The MSL is the official narrative record maintained to record significant events (e.g., power failures, complete system outages, major equipment outages or impairments such as HAZCON'S and any other event that may have an impact on operations, time verification, shift or watch changes, special tests, etc.). Every communication space must maintain a Master Station Log.

Entries must be made in chronological order. The shift or watch supervisor is required to sign the log when logging "on" and "off" duty and at the end of the RADAY.

If the MSL is an automated log, it shall be designed so that it does not allow alternations. For manual logs, a hard copy of the MSL must be filed at the end of each RADAY. MSLs must be retained for a minimum of 12 months.

THE COMMUNICATIONS PLAN

The communications plan satisfies the communications requirements of an operation. It specifies circuits, channels, and facilities to be used and stipulates the policies and procedures that are applicable. The plan is, in effect, an assignment of communications tasks to be performed by subordinate commanders or by supporting commands.

The planner first establishes requirements for communications and then determines the best means for satisfying them. This process may reveal shortages or inadequacies in what is available. If inadequacies are identified, it may become necessary to share circuits or facilities, as well as to merge or consolidate requirements. All possibilities should be considered to support valid operational requirements.

In planning communications, the planner must evaluate such factors as the performance, capabilities, and capacities of systems and facilities, as well as the personnel. These factors are merely guides and averages. They represent the sum result of experience in previous similar situations, and are considered only after any local factors are determined. These factors change from time to time and must all be available for final determination of communications requirements.

QUALITY CONTROL

The AN/SSQ-88/A/B system was designed to provide a means of monitoring and evaluating performance of any communications system used by forces afloat. You will utilize this system with RCS interface as well as various other types of monitoring systems; for example, oscilloscopes, meggers, and visual, just to name a few.

You will be checking for various signal quality characteristics, including dc distortion, audio distribution levels, frequency accuracy of RF signals, spectrum analysis and loop current. Those measurements are broad categories and can be broken down to specific tests for specific systems.

You will correct all discrepancies, complete the appropriate reports, and send them to the proper authority or file them for further reference.

CIRCUIT SETUP/RESTORATIONS

RADAY is the start of a new 24-hour period. At that time all designated systems will restart. It can be a crypto restart, the simple methods of starting (opening) a new log, or message numbering system, starting at the number 0001.

RADAY starts at 0001Z worldwide. The 0000Z time frame does not exist and **WILL NOT** be used. The following restart items is a rudimentary list to give the user an idea of areas and items that require restart at the beginning of the new radio day.

DETERMINE COMMUNICATIONS PROTOCOLS

Protocols are generally set by the CINCs, area commander, Naval instructions, and local instructions. Protocols are also determined by the mission and the area of operations.

COMMUNICATIONS CIRCUITS

The use of communications circuits require that those circuits at various times of the day be placed online, in reserve, or taken offline. The reasons have to do with whether the circuit is needed immediately, or can be placed on ready reserve for use, or if the requirement for that particular circuit has expired.

Activate

Activating communications circuit usually means turning on or starting a circuit to allow for communications signals to ride (or pass) on them. When a circuit is activated, it will be logged in an active status on the status board. A circuit can be activated for any number of reasons, including special communications, overload, or installation of a new circuit path.

Deactivate

To terminate or deactivate a circuit is to stop using that path and remove all your equipment from that particular path. The deactivated circuit is then logged out on the status board.

Standby

By placing communications circuits standby, you are placing them in hold. They are ready for activation or deactivation should the need arise. Again, this type of circuit is placed on the status board so that the supervisor knows the status of each of the circuits under his control.

SHIFT FREQUENCIES

Shifting frequencies or changing frequencies is accomplished to allow for stronger propagation of the circuits. When the signal strength begins to decay, the operator will shift frequencies to another or stronger frequencies in accordance with naval and local instructions.

TRANSMIT OR RECEIVE CRYPTOGRAPHIC KEYING MATERIAL VIA OTAT/OTAR

Some of the new cryptosystems will use a 128-bit electronic key that is called over-the-air-rekey (OTAR) or over-the-air transfer (OTAT). Using this system reduces the amount of physical keying material held on board a command.

The key can be extracted using a KYK-13 or KYX-15/KYX-15A. The key is then loaded into another cryptosystem.

For amplifying information, refer to *Procedures Manual for Over-the-Air Transfer (OTAT) and Over-the-Air Rekey (OTAR) and Field Generation and Over-the-Air Distribution of Tactical Electronic Key*, NAG-16/TSEC.

ANALYZE NETWORK CAPACITY AND RELIABILITY

When trying to analyze a network's capacity and reliability, you must first establish the criteria or level at which you wish the system to work. Does the network have set boundaries, or can it be expanded to include updated or new parameters? Many avenues can be

explored to find the most efficient methods and levels at which a network can work.

Accurate documentation is a key factor for showing the user what, where, total numbers, and reliability of the network.

You will find that with the correct numbers you can see where a system or network is falling short or surging ahead of the set projection data.

SUMMARY

In this chapter you have been introduced to communications systems, networks, and administration concerns in their most basic forms.

Not all of our work is concerned with strategic or tactical operations. Establishing circuits or networks, quality control, and the various operations of the STU-III are just a few of the many facets of our complex and diverse jobs.