



LB-31600

Mobile Communications

VOICE GUARD[®]
DIGITAL SPEECH ENCRYPTION

System Manual

TABLE OF CONTENTS

INTRODUCTION	6
CHAPTER 1	7
SUMMARY OF VOICE GUARD METHODS	7
Types Of Voice Security	7
Frequency Domain - Analog	7
Time Domain - Analog	7
Digital	7
Levels Of Security	7
Voice Guard Product Line - Overview	8
Algorithm	8
Package Configurations	8
Station Configurations	8
Mobile Configurations	8
Portable	9
Specification Sheets	9
Station Field Upgrade	9
Jargon List	9
CHAPTER 2	13
SECURITY/KEY MANAGEMENT	13
Security And The Keys	13
Data Encryption Standard (DES)	13
VGE Algorithm	13
FED-STD-1027	13
Key-Entry Requirements	13
DES	13
VGE	14
Key Loader (19A148910)	14
Features	14
Keyloader Options	15
Group Option	15
Destination Option	15
Keyloader Tests And Responses	15
DES (19A148910P1)	15
VGE (19A148910P4)	16
Key Loader Error Messages	16
Key Management	17
Operational Security	17
Key Loader	17
Mobile And Station	18
Personal	18
MPS	18
M-PD	18
Mechanical Key Security	19

TABLE OF CONTENTS CONT.D

CHAPTER 3	21
GE OUTSIDE ADDRESSING	21
Outside Addressing	21
Concept	21
Mobile	21
Personal	22
MPS	22
M-PD	22
DELTA Desk-Top Stations	22
End-To-End Stations And Repeaters	22
Station Shelf Configuration Switches	22
Console Interface Unit (CIU) - Tone control only	23
Channel Guard Monitor	23
E/D Remote Only Station	23
E/D Remote/Repeat Station	23
System Applications	24
Notes And Comments	25
CHAPTER 4	27
VG TRANSMISSION CHARACTERISTICS / TEST METHODS	27
System Parameters	27
Control Line Characteristics	27
Remote Control Circuit	27
Typical Line Specifications	28
Voice Grade (2000)	28
Data Grade (3000)	28
Digital Transmission - Radio	28
Data Filtering - Radio	29
Eye Pattern Display - Two Level Data	29
Station Receiver Data Mods	29
Digital Transmission - Wire Line	31
Data Modems - General	31
Voice Guard Wire Line Modems	31
Wire Line - Diagnostics	32
Data Polarity	32
Standard	32
Inversion	32
Inversion Test Method	36
Test Equipment Verification	36
Transmitter Polarity Determination	36
Receiver Polarity Determination	36
VG Test Device	36
Expected Performance Deviations	37

TABLE OF CONTENTS CONT.D

CHAPTER 5	39
VG SYSTEM HARDWARE AND CONFIGURATION	39
System Configuring	39
General Discussion	39
Encryption	39
Line Requirements	39
Outside Addressing	39
Multi-Frequency Operation	40
Channel Guard Operation	40
Voice Guard Station Shelves	41
GETC Configuration	43
Console Interface Unit	46
Voice Guard Modules	46
Repeater Configuration	47
End-To-End Encryption Configurations	47
Remote Only	48
Remote/Repeat	48
Voted Remote	49
Voted Repeat	49
Voted Remote/Repeat	51
Satellite Receiver	51
Station Field Upgrade	51
Mods Common To All Stations	51
End-To-End Station Modifications	51
RF-Only Encryption/Decryption Configurations	52
E/D Remote-Only - Options (9783,9784,9785,9789,9790,9797)	53
E/D Remote/Repeat - Options (9786, 9787, 9788)	53
Decrypt Satellite Receiver	54
E/D Voted Systems	55
E/D Station Modifications	55
Mobiles	57
DELTA S/SX	57
RANGR	57
Dual Control	58
Portable	58
MPS	58
M-PD	58
System Checkout	58
Mobiles And Portables	58
Voice Guard Station Shelf - Options 9780 & 9781	59
Status Display	59
Receiving Function	59
LED Observation	59
Interrupt Line Observation	60
Transmitting Function	60
Voting Receiver	60
Voting Selector	61
Telephone Line Setup	61
Data Polarity Consideration	61
Level Setting Criteria	61

TABLE OF CONTENTS CONT.D

Intelligibility General	62
VG-9600	62
M-PD	62
Console Applications	62
CHAPTER 6	65
VG VOTING SYSTEMS	65
Voice Guard Voting	65
Introduction	65
Analog Voting Methodology	65
Digital Voting	65
Voice Guard Voting Methodology	65
Voice Guard System Hardware	65
Satellite Receiver	65
Description	65
Operation	66
Digital Voter	66
Description	66
Operation	66
Interface Adapter	67
Voting Station - Description	67
Console Interface Unit	67
Description	67
Operation	68
Remote Keying Panel (RKP)	68
Function	68
Modification Summary	68
Operation	69
System Configurations	69
Voted Remote	69
Analog Operation	69
Voice Guard Operation	70
Voted Remote/Repeat	70
Analog Operation	71
Voice Guard Operation	71
Voted Repeat	71
Unique Characteristics	71
CHAPTER 7	77
VG PUBLICATIONS	77
APPENDIX A	
"Design and Performance of a Digital Voice Privacy System for Land Mobile Radio" G.D. Rose, S. Kappagantula 36 th IEEE Vehicular Technology Conference - May 86	
APPENDIX B	
Federal Standard FS-1027, 14 April 82	

INTRODUCTION

As the process of Voice Guard instruction book writing progressed, it became clear that the application of General Electric Voice Guard as well as the whole subject of digital voice privacy system planning needed to be addressed in more detail. It also became apparent that no single document existed which could support the all encompassing collection of material needed for good voice privacy systems planning. Thus - the birth of the Voice Guard System Manual.

Chapter 1 contains a quick exposure to the various methods by which voice privacy can be obtained and a summary of the Voice Guard product line. Chapter 2 covers the subject of "security" and addresses key management as it applies particularly to Voice Guard. Chapter 3 covers the concept and application of the unique GE "Outside Addressing" capability. Chapter 4 addresses the required Voice Guard transmission characteristics and test methods associated with transmitting digital data. Chapter 5 covers Voice Guard system hardware and system configuration information and, Chapter 6 addresses the subject of Voice Guard voting systems.

In addition, appendices contain a reprint of an IEEE convention paper on the subject of Voice Guard and a reprint of Fed STD 1027.

This system manual is intended for use by both newcomers and those experienced in the subjects of digital transmission and voice privacy. It is also intended that it be used by systems planners and users alike.

CHAPTER 1

SUMMARY OF VOICE GUARD METHODS

TYPES OF VOICE SECURITY

There have, for a number of years, been a variety of methods available for providing Voice Security (VS) capability on land mobile radio systems. The techniques employed usually fell into one of three categories. These were: frequency domain, time domain or digital. The individual VS products varied in the number of available unique codes, in required circuit complexity and in the level of security that each provided. The following discussion is meant to only describe some of the various approaches and is not intended to be an all-inclusive listing of Voice Security equipment.

FREQUENCY DOMAIN - ANALOG

The first and simplest attempt to provide a VS add-on to land-mobile radio was the frequency inversion technique. This involved applying the 300 to 3000 Hz voice band to the input of a balanced modulator being switched at 3.3 kHz, and then passing only the lower sideband products on to the radio. This had the effect of turning over (inverting) the voice spectrum in the frequency domain. There was effectively only one code and not much technical sophistication was needed for someone to monitor the transmissions. This method provided almost no security and can be considered as the lowest on a list of perceived levels of voice security.

Another method of frequency domain scrambling involved breaking up the 300 to 3000 Hz band into several frequency sub-bands by means of individual filters and then shifting these bands into different spectral positions. An adaptation of this dynamically changed the spectral position of the sub-bands every few seconds. While these techniques could provide more than just one coding combination, the number of available code combinations was still relatively small. In addition, since the syllabic intervals of the speech and, to some degree, voice intonation were not materially affected, much information could be gained by monitoring the VS transmissions even though they were not decoded. Furthermore, a dedicated adversary would not have too much difficulty in decoding this type of VS. Hence, this type of VS would still rate very low on the perceived levels of voice security.

TIME DOMAIN - ANALOG

Time domain VS generically involves taking 1/2 to 1 second major intervals of speech, dividing these intervals sequentially into a number of smaller intervals, and then scrambling the small intervals prior to transmission. The arrangement of the small intervals can be changed dynamically for each major

interval. A very large number of rearrangement plans or encryption codes can be made available thus making complete decoding of the VS signal by an adversary quite difficult. However, as with frequency domain systems, the time domain VS systems still do not totally mask the inter-syllabic gaps in speech and voice intonations even though the text of the transmission may be more difficult to decode. Thus considerable information can still be gained such as: anxiety in the speaker's voice, whether it is a man or woman, or different speakers.

Even though time domain VS has shortcomings similar to those of frequency domain VS, time domain VS would rate better on a list of perceived levels of voice security.

DIGITAL

While several different implementations of digital VS exist, the basic approach is similar for all. The analog speech to be transmitted is first digitized. This string of real-time ones and zeros is then scrambled in accordance with some predetermined plan and then, after appropriate filtering, directly transmitted. This transmitted modulation has a white noise sound throughout the transmission. There is no perceived change in the sound of the modulated signal whether there is any analog speech being processed or not. Hence, there is total masking of the speech, inter-syllabic intervals and intonations. The only information to be gained by an adversary would be that a VS transmission is in progress and perhaps some indication of RF signal strength. These methods of VS would occupy the highest place on a list of perceived levels of voice security.

LEVELS OF SECURITY

The following is a list of relative levels of perceived voice security as provided by some of the various VS methods:

1. Simple Frequency Inversion - Least secure
2. Frequency Band scrambling
3. Dynamic Frequency Band scrambling
4. Time Domain scrambling
5. Dynamic Time Domain scrambling
6. Digital scrambling - Most secure

Of the above generic methods of providing voice security, those that can support a large number of unique encryption combinations or codes provide a higher level of security than those that support a small number of codes. For example, if a particular system can only support a small number of codes (ie. 255), it is not a very difficult job to tape record a segment of an encrypted transmission and then play it through a test setup and try each of the 255 code combinations until the correct one is found. This is called an "exhaustive search". As the number of available code combinations gets up into the billions and

greater, an exhaustive search becomes very time consuming, thus less effective. Some encryption systems can provide of the order of 10 to the 19th power available codes.

VOICE GUARD PRODUCT LINE - OVERVIEW

ALGORITHMS

Voice Guard can be provided with either of two different encryption algorithms. These are DES (Data Encryption Standard) and VGE (Voice Guard Encryption). The algorithms are the mathematical manipulations used to scramble the digitized voice bit pattern. Both algorithms offer the user a high level of voice security by virtue of the extremely large number of available cryptographic keys. DES has 7.2 times 10 to the 16th power and VGE has 1.8 times 10 to the 19th power cryptographic keys that are user selectable by means of cryptographic key variable loaders. In addition, VGE also has a customer unique encryption (CUE) code that provides another layer of security. The CUE is a second 64 bit word that a user can uniquely set with a TQ-2310 programmer so that even if an adversary has obtained the cryptographic key in use, he still cannot decrypt a VGE transmission without also having the CUE. The DES algorithm versions are generally not available for export outside the United States. The VGE algorithm version is exportable, but only with a valid U.S. State Department, Office of Munitions Control (OMC) export license. Separate cryptographic keyloaders are required for the DES and VGE algorithms. One type of keyloader will not work with the other type of algorithm.

PACKAGE CONFIGURATIONS

Voice Guard units for application with mobiles and stations are available in two basic package configurations. The one most used by U.S. Federal Government agencies has FS-1027 endorsement. This endorsement means that the equipment operates with the DES encryption algorithm in accordance with the specific requirements of FED-STD FS-1027 and has been endorsed by the National Security Agency (NSA).

The second available Voice Guard module package for mobile and station application does not possess the physical security of the FS-1027 endorsed package. Versions containing the DES algorithm are available in the non-1027 endorsed package. Voice Guard modules with the VGE algorithm are only available in the non-1027 endorsed package.

Portables and the cryptographic keyloader are exempted from some of the physical security requirements of the mobile and station equipment. However, they must meet the DES and most of the electrical requirements. MPS and M-PD portables equipped with DES Voice Guard have FS-1027

endorsement while those equipped with VGE Voice Guard do not meet the FS-1027 requirements.

STATION CONFIGURATIONS

Voice Guard MASTR II stations are available with elements to provide end-to-end encryption between users or between a user and a control point; or RF only encryption (E/D stations) with the station to control point link always being unencrypted (clear).

In end-to-end encryption, the voice is encrypted at the control point and remains encrypted all the way to the properly equipped mobile or portable radio. A Voice Guard module is connected to a console interface unit which is located at or nearby a dispatch center. The four-wire interconnection to a base station is encrypted when operating in the guarded mode. The four-wire interconnection with one or more consoles is always in the clear mode. This assumes that the dispatch center is secure and that the CIU/console interconnection will be by short, local cable runs that are adequately secure.

In RF only encryption, a Voice Guard module is connected to an RF base station. The voice signal is always delivered clear (unencrypted) from the dispatch center to the base station where it can then be encrypted and sent over the radio path to properly equipped mobiles and portables. One or more station consoles operate in essentially a standard clear mode, tone control configuration.

Voice Guard DELTA desk top stations are also available with the VGE algorithm or either package version of the DES algorithm.

MOBILE CONFIGURATIONS

The Voice Guard modules for mobile applications are the same as those used for station applications except that the VG module case has a mounting support on top for supporting a control unit bracket. In the station applications, the VG module case does not have the control unit mounting support.

Voice Guard can be operated with DELTA-SX and DELTA-S high band and UHF radios that have a Voice Guard mobile interface board installed. The radios will operate normally in the clear mode with the mobile interface unit installed but without a Voice Guard module. All Delta-SX radios are Voice Guard ready as shipped from the factory. Voice Guard is also available on RANGR mobile radios.

The Voice Guard module will operate with an S550, S950 or S990 control unit and is capable of supporting 32 independent transmit and receive outside addresses that track with the radio channel frequency selector. In addition, the

S950 and S990 control units also have a channel frequency storage capability of 128 channels and the ability to down load these in 4 blocks of 32 to the DELTA radio on command.

The outside addresses, data polarity, alert tones and attack times may be programmed into the Voice Guard unit using a TQ2310 universal programmer that is equipped with a Voice Guard PROM TQ-2344 and cable TQ-2322. The cryptographic keys must be loaded with a Keyloader 19A148910 (P1 for DES and P4 for VGE).

PORTABLE

The Voice Guard equipped M-PD and MPS portable radios only come in two versions, the DES FS-1027 endorsed and VGE versions. Because a portable radio is under the personal control of the user, there is no requirement for keylocks. Therefore, there is no DES, non-1027 version of portable radio available.

SPECIFICATION SHEETS

See the "Voice Guard System Guide", ECR 3398, for a complete list of Voice Guard system specification sheets.

STATION FIELD UPGRADE

MASTR II stations for both end-to-end and RF only (E/D) encryption are not only available from the factory but can also be field modified to support Voice Guard operation. See Chapter 5 for more information.

JARGON LIST

Voice Guard is a unique product involving a number of new techniques. This, of necessity, brings forth a number of new terms and abbreviations. The following list is an attempt to tabulate and define some of the more common of these terms and where they might be used.

NAME	DEFINITION	ASSOCIATION
BAUD	A single data element per second	data format
BIT	Single two-level element of data	data format
CG	Channel Guard (CTCSS)	receiver/TX
CAS	Carrier activity sensor	receivers
CIU	Console Interface Unit	stations
CODEC	Analog/digital encoder-decoder	VG module
COR	Carrier operated relay	voter
CPTT	Combined push to talk	transmitters
CTS	Clear to send	data modem
DELTA	GE mobile radio product line	
DES	Data Encryption Standard	encryption
DPTT	Delayed push to talk	transmitter
E/D	Encrypt/decrypt or RF only	
EEPROM	Electrically erasable PROM	stations
EOM	End of message	VG module/radio
GETC	G.E. Trunking Card- Updated VG control shelf	data format
GMSK	Gaussian minimum shift keying	stations
ICOM	Oscillator module	VG module
IFAS	IF-Audio-Squelch	stations
IV	Initialization vector	receiver
KEY	Cryptographic key	encryption
LPTT	Local push to talk	encryption
MASTR	GE station product line	transmitter
MODEM	Module to send 9600 baud data over a 4-wire line or eqv.	
MODEM IC	Interfaces serial NRZ data to VG microprocessor	stations
MIF	Mixer-IF	units using VG
M-PD	GE personal radio product line	receiver
MPS	GE personal radio product line	
OA	Outside address	VG module
PROM	Programmable read-only memory	VG module
PTT	Push to talk	transmitter
RAM	Random access memory	
RANGR	GE mobile radio product line	
RemPTT	Remote push to talk	transmitter
RKP	Remote Keying Panel	voter
RptPTT	Repeater push to talk	transmitter
RTS	Request to send	data modem
RUS	Receiver unsquelched sensor	receiver
SBC	Sub Band Coder	VG module
SECURIT	2175 Hz TX control tone	transmitter
SIMON	Simple MONitor	VG module
Sync	Synchronization word	data format
TX Aud	Clear audio to TX audio switch	VG module
TX Data	VG data to TX audio switch	VG module
TX Mod	Modulation to TX modulator	VG module
TQ-2310	Universal Radio Programmer (URP)	VG module/TX

NAME	DEFINITION	ASSOCIATION
VG	Voice Guard	
VG-9600	Voice Guard DES mobile/station	module
VGE	GE proprietary encryption algorithm	
VGE-9600	GE proprietary encryption mob/stn	module
VS	Voice security	
4-wire	Data grade 4-wire control line	modem

(This Page Intentionally Left Blank)

CHAPTER 2

FED-STD-1027

SECURITY/KEY MANAGEMENT

SECURITY AND THE KEYS

DATA ENCRYPTION STANDARD (DES)

The DES or Data Encryption Standard is a public domain encryption system that is described in the U.S. Department of Commerce, National Bureau of Standards publication FIPS PUB 46, titled: DATA ENCRYPTION STANDARD. DES employs a 64 bit cryptographic key, 56 bits of which are used for encryption and the remaining eight bits are parity bits. This results in 7.2×10^{16} unique cryptographic keys being available. The security of a DES equipped system comes about because of this extremely large number of available keys, in that the key is the only unknown element in a DES equipped system. It has been estimated that to accomplish an exhaustive search of the available DES keys, employing a high speed computer, would require many tens of years.

The U.S. Government presently prohibits from general export, communications gear equipped with the DES encryption algorithm. DES equipped gear can, however, be used commercially within the U.S.

VGE ALGORITHM

The VOICE GUARD VGE algorithm is a very secure, GE proprietary, encryption algorithm which was developed to meet the security needs of international and domestic customers. The encryption algorithm utilizes highly complex nonlinear data spreading and iterative key scheduling to insure the security of encrypted voice data. GE will not disclose design details of the VGE algorithm in order to maintain an extremely high level of security.

The VGE algorithm utilizes a 64-bit cryptographic key, and thus offers the security of 1.8×10^{19} power permutations of keys. It also utilizes a key scheduling algorithm, bit permutations, and nonlinear product transformations to provide a very high level of bit spreading.

In addition, the VGE algorithm offers an additional level of security, in the form of Customer Unique Encryption (CUE). The programming of a second 64-bit CUE code (16 hex characters) allows a user an increased level of security in his equipment. This CUE is programmed into a VGE Voice Guard unit by means of a TQ-2310 programmer. Even if two parties use the same cryptographic key, their equipment will not communicate unless they use the same CUE. This, effectively, increases the number of key and CUE permutations to 3.4×10^{38} power.

The U.S. Government has, by Executive Order, mandated that all Federal Government radio (and other telecommunications) systems that are to be equipped with voice privacy, shall employ the DES algorithm. Furthermore, such equipment shall carry the endorsement of the National Security Agency (NSA) in the form of a USGEID number which shall appear on each approved piece of equipment. These numbers are issued after completion of an endorsement process for each model of equipment to be offered for sale to any U.S. Government agency. Non-Federal government agencies are not required to have equipment possessing USGEID numbers.

Endorsed mobile and station equipment have, but are not limited to, the following general characteristics:

- Mounted in tamper-resistant boxes.
- If tampered with, the cryptographic keys contained therein will be destroyed.
- Be equipped with pick-proof locks for both mechanical and operational access.
- Provide malfunction alarms.
- No single electrical component failure shall permit transmission in the clear when the Guarded mode has been selected.

Endorsed personal handheld radios shall have similar characteristics as the mobile and station units except that pick-proof locks on the equipment are not required.

KEY-ENTRY REQUIREMENTS

DES

The DES key consists of 16 sequential hexadecimal characters, see Figure 2-1. This would imply that 16 to the 16th power combinations of keys could be employed; however, there are certain restrictions on the entry of DES keys that restricts the maximum available number of DES keys to 16 to the 14th power (i.e., 16 times 16 - 14 times).

DES keys are entered as 8 pairs of two HEX digits each. The first digit of a pair can assume any HEX value without restriction. The second HEX digit of a pair, combined with the first digit of the pair, must have ODD ONES parity. That means when converted to the binary form (see Figure 2-1), the two characters of the pair must have an odd number of ones. For instance, both characters of a pair can never have the

DECIMAL	HEX	BINARY
0	0	0000
1	1	0001
2	2	0010
3	3	0011
4	4	0100
5	5	0101
6	6	0110
7	7	0111
8	8	1000
9	9	1001
10	A	1010
11	B	1011
12	C	1100
13	D	1101
14	E	1110
15	F	1111

Figure 2-1. Table of Decimal, HEX and equivalent Binary values

same value; however, the second character of one pair and the first character of the next pair can have the same value since there is no restriction on the first character of a pair. Hence, two adjacent characters in a DES key can be the same as long as they are not in the same pair. Figure 2-2 depicts a valid and an invalid key. In the invalid key example, both the 55 and 47 number pairs have even ones parity.

VALID KEY = 1A 45 57 4A A1 10 6E 7C
INVALID KEY = 1A 55 47 4A A1 10 6E 7C

Figure 2-2

This parity limitation reduces the available number of cryptographic keys from 16 to the 16th power (1.8 times 10 to the 19th power) to 16 to the 14th power (7.2 times 10 to the 16th power).

VGE

The VGE cryptographic key consists of 16 sequential hexadecimal characters (see Figure 2-1). There are no parity entry restrictions as with DES therefore, all 16 to the 16th power combinations of keys may be utilized. This equates to 1.8 times 10 to the 19th power combinations of available keys.

In addition, a Customer Unique Encryption (CUE) word must also be programmed into the VGE unit personality PROM by a TQ-2310 Universal Radio Programmer (URP). This CUE word also consists of 64 bits.

KEYLOADER (19A148910)

The cryptographic Keyloader (19A148910) is a small, handheld, calculator-like keyboard display unit. It permits easy user storage and transfer of the cryptographic key word for use by Voice Guard modules. The keyloader requirements are different for the DES and VGE algorithms therefore, two types of loaders are provided:

19A148910P1 = DES Keyloader with cable

19A148910P4 = VGE Keyloader with cable

The key loader hardware for both algorithms is identical, but they employ different microprocessor operating programs. Each type of unit sign-ON message identifies the algorithm it supports.

Should one attempt to transfer a key utilizing the wrong type of loader, it will display the message "ERROR 1" and the radio will give a single "bleep" (also see DES in the KEYLOADER TESTS and RESPONSES section below).

FEATURES

Main features of both types of keyloader are:

- All functions are keyboard controlled and all entries are display prompted.
- Keyboard correction includes capability to correct any entry before execution.
- Automatic testing prevents the transferring of an improper algorithm key to the radio.
- Security provisions prevents redisplay of a stored key.
- Zeroization provisions allow for rapid emergency destruction of all keys stored in the loader.
- Loader automatically turns itself off after 60 seconds of no keyboard activity.
- MASTER and SLAVE modes protected by keyboard entered passwords provide for key transport only operation. In the SLAVE mode, no key can be changed and, zeroization is possible only with the power-on method (see KEYLOADER in the OPERATIONAL SECURITY section).
- LOCKED mode protected by keyboard entered passwords shuts down most of the keyboard initiated activities. In this mode, the stored keys cannot be accessed at all.

-In case of a malfunction, an error message is displayed on the keyloader. See the KEYLOADER ERROR MESSAGES section below.

KEYLOADER OPTIONS

Two independent hardware options are available inside all Voice Guard Keyloaders. These options are selected by the proper configuration of wire jumpers located on the Keypad Board. The GROUP option allows for the storage of either a maximum of one group of seven cryptographic keys, or for the storage of eight groups of seven (56 total) cryptographic keys. The DESTINATION option controls the internal destination of a key when it is downloaded to a Voice Guard unit.

GROUP OPTION

When the Keyloader is configured for seven key storage, up to seven cryptographic keys can be stored in the Keyloader in seven adjacent memory positions. These positions are numbered one through seven. A cryptographic key can be entered, downloaded or erased from any position without affecting the stored key in any other position. In the seven key mode, the Keyloader will always display the key number 1.x with the "x" denoting a digit 1 through 7. The display cursor will always appear under the "x" position.

A jumper located on the Keyloader Keypad Board is connected to IC U1 pin 14. This jumper can be cut to enable the eight groups of seven keys (56 total) option. These keys will be identified 1.1 - 1.7 through 8.1 - 8.7. With this 56 key mode enabled, the Keyloader display will show the group number (1 through 8) before the decimal point and the position number (1 through 7) following the decimal point. With the 56 key mode enabled, the display cursor will always first appear under the group number position.

DESTINATION OPTION

Within each of the eight groups of cryptographic keys, each key is assigned a memory position number one through seven. This position number corresponds to the number following the decimal point shown on the Keyloader display. This position number, along with the corresponding cryptographic key is normally sent to the Voice Guard unit during a key transfer.

With a Keyloader configured for DESTINATION Option 1, a cryptographic key being downloaded to a multi-key Voice Guard unit will be stored in the Voice Guard unit's cryptographic memory position that corresponds to the position number sent from the Keyloader. The key group number, the number preceding the decimal point in the display, is not transferred to the Voice Guard unit. For example, key 1.5 and key 6.5 will both be transferred to multi-key Voice Guard units key position 5, and the last key transferred will be the active key #5 in the Voice Guard unit.

Some Voice Guard units, such as the VG-9600 and the MPS, can be preset to either ignore the position number during a download and put all keys into position one, or to direct each key into the corresponding position described by the position number.

The M-PD portable is configured only for multiple key operation. The key selection is coupled to the radio channel number by means of the personality information programmed into the radio. The keys are always loaded into the key position identified by the Keyloader position number.

Some users wish to store several cryptographic keys in their Keyloader and be able to load any of them into key position one of an M-PD. This is possible by increasing the Keyloader storage capacity to 8 groups via the GROUP option. The keys can then be loaded into position 1.1, 2.1, ..., 8.1 and selectively transferred to the M-PD to position one. Some users, including all IFS-1027 applications, do not wish to enable the 56 key storage mode.

Both the DES and VGE Keyloader firmware has been revised to support the DESTINATION Option 2. This option assigns the position number one to all keys as they are transferred to a Voice Guard unit, irrelevant of their position in the Keyloader. A jumper, located on the Keyloader Keypad Board at IC U1 pin 16, can be cut to enable the Option 2 mode.

All DES Keyloaders with firmware version 2.1 and all VGE Keyloaders with firmware version 1.1 have the DESTINATION option capability. The Keyloader display will show the selected option at the power-ON sequence. All earlier versions of Keyloaders only support the Option 1 mode, but they may be upgraded by changing the EPROM IC U5 on the Display Board.

KEYLOADER TESTS and RESPONSES

DES (19A148910P1)

The DES Keyloader automatically checks the parity of the second character of each pair as they are entered and rejects digits not producing an odd-ones parity for the digit pair. This is indicated by the cursor on the display not advancing after an improper character has been entered and the improper character flashes. Another entry from the keyboard will be checked for proper parity with the first character and the new character will overwrite the improper character. If the parity check of the new character is good, the cursor will advance. If the parity of the new character is not good, the cursor will not advance as described above.

In addition, the DES keyloader performs a parity check on the key to be transferred at the beginning of the transfer process. Should the stored key have somehow been corrupted in the a keyloader memory, a "BAD PARITY"

message will be displayed and the transfer immediately halted. In addition, a series of tests with the radio during the key loading process before a key is transferred. After the key transfer, the radio performs another parity check on the key and sends the status back to the loader before the "GOOD LOAD" message is displayed by the loader. In the event that any of these tests fails, the key transfer is halted and an error message will appear on the keyloader display.

There is a special DES failure condition where the radio may "bleep" at the end of a key loading sequence and the "GOOD LOAD" message appears on the Keyloader's display. This can occur due to a logic failure in the Voice Guard module. While this is a Voice Guard module failure, and is not associated with the Keyloader, it can happen at the end of a key

loading sequence. If it does occur, attempt to reload the key(s). If the radio does not "bleep" and the "GOOD LOAD" message appears, the problem was of a transient nature and the condition should be ignored. If the "bleep" continues to reoccur, there is a Voice Guard unit logic failure.

VGE (19A148910P4)

The VGE keyloader performs an ID test with the radio and looks for a specific return. Then, the keyloader will transfer the user selected key and again look for a defined status response from the radio before the "GOOD LOAD" message is displayed by the loader. In event that one of these tests fails, the key transfer is halted and an error message will appear on the keyloader display.

KEYLOADER ERROR MESSAGES

Table 2-3 shows the messages and probable causes for DES keyloaders (19A148910P1). Table 2-4 shows the messages and probable causes for VGE keyloaders (19A148910P4).

<u>MESSAGE</u>	<u>MEANING</u>	<u>CAUSE</u>
ERROR 1 -	Time-out during S-box test	Cable not connected- VG unit not in FILL- Wrong algorithm- VG-9600 logic board H21 not connected to H22
ERROR 2 -	External S-box test failure	VG DES chip defective
ERROR 3 -	Parity test failure	VG DES chip defective
ERROR 4 -	Test key failure	VG unit defective
ERROR 5 -	Time-out during Auto-test	VG unit failure
ERROR 6 -	Auto-test test failure	VG unit failure
ERROR 7 -	Auto-test status byte error	VG unit or loader failure
ERROR A -	Time-out during key transfer	VG unit failure
ERROR B -	Test key parity error	VG unit failure
ERROR C -	Key transfer status byte failure	VG unit or loader failure
BAD 1.(x) PARITY-	Key 1.(x) as stored is defective	Loader failure

Figure 2-3. DES Keyloader Error Messages

<u>MESSAGE</u>	<u>MEANING</u>	<u>CAUSE</u>
ERROR 1 -	Time-out during ID request	Cable not connected- Wrong algorithm-
ERROR 2 -	Illegal ID return	VG unit defective
ERROR 3 -	Time-out during key transfer	VG unit defective
ERROR 4 -	ID status byte failure	VG unit defective
ERROR 5 -	Key transfer error	VG unit defective

Figure 2-4. VGE Keyloader Error Messages

KEY MANAGEMENT

The real security in any voice privacy system comes from the fact that the specific cryptographic key being employed in any system at a specific time is not known. Furthermore, the more often a key is changed, the greater the level of system security. This is because:

- a) If the key being used has been discovered by an adversary, frequent changing of the key will negate the discovery.
- b) If an adversary is attempting an "exhaustive search", changing the key forces the search to be started over.

Maintaining the secrecy of the key is of utmost importance. Since the keyloader has the active key(s) stored in it, it is essential that the keyloader not be left laying on a service bench or in an unlocked desk drawer. Maintenance should be performed with test keys, not the operational key(s) and, upon completion of maintenance, the operational key(s) should then be installed by a person responsible for key security.

Ideally, a cryptographic key should be composed of randomly selected characters. Care must be taken to not use such sequences as one's Social Security number, phone number, address, etc. Such sequences are logical first tries for an adversary conducting an "exhaustive search". If several keys are to be employed in one area, the keys should be significantly different, not just differ by one or two characters. Otherwise, for an adversary to find one key gives him a distinct advantage on discovering the others.

In a large, dispersed organization where more than one keyloader must have the operational key, distribution of the key is one of the weakest links in system security. The Voice Guard keyloader attempts to address this problem by allowing all of the keyloaders to be programmed at a central, secure point then, electronically lock the keyloaders with their preset LOCK code. The units can then be transported to another location by courier and unlocked upon arrival by using the preset UNLOCK code.

*** REMEMBER *** System security is solely dependent upon maintaining of the secrecy of the operational cryptographic keys.

OPERATIONAL SECURITY

KEYLOADER

In an adversary situation where the keyloader is in imminent danger of being captured, it is possible to quickly destroy all of the cryptographic keys stored in the loader with one operation. This is accomplished most rapidly if the keyloader is OFF. First, depress and hold the "Z" button. Then depress the "PWR" button. The unit will power on and, upon detecting the "Z" button being depressed, will zeroize the entire key storage RAM. This procedure works for all three operational keyloader modes (MASTER, SLAVE and LOCKED).

If a DES (or 1 group VGE) keyloader is already powered on, press the "EXE" button to get the unit back into the MASTER MODE. Then, depress the "Z" button for zeroize, followed by the "A" button for all. The result will be

all 7 keys of group 1 will be erased. (NOTE: For FED-STD 1027 applications, the keyloader will only support 1 group of 7 keys.) For VGE keyloaders operating in the 8 group mode (56 keys), this method will zeroize only the selected group.

MOBILE AND STATION

The FED-STD FS-1027 endorsed models of VG-9600 Voice Guard module (VG-9600 C, S and SR) have anti-tamper and cryptographic key dumping capabilities.

These VG modules fit on a mounting plate that has four protrusions that extend up into the module. The module is then slid forward to position it to be locked in place with the mechanical FILL/LOCK key. The process of sliding the module forward causes one of the protrusions to press against a microswitch. Once locked, the mounting plate holds this microswitch operated which, in turn, completes the electrical path for applying power to the cryptographic key RAM. Any action that even momentarily allows the microswitch to move to its released position, will remove power from the key RAM and ground the RAM power input terminal. This immediately destroys the cryptographic key contents of the module's key RAM. Unless this microswitch is held operated, it is also impossible to load a key from the keyloader. See VG module Service Section manual for details.

The mounting plate also has four recessed holes on the bottom to cover the mounting hardware and make it inaccessible when the VG unit is locked in place. When employing the VG-9600 in a station application, it is intended that the mounting plate be screwed onto a table top. Removal or tampering with the mounting will at least leave marks on the table as a warning that security has been compromised.

The FS-1027 endorsed models of VG-9600 also have the capability of being quickly rendered cryptographically useless in case of an emergency where the unit is in imminent danger of falling into an adversary's possession. This is accomplished by fully depressing the recessed keydump push-button on the front of the VG-9600. This action removes power from the cryptographic key storage RAM and grounds the RAM chip power input pin. This immediately destroys all of the digital information stored in the RAM, thus obliterating the cryptographic key. To again make the VG-9600 functional, it is necessary to reload the operational keys from a keyloader. Upon depressing the keydump button, the frame of VG digital data being transmitted will be completed, but the VG module will not start transmitting the next frame of data. Each frame of VG data is approximately 0.25 seconds long.

The non-1027 endorsed Voice Guard mobile units (VG-9600 CW, SW and SRW and, VGE-9600 CW, SW and SRW) do not provide the anti-tamper and key dumping features.

PERSONAL

MPS

An MPS personal radio equipped with DES algorithm Voice Guard is only available in the FS-1027 approved configuration. It has anti-tamper and cryptographic key dumping capabilities. The VGE algorithm version of MPS Voice Guard does not include the anti-tamper and keydump features. Both versions of Voice Guard equipped MPS portable support only one cryptographic key.

The Voice Guard module is contained in an extended MPS radio rear cover and forms an integral part of the radio. The module is retained by four mounting screws in the standard MPS rear cover locations. Anti-tamper protection is accomplished in the DES models by means of a cover plate over one of the four rear cover retaining screws. The cover plate is retained by another small screw, and the removal of this screw causes the cryptographic key to be electrically cleared.

The DES cryptographic key is retained in a low power proprietary encryption chip which is powered directly from the unswitched radio battery. The DES VG module stores sufficient energy to retain the cryptographic key for at least 30 seconds while the radio is switched OFF, to facilitate battery change. Key dumping is accomplished by removing the battery with the radio power switch ON. This quickly discharges the energy stored in the DES module back into the radio electronics thus "dumping" the cryptographic key.

The VGE model stores the cryptographic key in non-volatile EEPROM memory. The cryptographic key is retained even if the battery is removed for extended periods. There is no provision for quickly destroying the cryptographic key in the VGE model of Voice Guard.

MPS personal radios can be equipped for up to 64 channel operation with OA's assigned on a channel by channel basis. MPS radios are programmable with a TQ-2310 programmer. Cryptographic keys are loaded with a 19A148910 keyloader.

M-PD

An M-PD personal radio can be equipped with either DES or VGE encryption algorithms. The Voice Guard function is contained on the M-PD main system board. Both the DES and VGE versions of M-PD are capable of supporting up

to 7 different cryptographic keys. These are selectable from the front keyboard of the radio or can be preprogrammed on a channel by channel basis. An M-PD can be programmed for up to 64 channels with OA's assigned on a per channel basis. Voice Guard operation can also be selectively inhibited on a channel by channel basis. The personality information can be programmed into an M-PD with an IBM PC or compatible having at least 512 kilobytes of memory and running GE software package TQ-3319. Cryptographic keys are loaded with a 19A148910 keyloader.

The key-dumping requirement of FS-1027 has been met by holding the upper left and upper right most keys on the M-PD radio keypad down for at least one second. A message "KEY ZERO" will flash on the display panel of the radio and all keys stored in the DES encryption chip will be erased.

The anti-tamper requirement of FS-1027 has been satisfied in that when the RF (rear) portion of the M-PD radio is separated from the controller (front) portion of the M-PD radio, a switch is automatically operated that removes keep alive power from the DES encryption chip. This erases the stored cryptographic keys.

With VGE, there is no requirement for the key-dumping and anti-tamper features supplied with all DES version M-PD radios.

MECHANICAL KEY SECURITY

The main objective of key control, either cryptographic or mechanical keys, is to restrict and control the acquisition of keys. Anyone with temporary access to the standard type of keys has no problem in getting duplicate keys made for their own purposes. The basic problem is the ready availability of most key blanks and the common availability of key cutting machines. The vendor of the keys and locks used on the FS-1027 approved versions of Voice Guard has restricted the duplication capability of keys to his plant. This is accomplished through using keys requiring angled cuts and critically tight tolerances. He also restricts the distribution of key blanks to his own manufacturing facility.

Duplicate Voice Guard keys can be ordered through GE, but only by the number on the tag supplied with the mechanical keys when the Voice Guard equipment was delivered. An order accompanied with a key requesting one or more duplicate keys cannot be accommodated.

If all of the keys to a particular Voice Guard lock are lost, it will be necessary to replace the lock with a new one accompanied with new keys.

(This Page Intentionally Left Blank)

CHAPTER 3

GE OUTSIDE ADDRESSING

OUTSIDE ADDRESSING

Voice Guard digital selective signaling or Outside Addressing provides a Guarded mode equivalence for clear mode multitone encode/decode Channel Guard.

CONCEPT

Outside Addressing is accomplished by utilizing eight (8) unencrypted data bits that are located in the Voice Guard digital sync word. Any combination of these 8 bits can be employed as an outside address (OA) however, hex "AC" is a special case. During Guarded mode operation, this sync word is repeated approximately four times a second.

Voice Guard units require that individual TX and RX OA's be programmed in their personality EEPROM for each operational radio channel. OA switching is ganged to the radio channel select leads. Failure of a Voice Guard (VG) unit to recognize a matching OA, even though the Guarded mode signal had a correct cryptographic key, will result in the receiver decrypted audio path not opening up and Channel Guard will keep the radio muted so that the encrypted data will not pass through the clear audio path.

A VG unit continually examines the OA contained in a received Guarded mode signal and looks for a match with the stored OA for that channel in the hexadecimal range of 00 through FF. If a hex "AC" OA is received, the VG unit will interpret it as a universal receive code and will open up the receiver audio path (assuming the cryptographic key is correct) independent of the receive OA programmed for that channel. Similarly, a transmit OA for a given channel programmed with a hex "AC" will serve as an all-call, independent of the OA(s) that might be programmed in the VG receivers being contacted. Again, the cryptographic keys must all be the same.

Remote, repeat and remote/repeat stations also have the capability of examining the OA on an incoming VG signal and either responding to or ignoring the signal. The stations can also optionally modify the OA of a VG signal received via the station RF receiver as it is retransmitted on the RF path. The OA's to and from the remote control point via the telephone line are retransmitted on the station RF path unchanged. Several different station configurations of OA operation are selectable by means of the three "DIP" switches on the VG station shelf.

It should be noted that Voice Guard disables the Channel Guard (CTCSS) encode and decode functions when operation is in the Voice Guard mode. However, the use of Channel Guard when in the Clear mode is highly recommended because, without Channel Guard to keep the receiver muted, a Voice Guard signal with a wrong key or non-matching OA will unquench the receiver and be heard in the speaker as a loud hiss for the duration of the transmission. In addition, all non-VG equipped receivers without Channel Guard will also receive all VG transmissions as a loud hiss.

Outside addressing makes a variety of Guarded mode control and selection functions possible. Multitone Channel Guard selection can be ganged to radio channel frequency select lines in a manner similar to OA selection, thus making it possible to configure parallel control paths for Guarded and Clear mode operation that appear as one to the user.

MOBILE

All versions of VG-9600 Voice Guard module that are applied to DELTA and RANGR mobile radios have OA's assigned on a channel by channel basis up to a maximum of 32 channels (16 channels for RANGR). In addition, the transmitted OA and the received OA for each channel are independently specified and need not be equal. These OA's may be any decimal value from 0 through 255 (hex 00 through hex FF) and are programmed into the VG unit's personality EEPROM utilizing the TQ-2310 programmer. See the CONCEPT section above regarding the all-call code hex "AC". See LBI-31523 for detailed TQ-2310 instructions.

The DELTA S and SX mobile radios channel select system involves the binary encoding of up to 32 radio channels on 5 frequency select lines (FB-1 through FB-5) in the control unit and their subsequent decoding in the radio synthesizer control circuitry. These five lines are read by the Voice Guard logic as the radio control cable is looped through the VG unit. The radio channel number and the states of the 5 frequency lines are shown in Chapter 5, Figure 5-9. These lines are normally pulled to a + voltage which appears as a logic "1" in Figure 5-9. Grounding of a frequency select lead constitutes a logic "0". RANGR mobiles employ the same frequency select system except only 16 channels are provided and only the four least significant select lines (FB-1 through FB-4) are utilized.

The DELTA S and SX mobile radios can have an additional 32 channel blocks of operating frequencies dynamically downloaded from some control units. These 32 channel blocks are called channel "MODES" and, the S990/S950

control units provide for the downloading of up to 4 modes of 32 channels each, for a maximum capacity of 128 channels. The Voice Guard unit however, only reads the five channel select lines and does not take cognizance of the channel MODE number. Therefore, radio channel 9 of control unit MODE 1 will have the same TX and RX OA's as radio channel 9 of control unit MODE 4, even though the radio frequencies for these two modes may be totally different. RANGR mobiles can support four modes of 16 channels each. The same OA assignment restrictions described for DELTA apply to multiple modes in the RANGR.

PERSONAL

MPS

Both the DES and VGE versions of Voice Guard modules for the MPS radio provide for separate assignment of transmit and receive OA's and data polarity on a channel by channel basis. This, along with other, personality information is stored in an EEPROM in the VG module and is programmed with a TQ-2310 programmer.

Outside addressing for the MPS operates in much the same way as for the mobile described in the MOBILE section above. The major difference is that the MPS personal can support up to 64 radio channels and the EEPROM has the capability of storing individual TX and RX OA's for each channel for a maximum total of 128 OA's.

M-PD

Both the DES and VGE versions of M-PD radio provide for separate assignment of transmit and receive OA's and data polarity on a channel by channel basis. In addition, VG operation can also be inhibited, and selection of any one of up to seven cryptographic keys can also be programmed on a channel by channel basis. This, along with other, personality information is stored in a lithium battery backed-up RAM inside the M-PD radio.

Outside addressing for the M-PD operates in much the same manner as for the mobile described in the MOBILE section above. The up to 64 channels of VG personality information along with other radio characteristics can be programmed with an IBM PC or compatible with at least 512 Kilobytes of memory and running GE software package TQ-3319.

DELTA DESK TOP STATIONS

The DELTA DESK TOP stations are DELTA mobiles mounted in a sloping panel cabinet with an AC power

supply. When equipped for Voice Guard operation, the original station cable harness is replaced with one that picks up the required interconnection to a VG unit. The VG unit, which is the same configuration as used with DELTA mobiles, is to be mounted adjacent to the station.

The DELTA DESK TOP station supports up to 16 radio channels. The radio channel select leads are also delivered to the VG unit so that each operational radio channel will have an individual programmable TX and RX OA. OA assignment and all-call operation is the same as that described for the DELTA mobile. No control unit downloading capability is provided with the DELTA DESK TOP station.

END-TO-END STATIONS AND REPEATERS

End-to-end encryption stations and all VG repeaters require a GETC or Voice Guard station shelf. Either of these shelves have three separate eight-section DIP switches, one switch (S1) is for programming the radio receive channel OA, the second switch (S2) is for programming the radio transmit channel OA and the third is for establishing the station configuration. See LBI-31546 and the VOICE GUARD STATION SHELVES section in Chapter 5 for additional details on the station shelf.

STATION SHELF CONFIGURATION SWITCHES

Switch S1 establishes the matching OA required before the received RF signal can key up the repeater transmitter or initiate the sending of VG data to the telephone line modem. If a hex "AC" set into switch S1, the shelf will respond to all valid format VG signals independent of the OA they contain, and the OA on the received RF signal will be retransmitted on both the controller (phone line) and repeater (RF) paths - unchanged.

Switch S2 establishes the OA that any repeat configuration station will transmit (RF) in the Guarded mode, provided that switch S1 is not set for hex "AC". Any remote configuration station will transmit the OA on the VG signal received via the wire line port, independent of the setting of the transmit OA switch (S2) setting.

If S1 is set for any value other than hex "AC", the received RF signal OA must match the value set in S1. The repeater (RF) transmitter signal will contain the OA value set in switch S2 and the value of the OA signal sent down the wire line will be the original received OA (i.e., the setting of S1 of hex "AC").

An additional operational choice is selected by switch S3-5 which either enables or disables the all-call decode. If

enabled, an "AC" OA received on the RF path will be accepted independent of what OA is set in S1. The repeated RF path signal OA will be the contents of S2 and an "AC" will be sent to the wire line path. If disabled, the station shelf will ignore the incoming RF path signal by virtue of a non-matching OA.

Configuration switch S3 establishes the mode of station operation (i.e., remote, repeat, remote/repeat, voted remote/repeat etc.), the data inversion criteria for the RF and wire line paths and the option of enabling or disabling the all-call decode. See LBI-31546 for additional details on setting switch S3.

CONSOLE INTERFACE UNIT (CIU) - Tone control only

In end-to-end encryption VG configurations, it is necessary to locate a VG-9600 at or near a dispatch center so that the station control lines can be encrypted during Guarded mode operation. Since a dispatch center of any size usually has several dispatcher positions, each with a separate console, the locating of cryptographic equipment at each console presents a significant cost penalty. Since most dispatchers are located at a common place and that place can be made secure, the obvious approach is to interconnect all of the consoles on a clear mode basis and then connect these clear lines to a Console Interface Unit (CIU) which is also located at the dispatch center.

Each console position is equipped for two frequency tone control operation. If a clear mode transmission is desired, the dispatcher transmits an F1 transmit select sequence. The CIU allows this tone sequence to pass and the remote transmitter is keyed up on the air on F1 in the clear. If a Guarded mode transmission is desired, the dispatcher transmits an F2 transmit select sequence. The CIU recognizes and intercepts the tone sequence before the transmitter is keyed on the air. The CIU then redirects the audio and keying paths so as to cause a VG-9600 to encrypt and connects the digital output to a wire line modem for transmission to the remote station.

If a VG signal is received from the remote station, the VG-9600 in the CIU recognizes the signal and directs the CIU to rearrange the audio paths so as to deliver a decrypted signal to all of the consoles.

Two-frequency station operation can be achieved if the console positions are equipped for four-frequency tone control. Frequency and mode selection occurs in the following manner:

<u>CONSOLE</u>	<u>MODE</u>	<u>TX FREQ</u>
F1	Clear	F1
F2	Guarded	F1
F3	Clear	F2
F4	Guarded	F2

The VG-9600 in the CIU can be programmed to produce and respond to different OA's for transmitted F1 and F2.

CHANNEL GUARD MONITOR

In the clear mode, when the Channel Guard monitor button on the microphone or console is momentarily depressed, the receive Channel Guard is disabled and the dispatcher hears all transmissions on the channel. In the Guarded mode, when the Channel Guard monitor button is momentarily depressed, the receive OA appears as if an "AC" had been programmed into switch S1. Any Guarded signal will be sent on to the dispatcher via the wire line port with the OA unchanged and, the repeater will key up in the Guarded mode with the transmitted signal having the OA value set in switch S2. To restore normal Channel Guard and Voice Guard operation, it is only necessary to momentarily key up the transmitter in the clear mode via the wire line path.

E/D REMOTE ONLY STATION

An E/D Remote only station has the VG-9600 unit installed at the station instead of at a remote control point and the control line between the two is always unencrypted. This is the only configuration of Voice Guard MASTR II station that does not require a GETC or VG Station Shelf. The E/D Remote only station can be configured for either one or two frequency operation. In either case, the VG unit is normally configured to support one OA.

An E/D Remote only station will respond to the all-call OA in addition to the programmed OA. The VG unit OA channel 1 is the channel that is utilized.

E/D REMOTE/REPEAT STATION

The E/D Remote/Repeat configuration of MASTR II Station combines the characteristics and hardware complement of both the VG Repeater and the E/D Remote only station. The VG-9600 unit performs the required encrypt/decrypt function for the local service microphone and speaker and, for

the remote control point via an unencrypted four-wire control line. The GETC or VG Station Shelf performs the required data storage and regeneration functions for repeater operation. The VG9600 unit and the GETC or station shelf operate quite independently except that a local (service microphone) or remote console initiated transmit command will preempt the repeater operation of the VG Station Shelf, even if a signal is being repeated.

Outside addressing of the VG unit is as described for an E/D remote only station. Since an E/D Remote/Repeat station is available only configured for only one frequency operation, there is only one TX and one RX OA available. These are associated with VG unit channel 1. The shelf RX and TX OA's are independently set with DIP switches S1, S2, and S3 and discussed in the END-TO-END STATIONS AND REPEATERS section above. A significant point of note is that the VG unit OA's and the shelf OA's do not necessarily have to be the same. See the SYSTEM APPLICATIONS section below for an example.

SYSTEM APPLICATIONS

The following are several examples of system configurations involving the use of outside addressing for digital mode control and selection. The counterpart clear mode control equivalence, while not discussed, is attainable with multitone Channel Guard or other available tone control techniques. It should be noted that while VG Outside Address operation readily supports an all-call capability, typical multitone Channel Guard systems may not be able to support all-call.

EXAMPLE 1. - Standard system

The simplest OA configuration of VG involves having all units and stations be programmed for the same OA (usually the default OA of hex 55). This is analogous to single tone Channel Guard clear mode operation.

EXAMPLE 2. - Subdividing a fleet

A fleet of units under the control of one dispatcher could be subdivided into groups so that all members of a group can communicate with all other members of his group but would not hear or be heard by the other groups. Furthermore, the dispatcher, with a base station - no repeater, would hear all of the groups and would be able to talk simultaneously to all members of all groups.

System setup criteria:

- All VG radios have the same key.
- Each group operates with a different OA assignment.
- The base station would be set for hex "AC" TX and RX OA.

EXAMPLE 3. - Dispatcher subdividing a fleet

A dispatcher can subdivide a fleet of units so as to communicate with 1 of up to 3 groups or talk to all of them. This is anticipated to be a simplex frequency operation utilizing an end-to-end remote only station.

System setup criteria.

- Station controller is set up for four-frequency operation with hex "AC" (all-call) for one TX OA and 3 unique TX OA's for the remaining 3 channels. The RX OA is set for hex "AC".
- Rig the station for single frequency operation. Set RX OA for hex "AC" (all-call) and mode 0 remote station operation.
- Each group of mobiles is programmed with one of the unique TX and RX OA's.

System operation

- The dispatcher selects one of the OA's and talks to that group.
- The dispatcher selects all call OA and talks to everybody.
- If a mobile TX OA is also set for hex "AC", he will be able to talk to all groups.

EXAMPLE 4. - Selective repeater keying

Where there are several repeaters located in different "zones", it may be desirable to allow the mobile operator the ability of selecting which repeater is going to be brought up.

System setup criteria:

- The mobiles, portables and control stations are programmed with the same frequencies but a different TX OA for each repeater to be selected.
- Set the RX OA for each repeater to be one of these unique values.
- The repeater TX OA's and the mobile RX OA's will all be the same value but different from the repeater input OA's (but should not be the all-call code hex "AC" as this would prevent repeater talk around).
- Input all-call (S3-5) enabled.
- For talk around, the mobile TX OA's will then be the same as the repeater TX OA's.
- To bring up all repeaters within range, program mobile TX OA for hex "AC" (all-call).

EXAMPLE 5. - Selective repeater access but always contact dispatcher.

A base/repeater system where the dispatcher hears and talks to all units, but the units each have the ability to enable the repeater or just talk to the dispatcher. This can be accomplished with the E/D Remote/Repeat station.

System setup criteria:

- All mobiles and portables are programmed for 2 channels with the same frequencies but two different TX OA's. Receive OA's are all the same.
- The repeater shelf receive OA is set for one of the mobile TX OA's. The station VG unit RX OA is set for hex "AC" (all-call).

- The station always transmits the mobile RX OA.

System Operation

- A mobile transmitting with the repeater OA will key up the repeater and the all-call station VG unit OA will receive the mobile.

A mobile transmitting with the non-repeater OA will still be heard by the all-call OA station VG unit.

The station/repeater output will always be heard by all mobiles as the TX OA always equals the fixed RX OA's in the mobiles.

NOTES AND COMMENTS

1. Even though OA codes can be assigned any value 00 (hex) through FF (hex), it has been noted that occasional falsing can occur when operating in the clear mode with Voice Guard equipped radios. This occurs when certain Channel Guard tones in the presence of noise (typically due to weak RF signal level) are improperly decoded as valid VG late entry start of preamble and valid OA. This briefly switches the VG unit to the Guarded mode, however the VG unit immediately discovers that the rest of the required VG signal is missing and the audio path is switched back to clear. This results in an occasional blank hole being punched in a clear mode received audio. This can be avoided by not using either of the two OA values 00 (hex) and FF (hex).
2. While it has been noted that the E/D station and CIU implementations of VG are limited in the number of OA's available, it should also be noted that this limitation has to do with the number of normally available frequency select leads. Should a particular system application require that more OA's be available at a dispatch point, it would only be necessary to go into the cable connected to the back of the VG unit and free up the leads identified as FB-1 through FB-5 and tape back the wires. It is now possible to extend these five wires to an external binary coded selector switch using the logic table shown in Figure 5-9. The desired 32 OA's would be programmed into the personality PROM of the VG unit and would be selectable independent of the transmit frequency.

(This Page Intentionally Left Blank)

CHAPTER 4

VG TRANSMISSION CHARACTERISTICS/TEST METHODS

SYSTEM PARAMETERS

In order to properly set up and operate a Voice Guard system, there are several system level parameters that require attention. These include: control line characteristics, transmitted digital waveform, data polarity and the outside address assignment. This section deals with these subjects except for outside address assignment which is covered in Chapter 3.

CONTROL LINE CHARACTERISTICS

There are two generic types of Voice Guard remote control stations. These are: a) end-to-end encryption and b) RF only encryption.

In end-to-end encryption, a Voice Guard unit is included as part of the dispatch console/CIU equipment and the remote station has digital data processing circuitry but does not have any cipher or encryption capability. Cryptographic key information is not required at the remote station. The control circuit, be it privately owned or telephone company supplied, or be it wire or microwave, must be a four-wire data grade circuit capable of supporting 9600 baud Voice Guard data. In this configuration the data transmitted over the control circuit as well as over the radio path(s) is encrypted. This provides the highest level of system security.

In RF only or encrypt/decrypt (E/D) stations, a Voice Guard unit is included as part of the remote station equipment. This requires that the working cryptographic key must reside in the Voice Guard unit at the remote station. The control circuit now only carries clear (unencrypted) information. The Voice Guard unit is remotely selected for CLEAR or GUARDED mode of operation at the start of each transmit PTT, receive mode selection is automatic. Four-wire control is still a requirement but now only needs to be a voice grade (not data grade) circuit. While this configuration only provides encryption over the RF path(s), significant system cost savings can be had, especially in voted receiver applications.

REMOTE CONTROL CIRCUIT

When a local telephone company is contacted about furnishing a dedicated radio remote control circuit, one immediately finds that there are a large variety of available transmission circuit characteristics - with a corresponding variety of

costs. These transmission characteristics are defined by such terms as:

- 2-wire
- 4-wire
- Frequency response
- Net loss
- Frequency error
- Group (envelope) delay
- 2000 grade
- 3000 grade

The following is an attempt to take some of the mystery out of this subject:

* Two-wire - Describes a single pair of dedicated metallic wires or the multiplexed equivalent. This type of circuit will support the bidirectional transmission of audio signals in the nominal 300 to 3000 Hz frequency range. Support of DC control signals is available only with physical or metallic equivalent circuits and may not be available in some areas.

* Four-wire - Describes two pair of (usually) multiplexed dedicated telephone circuits with one pair going each way. Each pair will support unidirectional transmission of audio signals in the nominal 300 to 3000 Hz frequency range. One pair is usually designated as the SEND pair while the other is designated as the RECEIVE pair. DC signaling and control is usually not available. These circuits may be obtained for voice only or for voice and/or data applications.

* Frequency response - This is usually defined as the maximum variation in attenuation (loss) of a particular circuit over the specified frequency range relative to the attenuation measured at 1000 Hz, or in some cases 1004 Hz. The frequency band of interest for most telephone circuits is 300 Hz to 3000 Hz though other ranges may be specified.

* Net loss - This is usually defined as the attenuation that a telephone circuit presents at 1000 or 1004 Hz. It can be determined by applying a 0 dBm signal to one end of a line and noting the absolute level delivered to a terminating load at the other end of the line. Typically, this loss ranges from 0 to 20 dB.

* Frequency error - Most present day telephone transmission is accomplished by some form of electronic multiplexing. This may be done by either time domain or frequency domain techniques, or combinations of both over cable or microwave facilities. Some of the frequency domain links are not frequency locked end-to-end but rely upon oscillator stability at both ends to minimize frequency shift of the recovered signal. Since these oscillators are not absolutely stable, the term "frequency error" is a measure of the spectral frequency shift of a received (delivered) signal relative to that which was transmitted.

* **Group delay** - This is a measure of the change of propagation delay through a telephone circuit (or any other transmission path) relative to the propagation delay that is presented at a reference frequency (usually 1000 Hz). This change of propagation delay can also be expressed as the rate-of-change of phase as a function of frequency.

The effect of group delay is to cause the various frequency components of a digital waveform to be propagated at different rates. It might be thought of as a measure of a transmission system's ability to carry square waves. Severe group delay will degrade the bit error rate of an otherwise good data signal. Telephone circuits that are intended to support high speed data signals will have much tighter group delay specifications than will lines that are only intended to support voice signals.

* **2000-grade** - This refers to a family of telephone circuits, covered by telephone company service tariffs, that are only intended to support voice signals. These are generically referred to as "voice grade circuits".

* **3000-grade** - This refers to a family of telephone circuits, covered by telephone company service tariffs, that are intended to support either voice or data signals. These are generically referred to as "data grade circuits". These circuits can be obtained with several levels of conditioning. These are referred to as: standard, C1, C2, C4 and D.

TYPICAL LINE SPECIFICATIONS

The following information represents the typical specifications that should be expected for voice and data grade circuits. The Voice Guard end-to-end encryption equipment requires a 3002 data grade channel without additional conditioning.

Voice Grade (2000)

Available in both 2-wire and four-wire configurations. Voice Guard E/D stations require four-wire.

Frequency response:	300-3000 Hz, -3 dB to +12 dB
(rel. 1 kHz)	

Frequency error:	+,- 5 Hz
Group delay:	Not specified
Net loss:	Various specs available
Minimum S/N:	20 dB

Data Grade (3000)

Available in four-wire configuration. The Voice Guard end-to-end stations require a type 3002 circuit without special conditioning.

Frequency response:	300-2700 Hz; -2 to +6 dB
(rel. 1 kHz)	500-2400 Hz; -1 to +3 dB
Frequency error:	+,- 5 Hz
Net loss:	16 dB maximum
Group delay:	800 to 2600 Hz; 2000 usec maximum
Minimum S/N:	24 dB

DIGITAL TRANSMISSION - RADIO

The Voice Guard encrypted signal can be characterized as: 9600 baud, two level, NRZ, serial data. This means that the data is a serial train of two-state data bits (i.e., 1's and 0's) occurring at the rate of 9600 bits per second. The NRZ (non-return to zero) characteristic means that the duration of each data bit is a full clock period (approximately 104 microseconds) instead of returning to zero before the next bit time starts. This NRZ characteristic also means that the data has frequency components that extend down to DC and if passed through an AC coupled transmission media, a DC wandering or bounce will be present. The better the low frequency response of the transmission media, the less the bounce. Voice Guard requires a radio (baseband) frequency response flat down to below 10 Hz.

A second characteristic of NRZ data is that if it is inverted, it appears as a totally different data train and will not be recognized. This means that it is necessary to keep track of all data inversions caused by the radio equipment, or other causes. The personality PROM in each Voice Guard module provides a means for inverting or not inverting the transmitted and received data trains independently for up to 32 radio channels. GETC and VG station shelves have four hardware switches which provide a means for data inversion on each of the station data input and output paths. See the DATA POLARITY section below for a further discussion of data polarity.

DATA FILTERING - RADIO

The Voice Guard data as delivered from the VG logic circuitry or station shelf is a TTL logic signal. This signal has a 5 volt amplitude and the data transitions typically have 20 to 30 nanosecond rise and fall times. To apply such a signal to the modulator of a radio transmitter would result in modulation sidebands that would extend to a displacement of several megahertz on each side of the RF carrier. Since the FCC spectral occupancy limitations for digital voice transmission in the Land Mobile Radio services clearly restricts the width of the modulation spectrum, filtering of the data prior to the radio modulator is absolutely required. Such filtering must be phase linear so as to not add group delay and hence skewing of the data transitions. In addition, this filtering must not have a sharp cut-off response but, instead, have a smooth transition between the passband and the stopband regions. Filters having such responses are called a Gaussian Minimum Shift Keying (GMSK) and Bessel filters.

When a logic level data signal is passed through a GMSK filter, the fast data transitions are slowed down to approximate the shape of a cosine wave at the data clock rate. If the filtering is phase linear, all of the filtered data transitions will continue to cross a line midway between logic 1 and logic 0 at precise clock intervals (104 usec for Voice Guard). If, on the other hand, the filtering is not phase linear (i.e., has group delay), the filtered data transitions will not cross a line midway between logic 1 and logic 0 at precise clock intervals but will be skewed in time on each side of the clock interval. If the filter frequency response rolls off too quickly, higher frequency data components such as single ones or zeros will be filtered more than longer groups of ones or zeros. This will result in a shrinking of the amplitude of the single data bits.

EYE PATTERN DISPLAY - TWO LEVEL DATA

A method of displaying these effects on an oscilloscope is to trigger the scope from the data clock signal. Set the scope sweep rate so as to display slightly more than a single clock period. Connect the data to the vertical input of the scope and adjust the display for a symmetrical presentation about the horizontal center line. This has the effect of stacking all of the successive data intervals upon one another. If the data is not bandwidth limited (filtered), the display will appear as two horizontal lines (the upper line for one logic state and the lower line for the other logic state) and two vertical lines which represent all of the data transitions. See Figure 4-1 (a) for the data train and eye pattern display. An ideally filtered data train and eye pattern is shown in Figure 4-1 (b) while a non ideally filtered data train and eye pattern are shown in Figure 4-1 (c).

An alternate method of obtaining scope sync, when data system clock is not available, is to sync from one edge of data and display about three periods of data (i.e., three eyes). This method will not show the dispersing or skewing of zero-crossings to be as great as the clock synchronized display however, the amplitude distortions as shown will be the same. This alternate display method will be adequate for most system setup and troubleshooting purposes.

If the VG transmitter data deviation is set for ± 3.0 kHz and the eye pattern approaches the ideally filtered display shown in Figure 4-1 (b), the modulation spectrum of the transmitter will be within the required limits as presently defined by the FCC.

STATION RECEIVER DATA MODS

The IF crystal filter sections employed in the MASTR II station IFAS and MIF boards are normally adjusted for optimized SINAD performance. The majority of the important modulation sideband energy is confined to the approximately middle two-thirds of the receiver IF passband. When Voice Guard data, at 9600 baud, is being transmitted, the modulation energy is uniformly dispersed over more than three-fourths of the receiver IF passband. In order to minimize the group delay and amplitude response effects of the receiver IF crystal filters on the Voice Guard digital signal, it is necessary to readjust the MIF and IFAS board IF's in the presence of Voice Guard data.

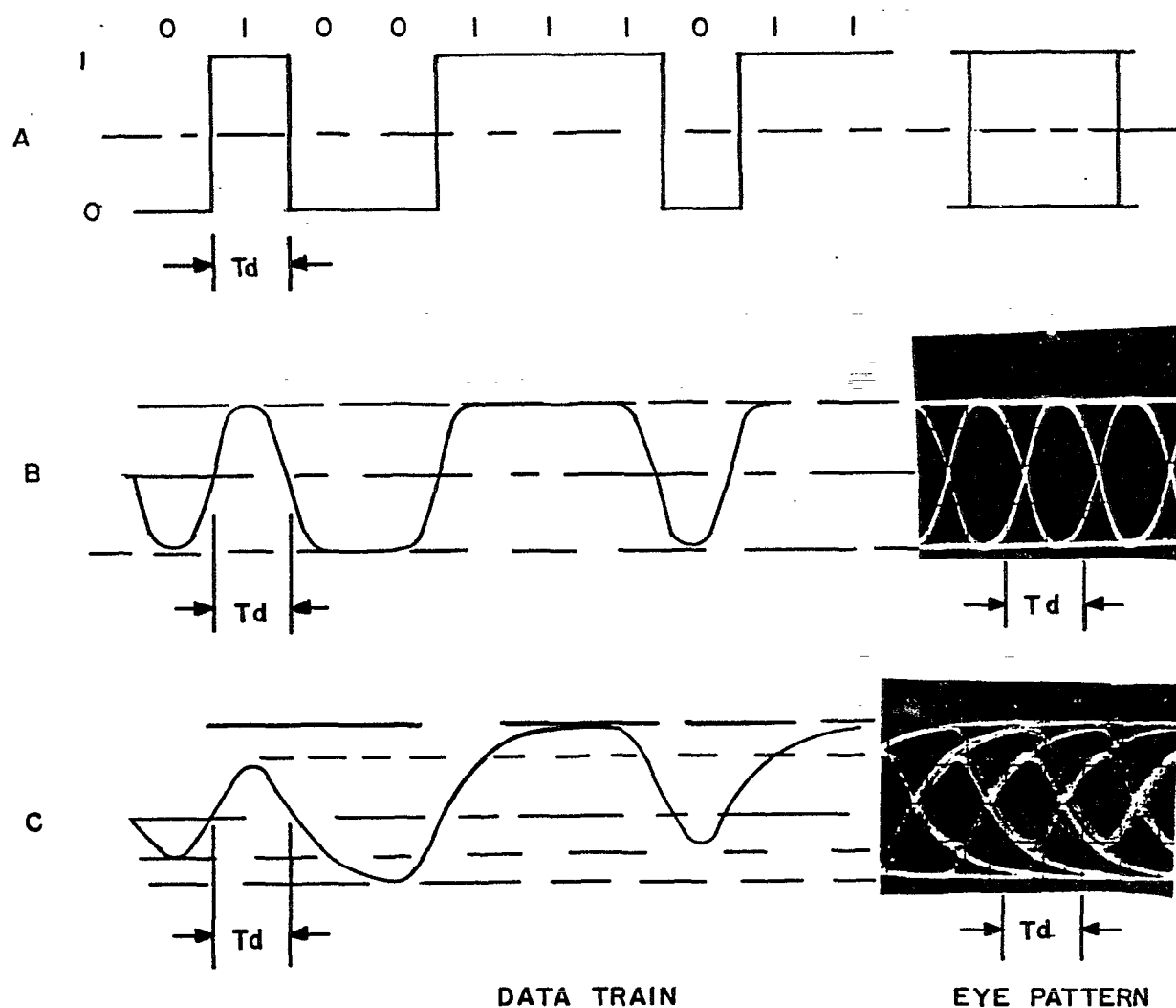


Figure 4-1. Data Train And Eye Pattern

IFAS board type 19D432667 provides the required adjustments on the crystal filters to permit VG data optimization. A Voice Guard unit or a pseudorandom test generator (19A149117P2) can be utilized as the external modulation source for a signal generator for IF alignment. The alternate (data sync) method of eye pattern display is adequate for the IF realignment. The realignment procedure is described in the VG station service manuals.

A coupling capacitor on the output of the FM detector has also been increased in value from .47 uf to 10 uf in order to improve the low frequency response, thus minimizing the "bounce" of the received NRZ data train. This modification is described in the VG station service manuals.

DIGITAL TRANSMISSION - WIRE LINE

It will be noted that the telephone line specifications listed in the DATA GRADE (3000) section above indicate that the frequency response of a data grade telephone line can only be expected to be usable from 300 to 2700 Hz. This is much less than that required by a two-level, NRZ, 9600 baud data signal. In order to accommodate these high data rate signals on wire lines, data modems are generally employed to convert the two-level, NRZ data to another form that will fit in the available passband of telephone circuits.

DATA MODEMS - GENERAL

Data modems have to perform two basic transformations on the two-level data in order to convert it into a data signal that will only require use of the spectrum between 300 and 2700 Hz. The first of these transformations is to eliminate the low frequency (DC) response requirement. This is usually accomplished by some form of subcarrier modulation scheme.

The second basic transformation is to reduce the overall bandwidth required by the two-level data. This is usually accomplished by employing multilevel modulation, either multiphase or multi-amplitude or both. Multilevel modulation has the benefit of reducing the required bandwidth as a function of the number of levels or states. For example; a four-level modem signal requires only half the bandwidth required by a 2-level signal, an eight-level only requires 1/3 the original bandwidth and, a 16-level signal only requires 1/4 the original bandwidth. This bandwidth reduction comes at the expense of an increase in the required modem link signal-to-noise ratio in order to maintain a given bit error rate. As the number of modulation levels increases, the minimum required signal-to-noise ratio also increases.

Since most modem schemes almost always employ some sort of subcarrier modulation, there is a side benefit in that the resulting modem output is an RZ (Return to Zero) signal.

This means that there is no data inversion if the wire line is disconnected and then reconnected - reversed.

VOICE GUARD WIRE LINE MODEMS *

The wire line data modems, 19A705178, employed in Voice Guard applications are 9600 baud, asynchronous, 16-state, commercially available units similar to the Rockwell International model R96-FT. The 16-state operation is achieved by a four-level, four-phase quadrature amplitude modulation (QAM) scheme. In QAM, two multilevel amplitude modulated (AM) carriers are transmitted simultaneously. Interference between these two modulated carriers is minimized by using carriers of identical frequency with a constant 90 degree relative phase angle. The weighted value of four sequential, 9600 baud data bits is converted in the modem to a unique amplitude and phase state. The weighted value of the next four bits is again converted to another unique amplitude and phase state, etc. Since the modem is converting four input bits at a time, there is four times more time to transmit the 16-level data bit than was required by the two-level data bit. This, in effect, has reduced the modem output data rate to 2400 baud. It should be noted that in two-level data signals, one baud equals one bit per second. However, in a 16-level data system, one baud equals four bits per second since each of the 16 modem signal elements (states) represents binary 4 data bits. Figure 4-2 shows the bit constellation which depicts the relative phase and amplitude versus the weighted bit values.

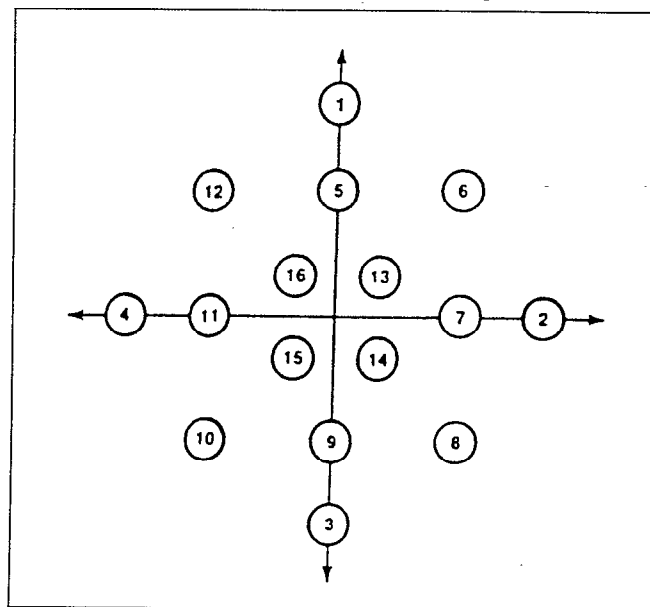


Figure 4-2. 16-Level Bit Constellation *

* Figure 4-2 and the VOICE GUARD WIRE LINE MODEMS section above derived from copyrighted material (C) Rockwell International Corporation, 1986, all rights reserved, and used by permission.

WIRE LINE - DIAGNOSTICS **

In a Voice Guard system where wire line modems are employed, there is the potential of an ever recurring interface problem with the telephone company supplying the wire facility. When a system problem involving data transmission occurs, the first question to be answered is - is the problem with the VG equipment or with the wire line.

A method for separating modem and line problems from VG equipment problems can be established by displaying the demodulated, multilevel baseband signals from the modem on an oscilloscope. The set of levels received on one carrier are displayed on the X-axis and the set of levels received on the other carrier are displayed on the Y-axis of an oscilloscope. Since these signals consist of discrete levels sent at high data rates, the resulting pattern displayed on the oscilloscope appears to be a fixed set of points in the form of the constellation shown in Figure 4-2.

The modem outputs "EYEX" and "EYFY" provide two serial bit streams containing data for display on an oscilloscope X and Y axis, respectively. Since this data is in a serial digital form, it must first be converted to parallel digital form by two serial to parallel converters and then to analog form by two D/A converters. A clock for use by the serial to parallel converters is furnished by "EYECLK". A strobe for loading the D/A converters is furnished by the signal "EYESYNC". Figure 4-3 is the basic schematic diagram of the hardware to generate the 16-level eye pattern constellation with eight-bit resolution.

It is assumed that the modem transmitter sends the data without noise or distortion hence, all 16 states in the data constellation will appear as unique points and will appear as in Figure 4-4(a). The center of the constellation represents zero volts and increasing radial distance from the center represents increasing voltage on the line.

Should the received signal also have significant random noise along with the data, the individual dots in the constellation would uniformly cluster about each ideal point in a circular manner. See Figure 4-4(b). Should the line impairment be periodic or is a function of the received signal itself, such as harmonic distortion, the distribution of individual dots about the ideal point will not be random. Figure 4-4(c) shows the radial distribution of dots due to a nonlinear device on the line. The higher level signal elements are distorted more than

the lower level signal elements. Figure 4-5 shows the tangential distribution of dots due to phase jitter or envelope delay. If a line impairment is marginal, it may not be obvious at just looking at an oscilloscope face however, a storage scope or scope camera with a 10 - 15 second exposure will show it up.

A piece of test equipment called an "EYE PATTERN ADAPTER", drawing number 19A149431, incorporates the circuitry shown in Figure 4-3 and is available through GE Service Parts.

DATA POLARITY

STANDARD

A data polarity standard for all Voice Guard operation has been established. This is:

- A). A logic one shall be a nominal +5 volts and a logic zero shall be a nominal 0 volts.
- B). A logic one shall cause the transmitted RF frequency to increase or be shifted higher. A logic zero shall cause the transmitted RF frequency to decrease or be shifted lower.

INVERSION

As noted earlier, Voice Guard NRZ data cannot be inverted and still be recognized by a Voice Guard receiver. Data inversion can occur in a radio by simply passing the data through an amplifier. Depending upon the amplifier design, it may or may not invert the data. In addition, superheterodyne receiver and transmitter PLL mixers will invert direct FM, NRZ data if high-side local oscillator injection is employed. Conversely, no inversion occurs if low-side local oscillator injection is employed.

Table 4-1 displays the data polarity characteristics of the various bandsplits of HB and UHF DELTA S and SX radios. RANGR radios do not invert either transmit or receive data on any split of any band (HB through 800 MHz). Table 4-2 displays the data polarity characteristics of RANGR mobile and MASTR II base stations. If the table indicates non-inv, the transmitter or receiver does not invert the data. If the table indicates invert, the transmitter or receiver inverts the data. If inverted data is applied to a transmitter that inverts, the resultant transmitted data will meet the conditions of the data standard. This means that if the particular entry in the table indicated "non-inv", the corresponding VG personality prom programming should also be noninverted. Conversely, if the table entry indicates "invert", the corresponding VG prom programming should be inverted.

** The WIRE LINE - DIAGNOSTICS section above was derived from material (C) Rockwell International Corporation, 1986, all rights reserved, and used by permission.

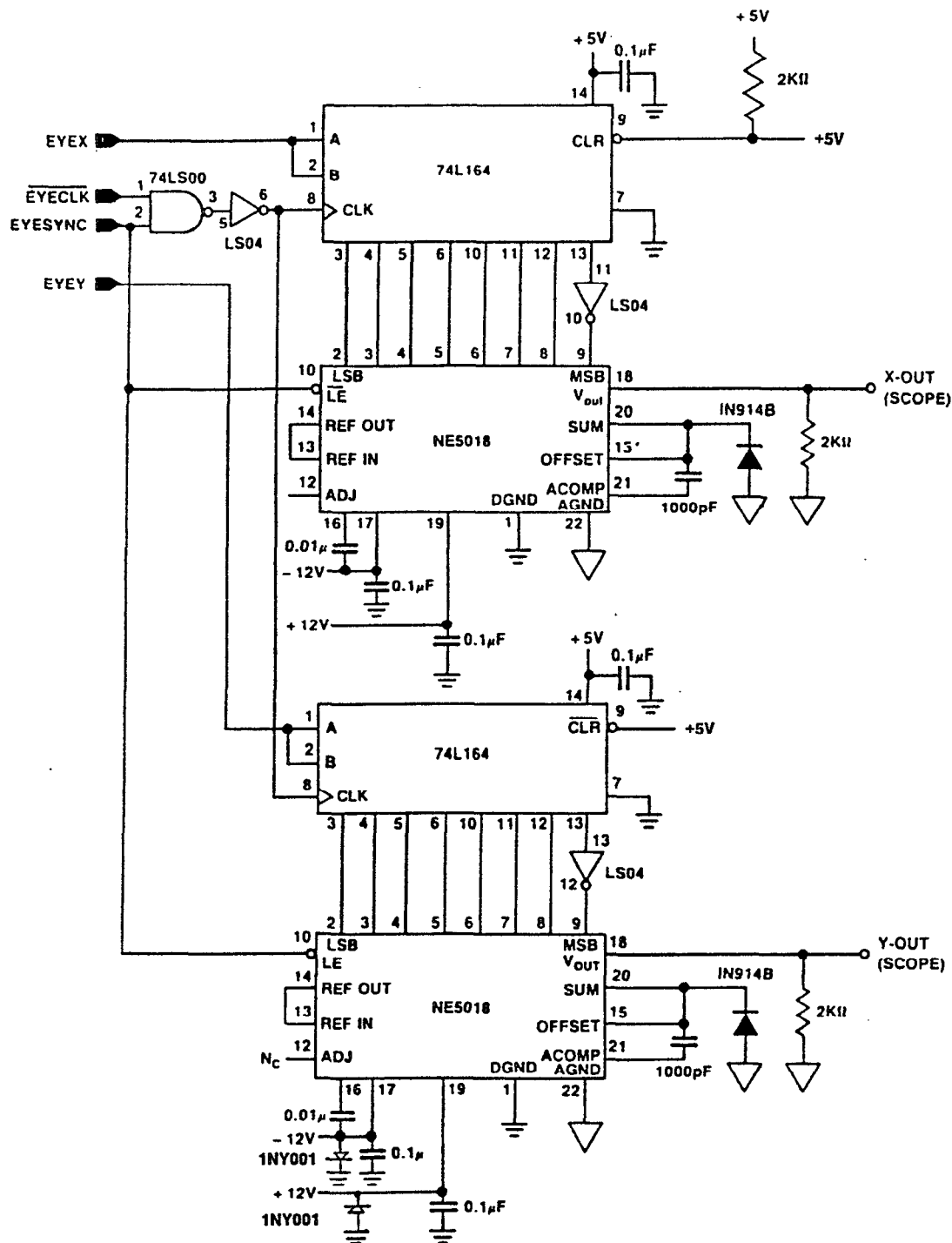


*Figure 4.3 derived from copyrighted material (C) Rockwell International Corporation, 1986, all rights reserved, and used by permission.

Figure 4-3. Eye Pattern Constellation Hardware

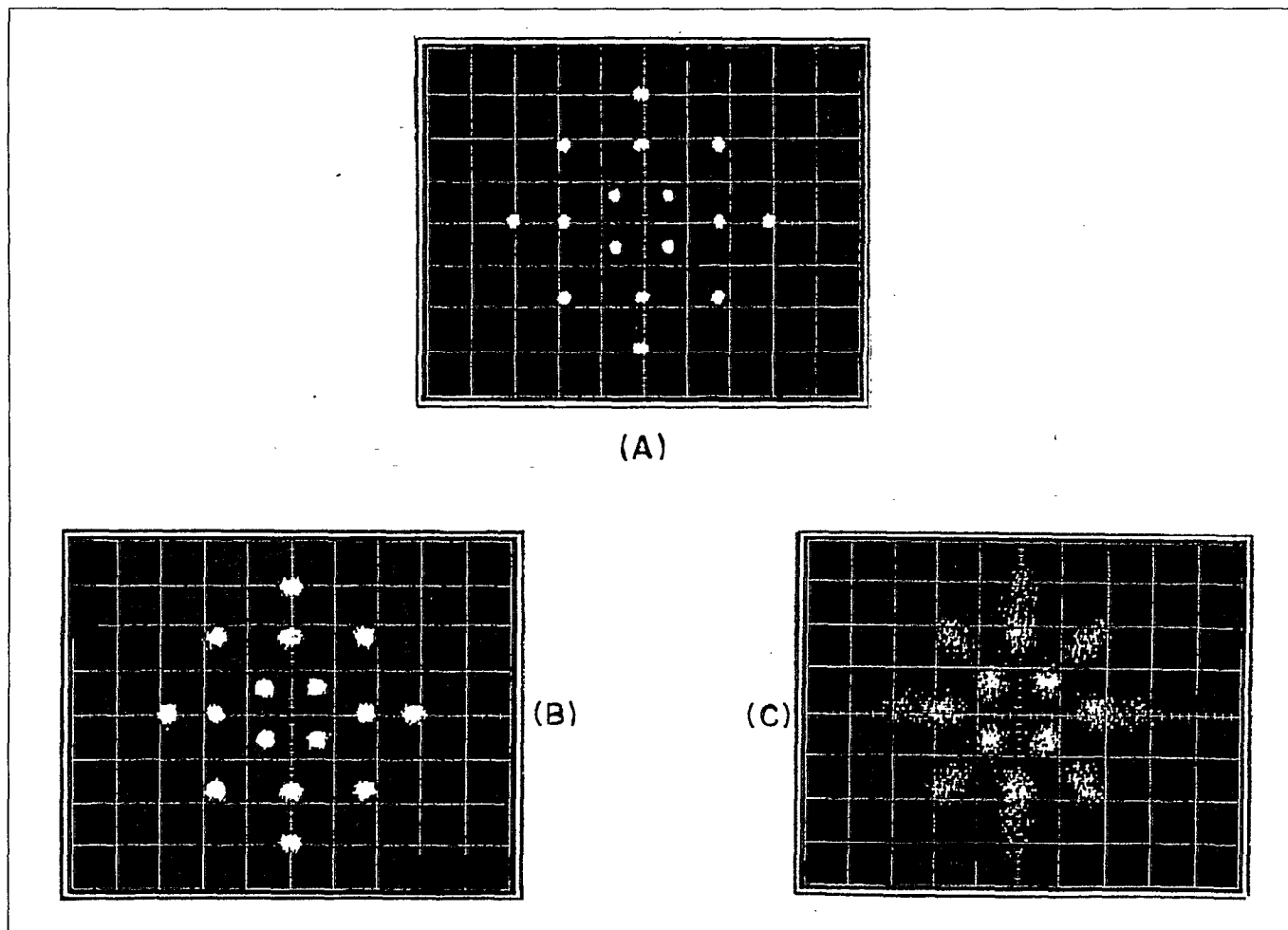


Figure 4-4. Eye Pattern Displays

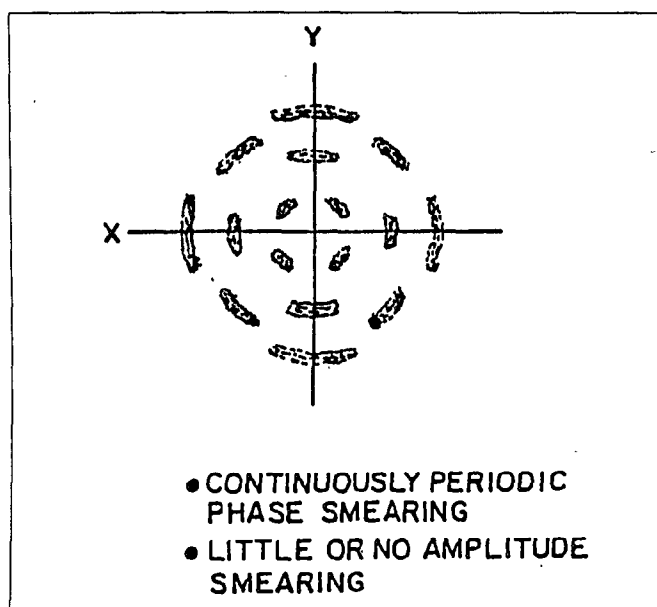


Figure 4-5

HIGH BAND			
System Board	OLD 'S' 19D900951	NEW 'S' 19D901720	'SX' 19D901650
TX Low Split	non-inv	invert	invert
TX High Split	non-inv	invert	invert
Rx Low Split	non-inv	non-inv	non-inv
Rx High Split	non-inv	non-inv	invert
UHF			
System Board	OLD 'S' 19D900920	NEW 'S' 19D901620	'SX' 19D901670
TX 403-430	non-inv	invert	invert
TX 403-440			
TX 440-470	non-inv	invert	
TX 470-494	non-inv	invert	invert
TX 494-512	non-inv	invert	
TX 440-470			
Rx 403-430	non-inv	non-inv	non-inv
RX 403-440			
RX 450-470	non-inv	non-inv	
RX 470-494	non-inv	non-inv	invert
RX 494-512	non-inv	non-inv	
RX 440-470			

Table 4-1. DELTA radio data polarity

All RANGR Receivers	= noninvert
All RANGR Transmitters	= noninvert
All MASTR II Receivers	= invert
All MASTR II Transmitters	= noninvert

Table 4-2. Data Polarity RANGR Mobile & MASTR II Station

INVERSION TEST METHOD

The following procedure supports a method to determine whether a particular piece of equipment inverts data or not. It is first necessary to verify the characteristics of the test equipment, then that equipment can be used for subsequent evaluations. The test equipment required for this procedure is:

- 1- Adjustable duty cycle pulse generator with a 50 to 100 msec pulse rate.
- 1- RF signal generator that can be FM modulated with the pulse generator.
- 1- System or deviation monitor such as Cushman CE-6 or equivalent with CRT modulation display.
- 1- Audio grade oscilloscope.

Test Equipment Verification

It is first necessary to determine the data inversion characteristics of the test equipment before proceeding with radio measurements. The test setup of Figure 4-6 describes a simple test setup.

- Manually increase and decrease the signal generator RF frequency and note the direction of the modulation display displacement from the nominal on-frequency position. This is effectively modulating the signal generator with a DC signal. This establishes the modulation polarity characteristics of the deviation monitor.
- Modulate the signal generator with a 4 to 1 duty cycle pulse at a 100 to 200 Hz rate. Note the polarity of the signal being applied to the

signal generator MOD input and compare it to the polarity of the output from the deviation monitor. This establishes the modulation polarity characteristics of the signal generator.

Transmitter Polarity Determination

Modulate the transmitter being tested with the output of the pulse generator as set up in the TEST EQUIPMENT VERIFICATION section above utilizing the digital modulator input of the transmitter. Observe the recovered modulation on the deviation monitor used in the TEST EQUIPMENT VERIFICATION section above. This will indicate whether the data has been inverted or not.

Receiver Polarity Determination

Modulate the signal generator with the pulse generator in the manner described in the TEST EQUIPMENT VERIFICATION section above. Put the generator on the RF frequency of the receiver being tested. Observe the recovered data at the output of the receiver with the oscilloscope (Vol/Sq high for MASTR II stations). This will indicate whether the data has been inverted or not.

VG TEST DEVICE

In order to functionally test a portion of a Voice Guard system, it is highly desirable to be able to generate and decode the digital signals employed by the system. Figure 4-7 shows a method of using a VG-9600-S module, in conjunction with a system monitor, to encode and decode Voice Guard signals. Other RF devices such as signal generators and deviation monitors may be substituted for the system monitor. Table 4-3 lists the strapping changes to be made to a VG-9600-S to permit proper interface with the test equipment as configured in Figure 4-7.

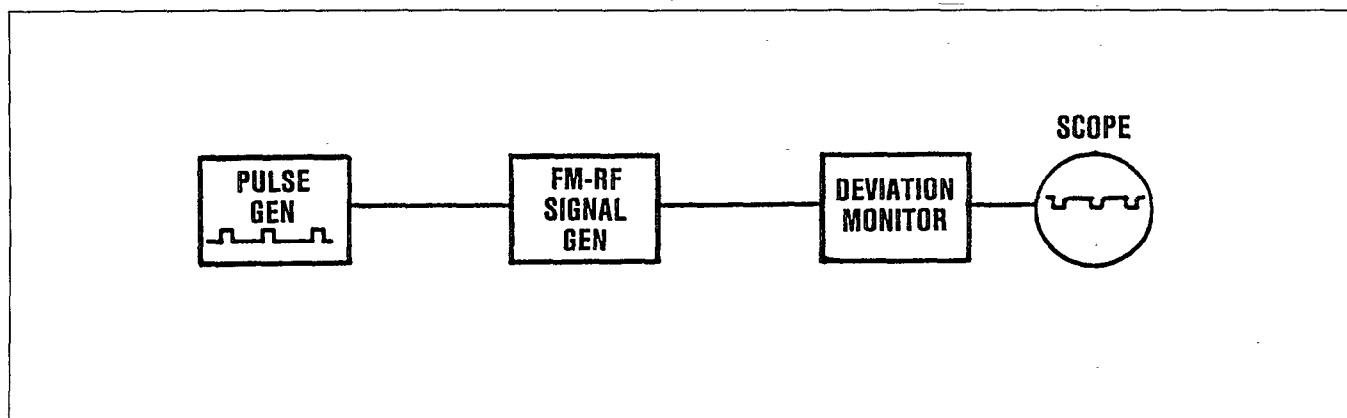


Figure 4-6. Test Equipment Setup

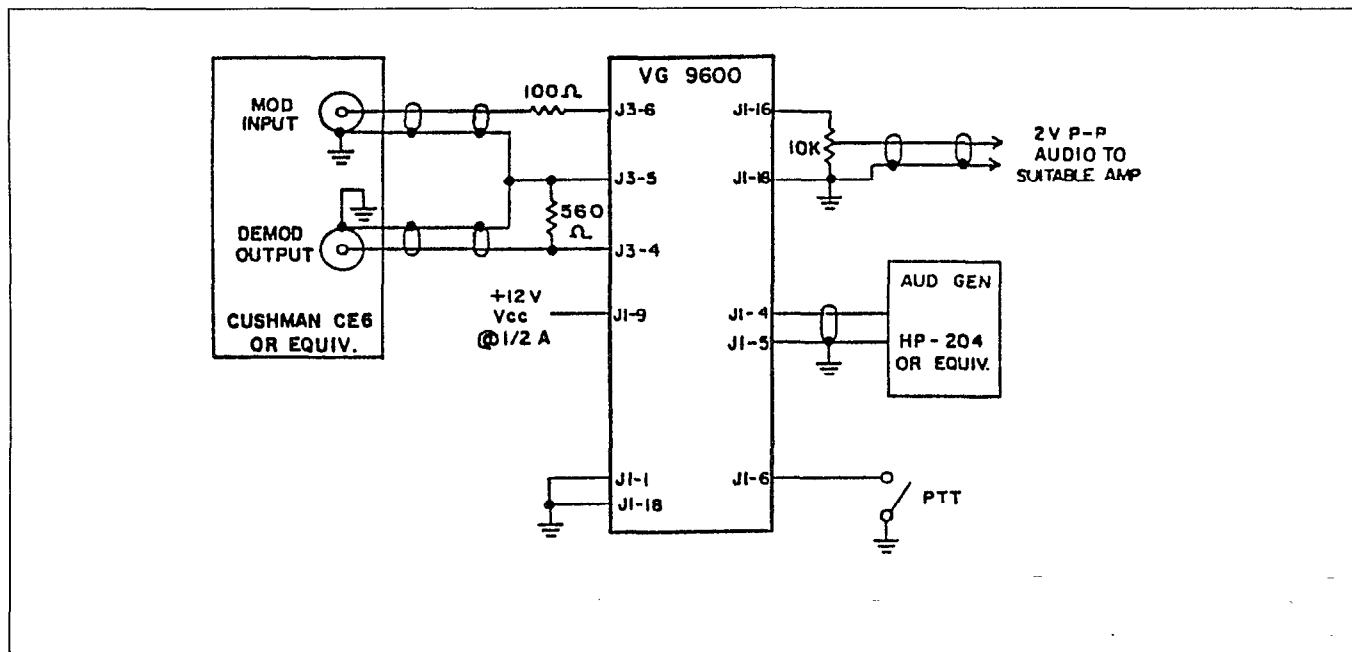


Figure 4-7. Voice Guard Test Setup

Jumper J14 - pin 2 to pin 3 = 2 section data filter
 Jumper J21 - pin 1 to pin 2 = TX data out J3-6
 Jumper J23 - pin 2 to pin 3 = RX data in J3-4

Table 4-3. VG9600 Test mode strapping

EXPECTED PERFORMANCE DEVIATIONS

The inclusion of the "VOICE GUARD" option to a DELTA or RANGR mobile radio will cause the following change in radio performance limits as noted. Similar effects can be expected with other Voice Guard equipped radios.

TX audio dist (clear mode)	
room temp	- no change
temp extremes	- 7%

RX audio dist (clear mode)	
room temp	- no change
temp extremes	- 7%

TX FM hum and noise (clear mode)	- 55 dB
----------------------------------	---------

RX hum & noise unsquelched	- 45 dB
----------------------------	---------

TX adjacent channel interference level degraded in the Guarded mode relative to the Clear mode:	- 25 to 30 dB
---	---------------

(This Page Intentionally Left Blank)

CHAPTER 5

VG SYSTEM HARDWARE AND CONFIGURATION

SYSTEM CONFIGURING

GENERAL DISCUSSION

Voice Guard capability can be provided on a complete system basis in high band and UHF. It is available on MASTR II base stations and repeaters, either with or without voting and with either end-to-end or RF only encryption. Voice Guard is available on DELTA-S or DELTA-SX and RANGR mobiles and will work with S550, S950 or S990 control units. In addition, DELTA desk top stations and, MPS and M-PD portables are also available with Voice Guard.

Encryption

In all configurations, clear or encrypted (Guarded) mode transmission is operator selectable by means of an easily accessible switch. Selection of the reception mode is always automatic in all but the FS-1027 endorsed mobiles and stations which also have a mode selector (OFF) position that disables both transmission and reception of encrypted signals. When in other than the OFF position, the FS-1027 endorsed equipments also provide automatic receive mode selection. See Chapter 1 and VG equipment instruction books for details.

Either of two encryption algorithms, DES and VGE, are available in all Voice Guard products. The DES algorithm is required for FS-1027 endorsed applications. The FS-1027 endorsement is a prerequisite for Federal Government use. Export of the DES algorithm is, in general, prohibited. The VGE encryption algorithm is acceptable for United States State Department export license to certain countries.

VGE and DES equipped radios will not talk to one another in the Guarded mode, even if the corresponding key-loaders contain the same cryptographic key. The same key-loader will not work on both types of equipment. See the SECURITY AND THE KEYS section for a detailed discussion of the cryptographic keys.

Equipment that has been endorsed as meeting the requirements of FED-STD FS-1027 has an assigned USGEID number which appears on the equipment name plate. Table 5-1 lists the assigned USGEID numbers and associated available Voice Guard equipment.

USGEID #	EQUIPMENT
00000021	VG-9600-S w/DELTA and RANGR mobiles
00000022	19A148910 DES Keyloader
00000026	MPS Personal radio
00000030	VG-9600-SR w/E/D stations
00000033	VG-9600-S w/DELTA desktop station
00000036	VG-9600-SR w/Console InterfaceUnit
00000037	M-PD Personal radio

Table 5-1

Line Requirements

All versions of Voice Guard remote stations require a four-wire control line between the control point and the remote station. In the case of end-to-end encryption, these facilities must be capable of supporting 9600 baud, 16-level telephone modem data and have transmission characteristics that are at least as good as a type 3002 telephone line. In the case of RF only encryption, the four-wire control circuit is still required but, it only needs to be voice grade. This equates to a type 2000 telephone line. The control circuit can be telephone company provided, private wire, radio, or microwave so long as the transmission characteristics are satisfied. While it is desirable to have the digital BIT ERROR RATE (BER) of the control circuit be better than 1 error in 100,000 bits (approximately 1 error in 10 minutes), Voice Guard will still operate with bit error rates worse than 5% (approximately 480 errors per second or, 1 error in every 20 bits). Since weak RF signals into the station receiver may have a 5% BER or worse, it is most important not to have the control circuit add further degradation to the BER.

Outside Addressing

When operating in the Guarded mode, eight programmable Outside Address (OA) bits located in the digital sync word provide a continual digital selective addressing capability that is roughly equivalent to Clear mode multichannel

encode/decode Channel Guard operation. If the OA of a Guarded mode signal being received matches the receive OA that has been programmed for that channel, and the cryptographic key is correct, the Voice Guard unit will pass recovered audio on to the receiver audio amplifier. If the OA's do not match, the receiver audio will not be enabled independent of whether the cryptographic keys match or not. An equivalent "all call" OA is provided that will match all receivers independent of the OA that they may have programmed. Up to 32 separate TX and RX OA's are stored in the mobile Voice Guard unit's EE personality PROM, while up to 64 separate TX and RX OA's are stored in the personality PROM of the Voice Guard equipped MPS or M-PD portable. OA selection is slaved to the channel selection switch of the radio.

A Voice Guard Station shelf or GETC only supports the programming of one TX and one RX OA. An additional response to the all-call character (hex AC) can be optionally enabled. These are set by the eight-section DIP switches (S1, S2 and S3) on the station shelf. See Chapter 3 for a detailed discussion of outside addressing.

Multifrequency Operation

Multifrequency operation is available with Voice Guard equipped radios. The DELTA mobile radio can support up to 32 channels with individual TX and RX OA's while the RANGR mobile can support up to 16 channels with individual TX and RX OA's. With an S990 control unit, a total of 128 channel operation can be obtained with the DELTA radio. This is accomplished by means of downloading a group of 32 channels. Since the Voice Guard module does not recognize the different downloaded groups, the OA assignment remains the same for each block of 32 channels. Voice Guard equipped MPS and M-PD personal radios can support up to 64 channels with individual TX and RX OA's.

End-to-end remote only stations in conjunction with a CIU and E/D (RF only encryption) stations can support two-frequency operation however, the TX and RX channels are ganged together. Frequency and Guarded/Clear mode selection is accomplished with the four tone control function tones as outlined in Table 5-2.

Function Tone- Hz	Channel	Mode
1950	F1	Clear
1850	F1	Guarded
1350	F2	Clear
1250	F2	Guarded

Table 5-2. Tone Control Function Tones

Two-frequency operation with a CIU permits separate OA's to be associated with each frequency while only one Voice Guard OA is available for both frequencies of a two frequency E/D remote station. (See the NOTES AND COMMENTS section in Chapter 3).

In the case of the E/D Remote/Repeat configuration, where the station has both a Voice Guard unit and a Voice Guard Station Shelf, the VG unit OA and the station shelf OA are independently selected and do not necessarily have to be the same.

Channel Guard Operation

While the application of Voice Guard to a system does not require that Channel Guard be employed during Clear mode operation, it is highly recommended. When operating in the Guarded mode, Channel Guard encode and decode are disabled as the Voice Guard data spectrum extends through the base band region used by Channel Guard. Since there is a finite time for a Voice Guard unit or station shelf to recognize the validity of an incoming digital signal and switch the audio paths, there will be a noticeable "burp" of data at the beginning of each Guarded mode transmission. If Channel Guard is employed in the Clear mode, this "burp" will not be heard as there will be no Channel Guard tone transmitted with the Voice Guard data hence, the receiver will not unsquelch until the Voice Guard data has been validated.

In addition, for systems without Channel Guard, non-Voice Guard equipped radios or Voice Guard equipped radios receiving an invalid OA or key, will unsquelch during a Guarded mode transmission and the data will be heard as a "white noise" hiss through out the duration of the transmission. While a Voice Guard signal sounds like noise, the modulation frequency components in the 5 to 7 kHz range, where the noise squelch operates, are filtered out to minimize adjacent channel interference and meet the FCC spectral occupancy requirements. This results in noise squelch receivers opening up in the presence of a Voice Guard data signal. Channel Guard operation in the Clear mode resolves this system situation.

VOICE GUARD STATION SHELVES

To add Voice Guard capability to a MASTR II station, equipment must be added to perform the data recognition and regeneration functions required by Voice Guard. These functions can be provided by either a VG Station Shelf, type 19D438054, or a GETC shelf, type 19D901868. Both shelves can perform the same identical Voice Guard station functions and they are directly interchangeable and operate with the same software PROM. They are each housed in a 1 rack unit (1.75 inch) high assembly that is added to a standard highband or UHF MASTR II station. Voice Guard capability may be factory or field installed. Field installation involves mounting the shelf, adding a new station harness and incorporating several simple station modifications. The station must have an FM exciter and a 19D432667 IFAS board and, if a remote configuration, be equipped for four-wire operation.

The basic functions of a VG station shelf or GETC are that of a Voice Guard data recognizer, regenerator and signal router. Either shelf consists of two serial data ports (the RF port and the line port), an RS-232 serial port, and various audio, data and control lines which interface the shelf to the station. No cryptographic information is required by a station shelf for proper VG operation. Only E/D stations, which also employ a VG-9600 module, require the operational cryptographic key to exist at the station.

The RF port modem chip receives data from the station receiver via volume/squelch high and sends reconstructed, filtered data to the transmitter modulator. When data is received, it is checked for a valid preamble, then for a valid outside address. After establishing that the signal is valid, the Voice Guard data that is continuing to be received is stored in a buffer, the preamble is reconstructed and the outside address is modified as required. Then, the entire reconstructed VG data signal is sent to the telephone line modem via the control line port modem chip in the case of remote station configuration

and to the transmitter modulator via the RF port modem chip and data filter in the case of repeat station configuration. The through-put delay to support the data recognition and reconstruction is approximately 200 msec.

The control line port on the shelf receives Guarded data from a Voice Guard equipped control point and sends Guarded data to the control point over a four-wire, data grade, control circuit. Data received on the control line port is sent to the transmitter modulator via the RF port and data filter. Transmission of Voice Guard data over the four-wire control circuit involves the use of 9600 baud, 16-level data modems at both ends of the line.

The VG station shelf and GETC both operate from the station 13.8 volt DC supply so that battery backup operation can be supported in Voice Guard as well as standard station configurations.

The shelves have eight possible operating configurations which are determined in the shelf software and are established by the settings of three configuration switches (S3 switches 5, 6, & 7). The OA characteristics are set by station shelf switches S1, S2 and S3-5. Figure 5-1 shows the OA flow diagrams for the four data signal paths in the station. See station shelf LBI-31546 for a detailed discussion. A summary of these three configuration switches follows.

Mode 0: Remote

When receiving a Guarded signal, the shelf receives data via the RF port. Upon validation of the format, the shelf then sends the data to the telephone line modem via the line port, where it is then sent to the control point via the control line. The Station Shelf, after obtaining a match with switch S1 or if the all-call function is active, passes the received OA on through to the control operator. OA detection will also be performed in the Voice Guard unit at the remote control point.

When the control operator wishes to transmit in the Guarded mode, 16-level modem data is sent up the control line to the telephone line modem and then on to the line port. Upon detection of proper format and transmit command, the shelf buffers the rest of the data, reconstructs the data preamble, keys on the transmitter, switches the modulation audio path to data and proceeds to transmit the buffered data being received. The transmit command also specifies transmitter frequency 1 or 2. The OA on the Guarded signal from the control point is retransmitted, unchanged, independent of the setting of the Shelf TX OA switch S2.

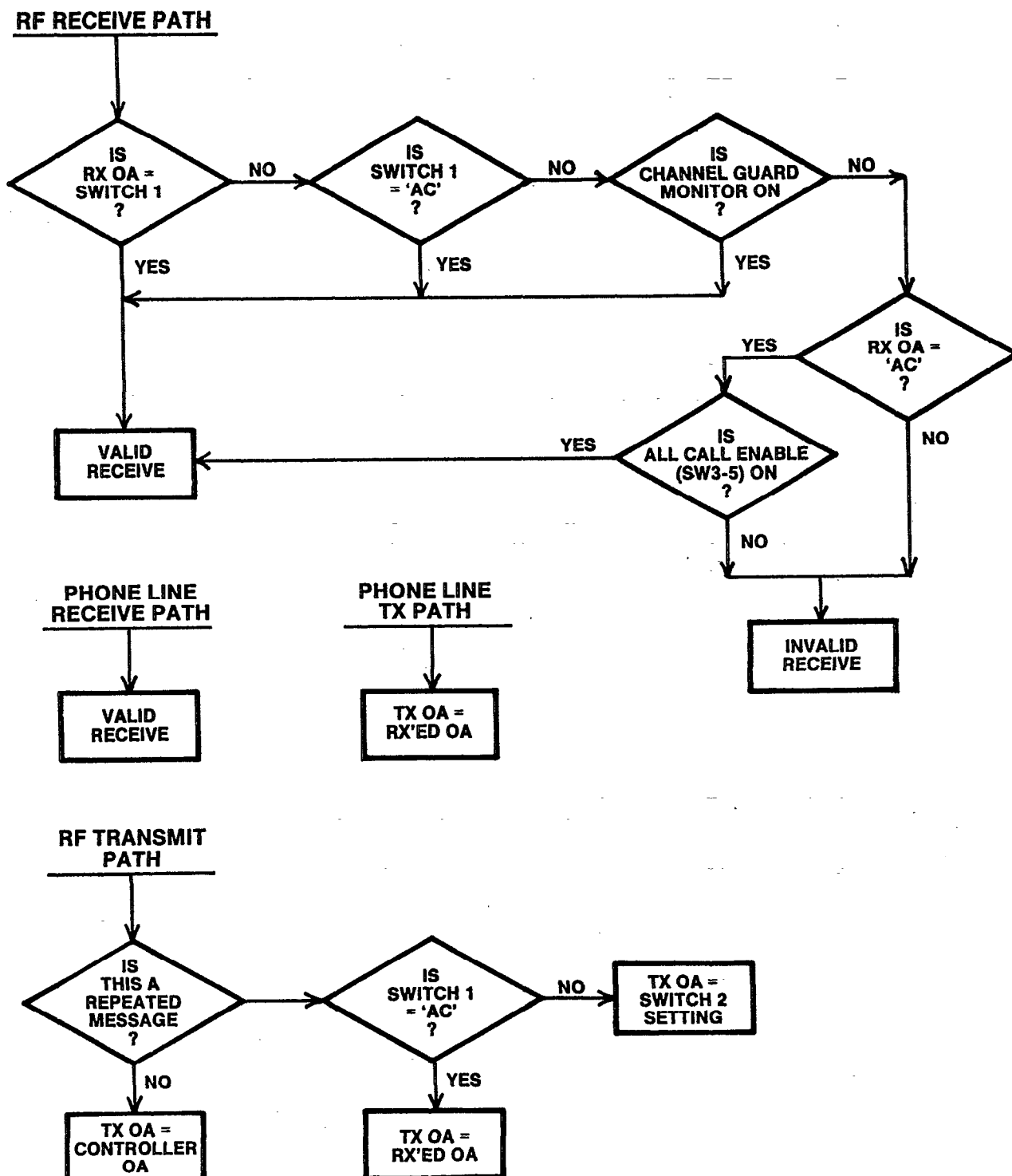


Figure 5-1. OA Flow Diagram

Mode 1: Remote

This mode is presently identical to mode 0.

Mode 2: Repeater

The shelf receives Guarded data from the RF port, checks for valid OA, buffers and delays the data, reconstructs the preamble, keys up the transmitter and retransmits the buffered data out the RF port to the transmitter modulator. Only one transmit and receive frequency are supported. The transmitted OA will be the value set into Station Shelf switch S2, unless switch S1 has been set to the "all call" character (AC) where upon the transmitted OA will be the same as the OA of the received RF signal independent of what it might be.

Mode 3: Remote/Repeat

The Shelf receives Guarded data from the RF port, checks for valid OA or the "all call" character (AC), buffers and delays the data, reconstructs the preamble, keys up the transmitter and sends the buffered data out the RF port to the transmitter and out the line port to the telephone line modem and then down the line. The received OA is sent down to the control point unchanged however, the transmitted OA will be the value set into switch S2 unless S1 is set for "AC" in which case the transmitted OA will be the same as the received OA.

Guarded data is also received from the line port via the control line and the telephone line modem. The shelf checks for valid format, buffers and delays the data, reconstructs the preamble, keys up the transmitter and sends the buffered data, via the RF port, to the transmitter modulator. The transmitted OA is the same as received from the control point independent of how S1 or S2 might be set. Only one TX and RX frequency is supported in this configuration.

Mode 4: Voted Remote/Repeat

In this mode, the signal paths are the same as for remote operation

Mode 5: Satellite receiver

This is a receive only mode. Guarded data is received on the RF port, OA validated, preamble reconstructed, data delayed to allow for telephone line modem training time and

the encrypted data is sent down the line to the voter. If the received signal is not encrypted, it is sent down the same line to the analog voter. The OA may be set for any discrete value or the "all call" character (AC).

Mode 6: Voter receiver

This configuration of Shelf software is used only for voting. The Voter Receiver receives Guarded data from a satellite receiver or a station receiver via its line port. The preamble is examined and a bit error rate is calculated. The RS-232 serial port is then used to communicate both ways between the Voter Receivers and the Voter Selector. The Voter Receiver receives commands from the Voter Selector and sends back status and reconstructed Guarded data when commanded to do so. The OA should be the same as that set in the corresponding satellite receiver.

Mode 7: Voter Selector

The Voter Selector polls each Voter Receiver over the RS-232 port and after deciding which one has the best bit error rate, commands that Voter Receiver to send its data to the selector at 19.2 kilobaud via the RS-232 port. The Voter Selector then buffers and delays the data approximately 250 msec and then sends it out through its line port. The received OA is passed in, unchanged, independent of switches S1 and S2. The Voting Selector revotes at the end of each data frame (approximately 4 times per second).

GETC CONFIGURATION

The GETC shelf (19D901868) is a versatile micro-processor based station communications control shelf that is utilized in GE Voice Guard and Trunking systems. The GETC shelf is a logical "superset" of the VG Station Shelf. Corresponding IC's, adjustments and connectors all carry identical reference numbers. Both types of shelf execute the same software code PROM.

There are a number of jumpers on the GETC which can be changed to permit system application reconfiguration. Table 5-3 shows the required jumper positions and equipment complement for the various Voice Guard station applications.

JUMPER	VG REM VG REM/RPT VG SAT RX VG VOTED REM/RPT	VG RPT	VG VOTER SELECTOR	VG VOTER RECEIVER	FUNCTION
P11	1 & 2	1 & 2	1 & 2	1 & 2	RX data select
P12	1 & 2	1 & 2	1 & 2	1 & 2	Modem CTS select
P13	2 & 3	2 & 3	2 & 3	2 & 3	No VG function
P14	2 & 3	2 & 3	2 & 3	2 & 3	Enables J6-10 for VG
P15	2 & 3	2 & 3	2 & 3	2 & 3	Sets U27-D for VG
P16	1 & 2	1 & 2	1 & 2	2 & 3	19.2 kB RXd path
P17	2 & 3	2 & 3	2 & 3	2 & 3	Holds U34-C open
P18	2 & 3	2 & 3	2 & 3	2 & 3	Q-5 no VG function
P20	2 & 3	2 & 3	2 & 3	2 & 3	Enables COMB PTT
P21	2 & 3	2 & 3	2 & 3	2 & 3	Sets RXd limiter T/C
P22	2 & 3	2 & 3	2 & 3	2 & 3	Removes notch filter
P24	2 & 3	2 & 3	2 & 3	2 & 3	Enables J6-14 for VG
P25	2 & 3	2 & 3	2 & 3	2 & 3	Enables J6-13 for VG
P26	2 & 3	2 & 3	2 & 3	2 & 3	Enables J7-7 for VG
P28	2 & 3	2 & 3	2 & 3	2 & 3	Enables J7-11 for VG
P29	1 & 2	1 & 2	2 & 3	1 & 2	Voter Sel 1950 osc
P30	2 & 3	2 & 3	2 & 3	2 & 3	Sets up clock sources
P31	4 & 5	4 & 5	4 & 5	4 & 5	NOTE: P30 & 31 go to J30
P44	2 & 3	2 & 3	2 & 3	2 & 3	Selects type 27128
P45	2 & 3	2 & 3	2 & 3	2 & 3	RAM A-11 to addr bus
P46	1 & 2	1 & 2	1 & 2	1 & 2	Disables U29-E output
P47	1 & 2	1 & 2	1 & 2	2 & 3	Voter RX displ mode
P48	1 & 2	1 & 2	2 & 3	1 & 2	Voter Sel displ mode
P50	1 & 2	1 & 2	2 & 3	1 & 2	Voter Sel function

JUMPER	VG REM VG REM/RPT VG SAT RX VG VOTED REM/RPT	VG RPT	VG VOTER SELECTOR	VG VOTER RECEIVER	FUNCTION
P51	2 & 3	2 & 3	2 & 3	2 & 3	Non-VG function
P52	2 & 3	2 & 3	2 & 3	2 & 3	Non-VG inverter
P53	2 & 3	2 & 3	2 & 3	2 & 3	Non-VG inverter
P54	1 & 2	1 & 2	1 & 2	1 & 2	Enables U15-A control
P55	1 & 2	1 & 2	1 & 2	1 & 2	Non-VG function
P60	1 & 2	1 & 2	1 & 2	1 & 2	TXd to data filter
P61	1 & 2	1 & 2	1 & 2	1 & 2	Selects type 27128
P62	1 & 2	1 & 2	1 & 2	1 & 2	Sets U4 freq for VG
P63	OMIT	OMIT	OMIT	OMIT	Data filter for VG
P64	OMIT	OMIT	OMIT	OMIT	Data filter for VG
P65	OMIT	OMIT	OMIT	OMIT	Data filter for VG
P66	OMIT	OMIT	OMIT	OMIT	Data filter for VG
P67	OMIT	OMIT	OMIT	OMIT	RX tel line term
P68	1 & 2	1 & 2	1 & 2	1 & 2	Enables J6-1 for VG
P69	1 & 2	1 & 2	1 & 2	1 & 2	Puts COMB PTT on bus
P70	1 & 2	1 & 2	1 & 2	1 & 2	Enables J7-6 for VG
P71	1 & 2	1 & 2	1 & 2	1 & 2	Enables RTS
19A705178*	YES	NO	YES	YES	Tel. Line Modem
19C336900*	NO	NO	YES	NO	1950 Hz OSC Module
19B235062*	NO	NO	YES	NO	1950 Hz OSC Cable
19A149219*	YES	YES	NO	NO	PGM'D PROM - Station
19A149334*	NO	NO	YES	YES	PGM'D PROM - Voter

Table 5-3. GETC Configurations For Voice Guard

*Hardware modules

CONSOLE INTERFACE UNIT

In end-to-end encryption remote station configurations, the VG 9600 encryption module must be located at or near the control point. In addition, a telephone line data modem must also be employed to interface the 9600 baud Voice Guard data to the control circuit. Moreover, it is necessary to be able to employ Voice Guard with several paralleled console positions. This is accomplished by means of a Console Interface Unit (CIU).

The CIU is normally located near a console or group of consoles which are all interconnected on a four-wire, AC tone control basis. All communication between the CIU and the console(s) is in the clear, independent of Voice Guard operation. The Voice Guard encryption/decryption is performed in the CIU and, when operating in the Guarded mode, communication with the remote station is encrypted. The CIU provides audio loop-around to the consoles so that each dispatcher can hear both ends of a Guarded conversation. The CIU also supports both remote and voted remote/repeat operation. Interconnection between the CIU and the remote station is by means of a four-wire data grade circuit. One CIU is required for each active remote radio station. Single and two-frequency remote station operation is supported.

The CIU normally monitors the tone control sequences being sent from console(s). The transmit tone control sequence usually consists of a 175 msec burst of high level 2175 Hz tone followed by a 40 msec burst of one-of-four function tones followed by continuous low 2175 Hz tone for the duration of the transmission. The four function tones are assigned as F1-Clear, F1-Guarded, F2-Clear and F2-Guarded. If the CIU detects that a function tone is associated with Guarded mode operation, it breaks the audio control path to the remote transmitter before the completion of the tone sequence so that the remote transmitter never keys on the air. The CIU also switches the VG unit into the proper audio paths and sends VG data to the remote station where the station shelf decodes the control information and turns on the transmitter.

If the CIU detects that the tone control sequence is not associated with Guarded mode operation, the tone control sequence is allowed to pass on to the remote station, unchanged, where the Clear mode control circuitry turns on the transmitter.

If a valid Guarded mode signal is sent down the control circuit from the remote station, the VG unit will detect its presence and initiate proper switching of receive audio paths inside the CIU.

The CIU consists of two shelf assemblies. One is a 1-rack unit shelf which houses the tone detectors, switching and control circuitry, and the telephone line modem. The other is a 2-rack unit shelf which supports a power supply, VG 9600 and optional Keep-alive power supply.

The keep-alive power supply is required with the DES configurations and provides a means of retaining the cryptographic keys for over 1000 hours when the AC line power has been removed. When AC power is applied to the CIU, the keep-alive batteries have only a few hundred nano-amperes drain and should be expected to provide a shelf life well in excess of 1 year. A low battery indicator LED is provided to warn that the keep-alive batteries require replacement. The batteries are standard alkaline AAA size cells. VGE operation does not require a keep-alive power supply.

The Voice Guard module to be employed with a CIU must be strapped internally as an (SR) configuration but requires special personality programming. See LBI-31670 or 31671 for additional information.

VOICE GUARD MODULES

The Voice Guard modules used with DELTA and RANGR mobile radio and with DELTA Desktop and MASTR II stations are all generically similar though they may be configured for different applications by rearranging a series of jumper plugs on the Voice Guard module audio board and by different programming in the personality EEPROM.

Two optional delays that are set in the EEPROM by means of a TQ-2310 programmer are:

TX ATTACK DELAY = The delay between the issuance of PTT and the switching of the TX audio path from analog modulation to digital modulation. This is the delay that would be set to support, for instance, G-STAR.

ADDNL DATA DELAY = The delay between the switching of the TX audio path to digital and the actual commencement of transmitting Voice Guard preamble. This delay would be associated with the training time for line modems in end-to-end encryption stations.

The standard strapping configurations of Voice Guard modules are shown in LBI-31545, LBI-31665 and LBI-31674. The default EEPROM programming provided by the TQ-2310 programmer is as follows:

DELTA SX Mobiles: use VG-9600 S or SW, or VGE-9600 SW

TX Attack Delay = 10 msec
 Addnl Data Delay = 30 msec
 Channels 1-22 OA = 55
 Channels 1-22 TX data = Inverted
 Channels 1-22 RX data = Inverted
 Channels 23-32 = Various test combinations

E/D Stations: use VG-9600 SR or SRW, or VGE-9600 SRW

TX Attack Delay = 10 msec
 Addnl Data Delay = 30 msec
 All channels OA = 55
 All channels TX data = Not inverted
 All channels RX data = Inverted

MASTR Controller: use VG-9600 C or CW, or VGE-9600 CW

TX Attack Delay = 175 msec
 Addnl Data Delay = 250 msec
 All channels OA = 55
 All channels TX data = Inverted
 All channels RX data = Inverted

REPEATER CONFIGURATION

A Voice Guard repeater system consists of Voice Guard equipped mobiles and portables, and a MASTR II repeater station that has been equipped with a GETC or Voice Guard Station Shelf. Clear mode messages are repeated normally. Guarded mode messages with proper outside address are recognized by the GETC or Voice Guard Station Shelf which then buffers and delays the data, reconstructs the digital preamble and outside address, keys up the transmitter and sends the entire data message. Figure 5-2 depicts a typical repeater system block diagram. Standard repeaters are equipped for one frequency operation.

Voice Guard repeater only operation is selected by station shelf mode 2.

END-TO-END ENCRYPTION CONFIGURATIONS

These configurations all require that a Voice Guard module be installed at the control point and that Guarded mode transmissions between the control point and the remote station will always be encrypted. There is no requirement for having the cryptographic key at the station location. The control line must be capable of supporting 16-level telephone line modem data as well as voice. A telephone company supplied four-wire line type 3002 meets these requirements. Special conditioning C1, C2 or C4 is not required but presents no problems. D1 conditioning, while it will most adequately handle the modem

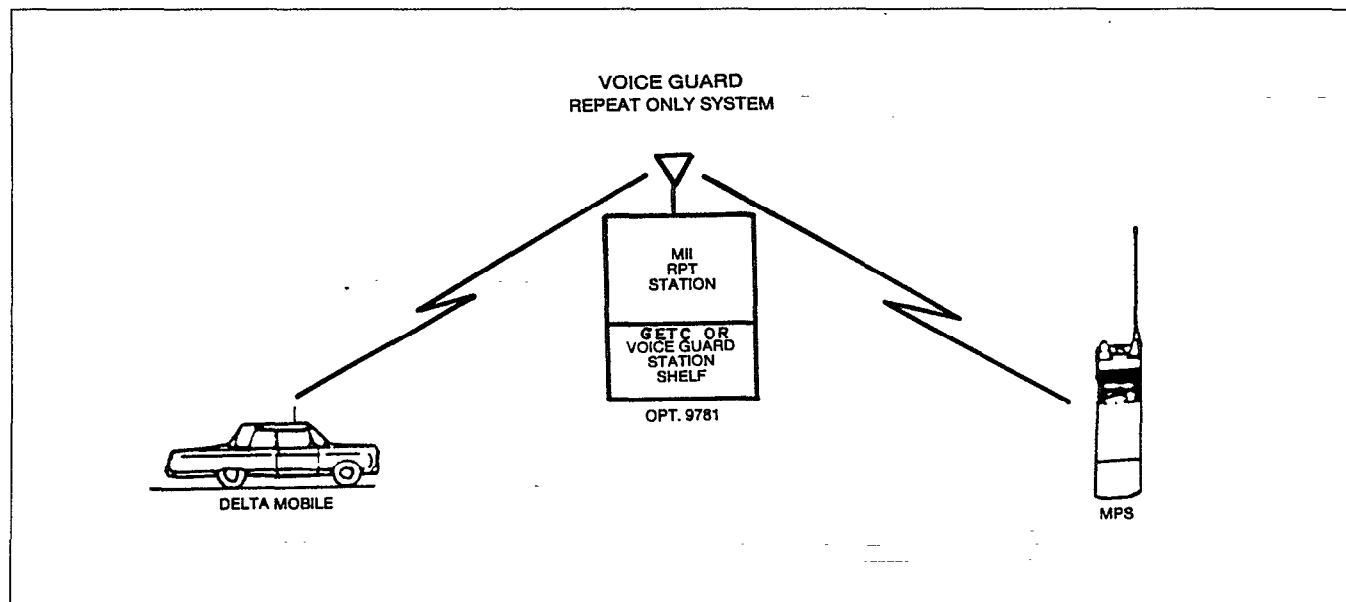


Figure 5-2. Typical Repeater System Block Diagram

data, may present problems in the handling of clear audio voice. Any equivalent data grade private wire, radio or microwave link may be employed.

REMOTE ONLY

An end-to-end Voice Guard Remote system consists of Voice Guard equipped mobiles and portables, a MASTR II tone remote controlled base station with a GETC or Voice Guard Station Shelf, a CIU and one or more consoles or consolettes. The station and CIU are interconnected via a four-wire (duplex) data/voice grade control circuit.

When idle, the station sends 1950 Hz tone down the control line to the CIU. This keeps the CIU speaker muted. When a clear signal is received, the 1950 Hz tone is removed from the control circuit and audio is sent to the controller (speaker). To transmit in Clear mode, the CIU allows the console generated keying tones and clear audio to go up the control circuit to the remote station.

When a Guarded signal is received by the station, the 1950 Hz tone is again removed from the down path, the GETC or Voice Guard station shelf buffers, reconstructs and delays the data and then sends it down to the controller as 16-level phone line modem data. The CIU converts the modem data back to two-level data and passes it on to the Voice Guard unit which decrypts the data and sends audio to the console(s).

When Guarded mode messages are to be transmitted, audio from the console is delivered, via the CIU, to the Voice Guard unit which encrypts it and sends it to the telephone line modem in the CIU. Digital data is then sent up the control

circuit between the two telephone line modems. Keying and channel select commands are in the data and are interpreted by the station shelf which selects the operating channel, keys up the station and transmits the data.

These remote only stations are normally supplied for single frequency operation but can be optionally supplied for two-frequency operation. However, the transmit and receive channels are ganged together and cannot be readily separately selected.

Voice Guard remote only operation is selected by station shelf modes 0 or 1. Figure 5-3 shows the block diagram configuration of an end-to-end Voice Guard remote only station.

REMOTE/REPEAT

A Voice Guard remote/repeat system combines the functions of a remote station and a repeater station with the remote function having priority over repeat. Clear and Guarded messages are repeated exactly as in the repeat system described in the REPEATER CONFIGURATION section above, if no remote message is in progress. Remote operation is as described in the REMOTE ONLY section above. Received messages are repeated and are also sent down the control circuit to the CIU at the control point. If the remote path is keyed up while a signal is being repeated via the RF receiver path, the station will remain keyed up but the modulation will be switched to the remote path. If the remote path is unkeyed while the repeat receiver is still receiving a signal, the station modulation will revert to the RF receiver path.

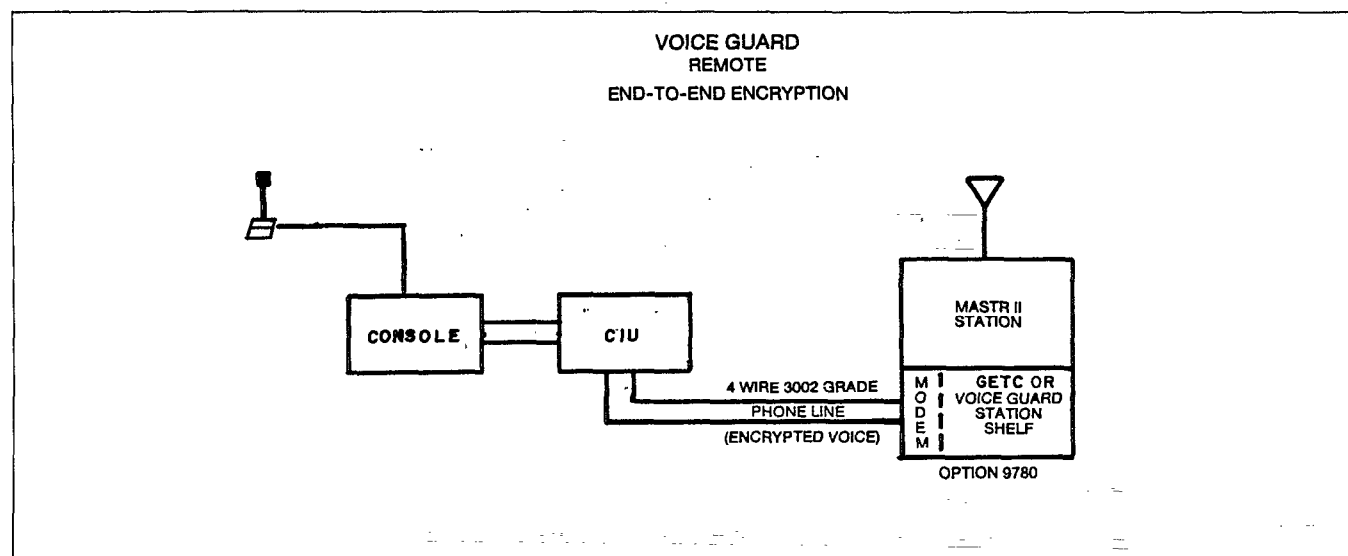


Figure 5-3. End-To-End Voice Guard Remote Only Block Diagram

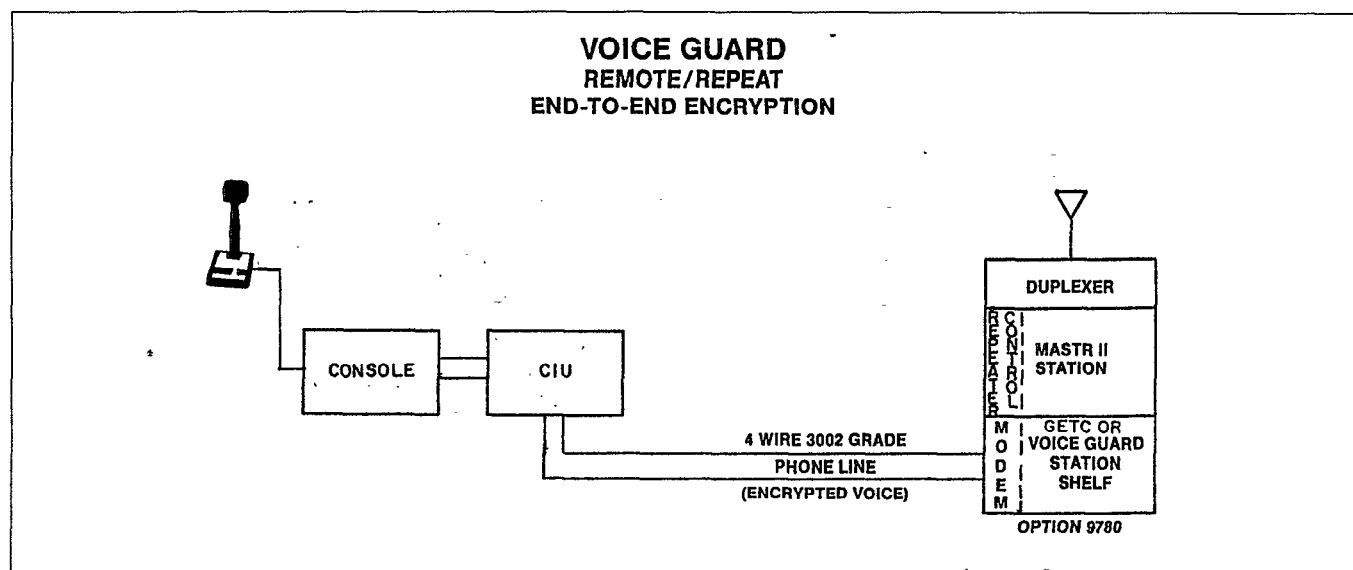


Figure 5-4. Remote/Repeat System Block Diagram

Voice Guard remote/repeat operation is selected by the station shelf mode 3. Figure 5-4 shows the simplified block diagram of a remote/repeat system.

VOTED REMOTE

In a Voice Guard voted remote system, up to 12 Mastr II satellite receivers, each equipped with a GETC or Voice Guard station shelf, replace the original analog satellite receivers. The received clear audio or VG data is sent via a single data grade phone line to a central location where the clear audio or VG data signals are compared in parallel analog and digital voters. The best message is passed on to a CIU. Digital voter addressing capability exists for handling up to 31 satellite receiver locations, however, such a system would be special.

Clear audio is voted by a normal GE VSD Voting Selector. Voice Guard data is voted by a special arrangement of GETC or Voice Guard station shelves, called Voter Receivers, plus one extra shelf called a Voter Selector to control the Voter Receivers and communicate to the CIU.

When not receiving, the satellite receivers apply a 1950 Hz tone to their lines which squelch the receiver modules in the VSD voter. A tone generator is added to the Voter Selector shelf which applies 1950 Hz to the downlink line to keep the CIU output to the console(s) muted during idle times.

When a clear message is received by some of the satellite receivers, the 1950 Hz is removed from the respective output lines. The VSD voter immediately votes and passes the best audio on to the CIU. At the same time, the VSD voter instructs the VG Voter Selector shelf to remove the 1950 Hz tone being sent to the CIU.

When a Guarded message is received, 1950 Hz is again removed from the respective satellite receiver output lines. The active VG Voter Receivers sync on the VG data in about 60 ms. Each active receiver buffers its received data and calculates a bit error rate (BER) based on the expected preamble bits. When polled by the Voter Selector, each Voter Receiver passes its BER calculation on to the VG Voter Selector which chooses one and commands it to send it one frame of data at 19.2 kilobaud. The VG Voter Selector buffers the data it receives from the VG Voter Receiver, reconstructs preamble, and sends the data on to the CIU at 9.6 kilobaud. The Voice Guard signal is voted every data frame (approximately 4 times per second) based on frame header bit error calculations.

The station configuration for Voice Guard Voted Remote only operation is the same as Voted Repeat and Voted Remote/Repeat operation and is selected by station shelf mode 4. See Figure 5-5 for a simplified block diagram of a Voted Remote system.

VOTED REPEAT

A Voice Guard Voted Repeat system requires a MASTR II Remote or Remote/Repeat station with a Voice Guard Station Shelf. The GETC or VG Station Shelf handles data in a full duplex manner when operating in this mode. The software employed in the station shelf is the same for all VG voted operation. The station receiver is included as one of the satellite receivers. Repeat keying is performed by a Remote Keying Panel (RKP) under control of both the analog and digital voters.

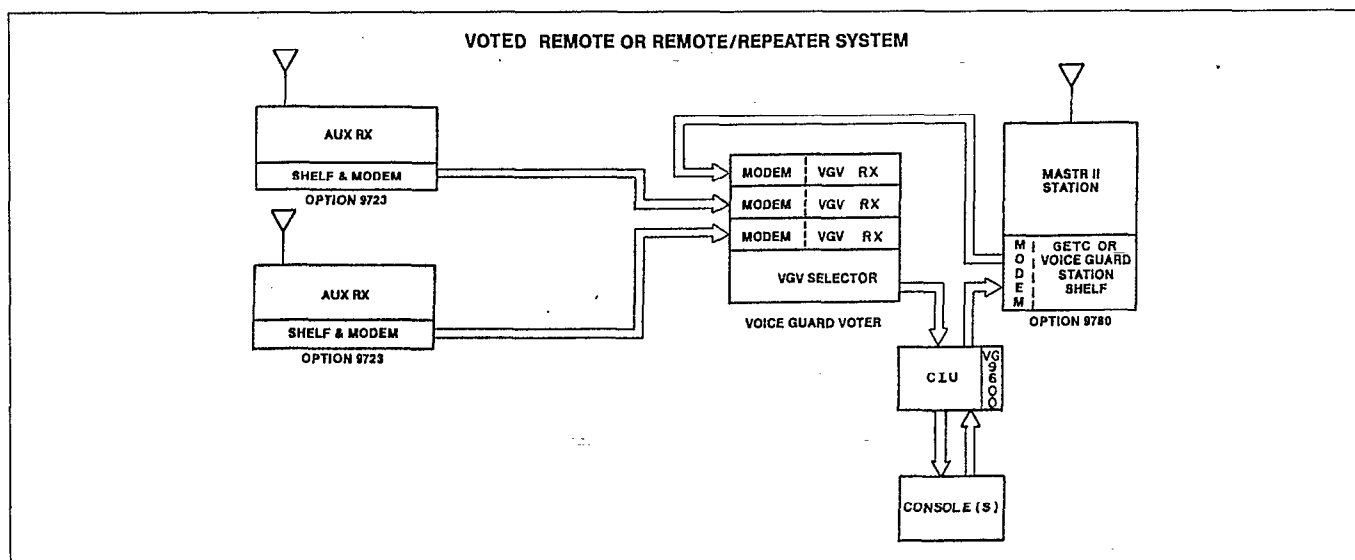


Figure 5-5. Block Diagram Voted Remote System

Each station receiver or satellite receiver applies 1950 Hz to its downlink control line when idle. When a clear message is received, 1950 Hz tone is removed from the line, the analog voter then votes and applies a keying signal to the RKP. The RKP generates the station keying tones, applies them to the uplink control line to the station and then sends voted audio.

When a Guarded message is received, the 1950 Hz tone is removed from the lines to the voter. The analog voter begins the keying sequence through the RKP. Before the keying sequence is complete, digital sync is recognized in the VG Voter Receiver shelves and the VG Voter Selector sends an inhibit signal to the RKP. The VG Voter Selector then

transmits the best data stream on to the station. The GETC or Voice Guard Station shelf interprets the keying command in the data, keys up the station and transmits the voted data.

In those special situations where the voter and the repeater transmitter are co-located, it is possible to eliminate the RKP and to interconnect the VG voter output to the station shelf by separate RS-232 lines and not use the telephone line modems. Voice Guard Voted Repeat operation is selected by station shelf mode 4. Figure 5-6 shows the simplified block diagram of a voted repeat system.

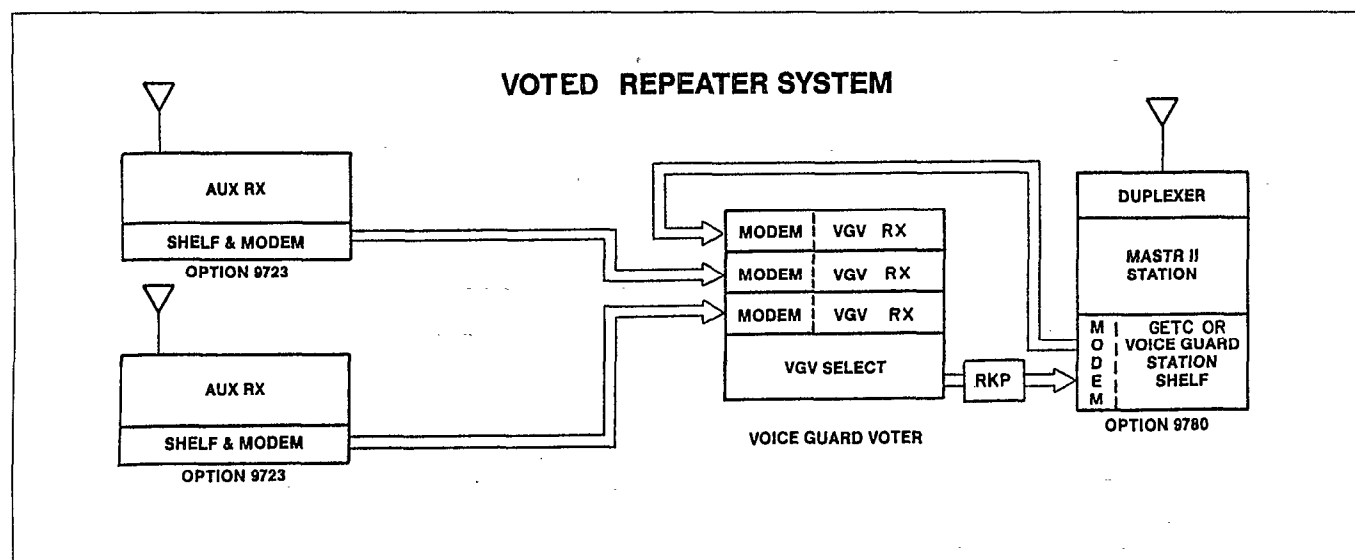


Figure 5-6. Voted Repeat System Block Diagram

VOTED REMOTE/REPEAT

This configuration is very similar to the combination of the VOTED REPEAT system and the VOTED REMOTE system described above. The GETC or VG station shelf must still handle VG data in a full duplex manner when operating in the Voted Remote/Repeat mode. All of the voted modes of Voice Guard station operation are also selected by the station shelf mode 4. See Figure 5-5 for a simplified block diagram of Voted Remote/Repeat operation.

SATELLITE RECEIVER

In end-to-end encryption voting systems, each satellite receiver applies a 1950 Hz tone to the downlink line when the receiver is idle. When a Clear mode message is being received, the 1950 Hz tone is removed and the analog audio is put on the downlink line to the voter.

When a Guarded mode signal is being received, the GETC or Voice Guard shelf examines the digital format and the OA. If valid, the 1950 Hz tone is removed from the line and the complete Voice Guard signal, as reconstructed by the shelf, is sent down the line to the Voice Guard digital voter via the telephone line modem. This circuit must still be data grade, as previously discussed however, no uplink path is required. The data modems do not require a full duplex path in order to be trained for one-way data transmission.

STATION FIELD UPGRADE

Voice Guard equipped MASTR II stations are not only available from the factory but can also be field modified to support VG operation.

Mods Common To All Stations

The following describes the modifications that must be made to all MASTR II station configurations in order to upgrade them to support Voice Guard operation. It is mandatory that a phase modulated exciter be replaced with an FM exciter. This, in conjunction with the proper application of the referenced modification instructions, should qualify the station for digital emission (FCC emission designators 16K0 F1D or 16K0 F1E). Table 5-4 shows the required new components that must be employed for all Voice Guard station configurations.

406 - 450 MHz	
Exciter	19D432679G1
Audio Processor	19C321542G2
FM ICOM	19A130605G3
450 - 512 MHz	
Exciter	19D432679G2
Audio Processor	19C321542G2
FM ICOM	19A130605G4 (450-470 MHz)
	19A130605G5 (470-494 MHz)
	19C130605G6 (494-512 MHz)
138 - 155 MHz	
Exciter	19D423249G2
Audio Processor	19C321542G2
FM ICOM	19A130605G1
Filter assy	19B226748G1
150.8 - 174 MHz	
Exciter	19D423249G2
Audio Processor	19C321542G2
FM ICOM	19A130605G2
Filter assy	19B226748G2

Table 5-4

End-To-End Station Modifications

Table 5-5 describes the additional applicable drawings and modification instructions that apply to Voice Guard end-to-end encryption station options 9780 (Remote or Remote/Repeat) and 9781 (Repeat only).

APPLICABLE DRAWINGS			
NAME	DWG NUMBER	9780	9781
VG Station Shelf or GETC Modem PROM	19D438054G1 19D901868G3 19A705178P1 19A149219	x x x x	
VG Station Shelf or GETC PROM	19D438054G2 19D901868G3 19A149219	x x x	
Wiring harness Voter tone board Capacitor Manual Manual	19C851484G4 19C336900G1 19A701534P7 LBI-4913 LBI-31532	x x x x x	x x x x
MODIFICATION INSTRUCTIONS			
NAME	DWG NUMBER	9780	9781
Exciter mods Appl. assy. Instl. assy. Harness mod. instr. Rx mod. instr.	19C336664P1 19D417483P22 19D417633P1 19C336664P2 19C336664P3	x x x x x	x x x x

Table 5-5. Options 9780/9781 Drawings & Modification Instructions

RF ONLY ENCRYPTION/DECRYPTION CONFIGURATIONS

These encrypt/decrypt (E/D) configurations all require that the Voice Guard unit be installed at the remote station and satellite receiver sites. The control circuit between the dispatch point and the remote site(s) will always be unencrypted (clear) independent of whether the RF path is encrypted or clear. This now requires that the remote site(s) be adequately secure as the operational cryptographic key must be at each of the remote E/D sites.

In order to deliver the Voice Guard unit generated alert tones to the control point, a four-wire control circuit is still required however, it only needs to be a voice grade, telephone type 2000 line, as opposed to the data grade line for end-to-end configurations.

Guarded mode as well as Clear mode transmissions can be made from an E/D station cabinet, utilizing the service microphone and speaker in the cabinet. The dispatch point will hear the Clear mode alert beeps but will not hear the transmitted audio in either mode. The station intercom option is not compatible with an E/D station with Voice Guard.

E/D stations can be factory or field modified. The option numbers that cover the E/D station combinations are 9783 through 9790 and 9797. The basic station configuration requirements are; tone remote controlled, four-wire audio and have an FM exciter. The added hardware for E/D operation is: Voice Guard control card, added station harness and a shelf assembly supporting the Voice Guard unit and optional keep-alive power supply. In the case of an E/D Remote/Repeat station, a Voice Guard Station Shelf or GETC (see the VOICE GUARD STATION SHELVES section above) is also required.

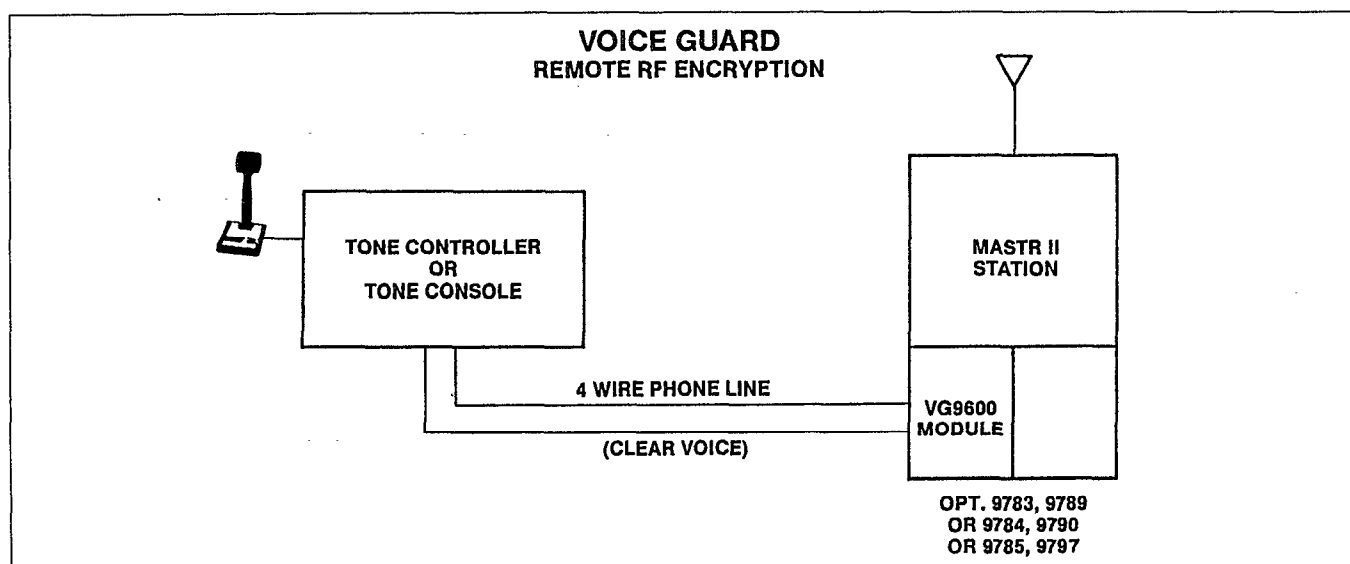


Figure 5-7. E/D Remote Only Block Diagram

E/D REMOTE ONLY (9783, 9784, 9785, 9789, 9790, 9797)

An E/D Voice Guard Remote system consists of Voice Guard equipped mobiles and portables, a MASTR II tone remote controlled base station equipped with a Voice Guard unit and ancillary hardware and a slightly modified tone control console. E/D stations are available in one frequency or two frequency configurations.

The tone remote control system employed in MASTR II stations sends the channel frequency select information at the beginning of each transmission. This information is in the form of a nominal 125 msec "SECUR-IT" tone burst followed by a nominal 40 msec burst of one-of-four function tones then a continuous, low-level 2175 Hz transmitter keying tone.

In the E/D Voice Guard stations, two of the frequency select tones have been reassigned for Clear mode and Guarded mode function select. This is to assure that the selected voice mode is always properly implemented at the start of each transmission.

The Voice Guard control card, which plugs into the station control shelf, performs the redirection of the control tone functions. Some station backplane wiring modification is also required to support this control tone function reassignment. The control tone frequency assignment for E/D stations is as follows:

FUNCTION		TONE CONTROL FREQUENCY (Hz)	
		Remote	Remote/Repeat
Clear	- channel 1	1950	1950
Guarded	- channel 1	1850	1850
Clear	- channel 2	1350	-
Guarded	- channel 2	1250	-
CG Monitor		2050	2050
Repeat enable			1550
Repeat disable			1450

The console or consolette employed with an E/D station should be configured for standard, four-wire operation except for the addition of a selector switch labeled GUARDED/CLEAR and for two frequency operation, a channel selector switch that is interconnected with the GUARDED/CLEAR switch so as to accommodate the control function table shown above. Figure 5-7 shows the simplified block diagram of an E/D remote only station.

E/D REMOTE/REPEAT (9786, 9787, 9788)

An E/D Voice Guard Remote/Repeat configuration combines the functions of an E/D Remote station (see E/D REMOTE ONLY section above) and a Voice Guard Repeater (see REPEATER CONFIGURATION section above) with the remote function having priority over the repeat function. This E/D station has a Voice Guard unit which encrypts and decrypts Voice Guard data at the station and interfaces with; the

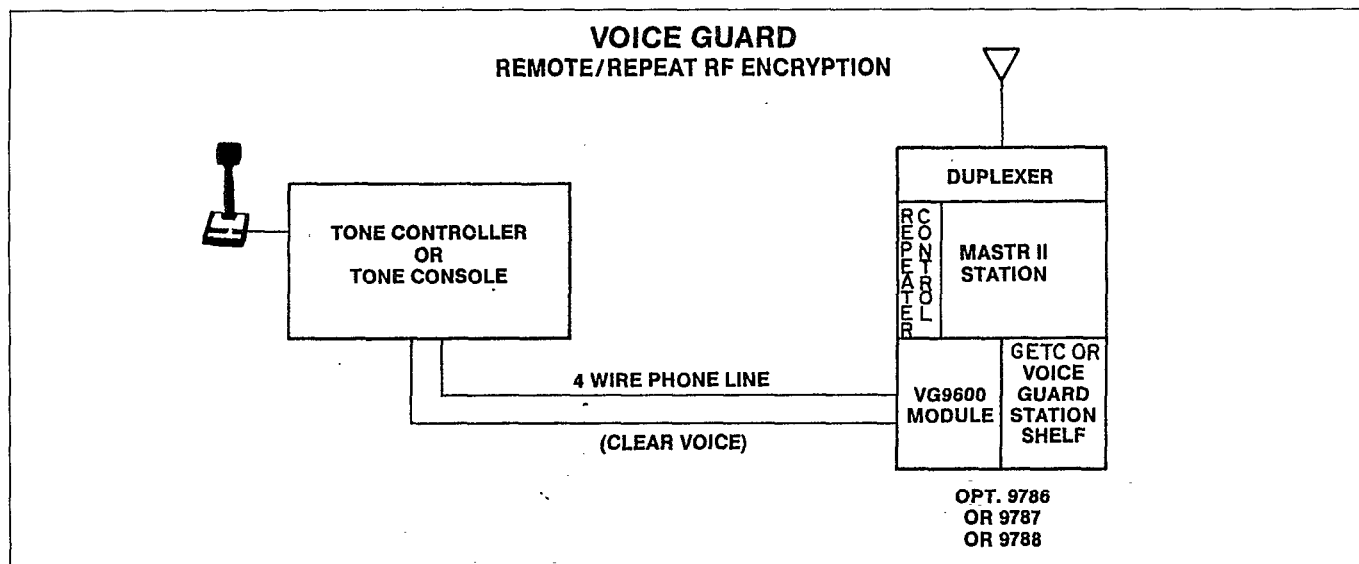


Figure 5-8. E/D Remote/Repeat Station Block Diagram

local cabinet service speaker and microphone, and by four-wire line facilities with one or more remote control consoles on a clear voice basis. To support VG Repeater operation, the station also has a GETC or Voice Guard Station Shelf that accepts Voice Guard data from the station receiver and, after validation, reconstructs the data and delivers it to the station transmitter.

In the Clear mode, the station operates in the normal manner. The E/D Remote/Repeat station is normally supplied only for single frequency operation. The OA for the Voice Guard unit, which services the Guarded mode remote function, and the OA for the station shelf, which services the repeat function, are selected independently and need not be the same. The table shown in the E/D REMOTE ONLY section above also shows the control tone assignments for E/D Remote/Repeat as well as E/D Remote Only applications.

The station shelf should be set for mode 2 (Repeater operation) instead of mode 3 (Remote/Repeat operation) because the Voice Guard module performs all of the remote control functions. Furthermore, when ever local or remote transmissions are being made, the station shelf is completely disabled. At the completion of such a transmission, if a signal to be repeated is present, the repeater path will immediately be established.

Figure 5-8 shows the simplified block diagram of an E/D Remote/Repeat station.

DECRYPT SATELLITE RECEIVER

The decrypt satellite receiver is a conventional satellite receiver with the addition of a Voice Guard unit. The unit and the optional keep-alive power supply are mounted on the same shelf as used in the E/D stations. The Voice Guard unit provides only the decrypt function. Since the PTT is never activated, the Voice Guard unit does not produce any operational alert tones.

If a Clear mode signal is received, the satellite receiver unsquelches, the 1950 Hz tone is removed and the audio is placed on the line to the voting selector. If Channel Guard is being employed and a wrong Channel Guard tone is received, the receiver will not unsquelch and the 1950 Hz tone remains on the line.

If a proper Guarded mode signal is received, the 1950 Hz tone is removed and decrypted audio is put on the line to the voting selector. If a Guarded signal with a wrong OA or non-matching cryptographic key is received, the receiver will not unsquelch and the 1950 Hz tone will remain on the line.

Since the Voice Guard unit requires about 0.5 amperes at 12 volts, it is recommended that the multireceiver power supply be employed, even for single decrypt receiver installations. The GE drawing numbers are:

19E501707G4 = 120/240 Vac 60 Hz operation

19E501707G5 = 120/240 Vac 50 Hz operation

E/D VOTED SYSTEMS

E/D systems require that VG-9600 Voice Guard units, complete with the operational cryptographic keys, be located at remote sites, thus potentially complicating the security aspects of a system. However, the decrypted audio from a Voice Guard unit will operate satisfactorily with the analog (clear voice) voter. Therefore, an E/D station with one or more decrypt satellite receivers in conjunction with an analog voter will satisfy the requirements for a Voice Guard voting system. This significantly simplifies the quantity of hardware, and line requirements associated with such a system.

It is recommended that E/D voting only be used with voted remote systems. It is further recommended that decrypted VG audio should never be re-encrypted.

Users will have to weigh their system security requirements against the voting circuit complexity and cost, in order to best satisfy their operational requirements.

E/D STATION MODIFICATIONS

The E/D (RF only) stations can be field modified to support Voice Guard operation. The mandatory electrical

modifications described in the MODS COMMON TO ALL STATIONS section above must be made for E/D station as well as end-to-end station configurations. Table 5-6 lists the available E/D station options. The FS-1027 endorsed stations would also require mechanical security modifications.

9783 - Remote only 1-freq w/VGE algorithm
9784 - Remote only 1-freq w/DES non-1027 endorsed
9785 - Remote only 1-freq w/1027 endorsement
9786 - Remote/repeat w/VGE algorithm
9787 - Remote/repeat w/DES non-1027 endorsed
9788 - Remote/repeat w/1027 endorsement
9789 - Remote only 2-freq w/VGE algorithm
9790 - Remote only 2-freq w/DES non-1027 endorsed
9797 - Remote only 2-freq w/1027 endorsement

Table 5-6. Available E/D Station Options

Table 5-7 describes the additional unique hardware required in E/D Voice Guard stations. The complement of standard cards employed in these stations is not shown. Table 5-8 lists the applicable assembly and modification instructions.

NAME	DWG #	9783	9784	9785	9786	9787	9788	9789	9790	9797
VG Station Shelf	19D438054G2					x	x	x		
or										
GETC	19D901868G3					x	x	x		
PROM	19A149219					x	x	x		
Harness	19C336748G1	x	x	x				x	x	x
Harness	19C336756G1				x	x	x			
Harness	19B234841G1	x	x	x	x	x	x	x	x	x
VG E/D shelf	19B234833G1	x	x	x	x	x	x	x	x	x
VG9600-SR	19A148909P13			x			x			x
VG9600-SRW	19A148909P14		x			x			x	
VGE9600-SRW	19A148909P23	x			x			x		
Keep-alive supply	19B234781G2		x	x		x	x		x	x
VG Control card	19D438133G1	x	x	x	x	x	x	x	x	x
Tx Control card	19D416660G7	x	x	x	x	x	x	x	x	x
Tx Control card	19D429082G1							x	x	x
Rx Control car	19D429100G1							x	x	x
Hdw kit	19A149124G1	x	x	x	x	x	x	x	x	x
Hdw kit	19A149098G2	x	x		x	x		x	x	
Hdw kit	19A149098G3			x			x			x
Harness kit	19C851484G3	x	x	x	x	x	x	x	x	x
AAA battery (2)	19B234891P1		x	x		x	x		x	x
Lock set	19B234880P1			x			x			x
Shelf	19C336763G1		x	x		x	x		x	x
Bracket	19C336762P1	x	x		x	x		x	x	
Capacitor	19A701534P7	x	x	x	x	x	x	x	x	x
Name plate	19A149096P1	x	x	x	x	x	x	x	x	x

Table 5-7. E/D Voice Guard Station - Unique Hardware Requirements

NAME	DRAWING #
Exciter	19C336664P1
Receiver	19C336664P3
10 V. regl.	19D438176P1
Repeater card	19C336774P1
Backplane	19D438189P1
Mod. instr.	19D438188P1
Mod. instr	19D438184P1
Harness	19C336664P4
Door lock	19A149204P1

Table 5-8. Assembly and Modification Instructions

MOBILES

DELTA S/SX

The DELTA S and SX are fully transistorized, synthesized radios with up to 32 channel capability. When made Voice Guard ready, an interface board (PL19D901775) is installed in the front option position. To make a DELTA radio Voice Guard operational, it is necessary to move several jumper plugs in the radio. Refer to the appropriate radio instruction book.

The interface board supports the Voice Guard TX/RX data switching and TX data filtering circuits. The TX data filtering is divided into two sections. The first section is located in the Voice Guard unit where the fast (TTL) data transitions are slowed down in order to minimize cross coupling of data into other wires in the radio control cable. The second section of data filtering is in the radio in order to filter out any high frequency noise that might be picked up on the radio control cable as well as complete the required filtering of the data.

When operated with an S990/S950 control unit, four different groups or channel select modes of 32 channels each, or eight modes or groups of 16 channels each can be stored in the control unit. These different groups can be down-loaded to the radio on command. The Voice Guard unit only looks at the five radio channel select leads, and has no way of recognizing the down-loaded group number. Therefore, for any specific channel number, the Voice Guard OA will always be the same, independent of the number of the down-loaded channel group. When operated with an S550 control unit, selection of only two blocks of 16 channels is available. This control unit has no down-loading capability.

PSLM (priority search lock monitor) operates in both the Guarded and Clear modes. It should be noted however, that when the radio is switched to the priority channel and a Guarded mode transmission is in progress, the Voice Guard unit will have to sync on late entry basis as the full preamble will have most probably been missed due to the PSLM switching. This means that the actual delivery of decrypted audio to the receiver (speaker) may be delayed by about half a second. The Voice Guard sync maintenance algorithm will maintain proper Guarded mode operation on a nonpriority channel during the periods that PSLM has switched the radio off channel.

The selection pattern for the five DELTA radio channel select leads (FB1 through FB5) is shown in Figure 5-9. A "1" denotes an open or high level on a line while a "0" denotes a grounded or low level on a line.

CHANNEL #	FB1	FB2	FB3	FB4	FB5
1	0	1	1	1	1
2	1	0	1	1	1
3	0	0	1	1	1
4	1	1	0	1	1
5	0	1	0	1	1
6	1	0	0	1	1
7	0	0	0	1	1
8	1	1	1	0	1
9	0	1	1	0	1
10	1	0	1	0	1
11	0	0	1	0	1
12	1	1	0	0	1
13	0	1	0	0	1
14	1	0	0	0	1
15	0	0	0	0	1
16	1	1	1	1	1
17	0	1	1	1	0
18	1	0	1	1	0
19	0	0	1	1	0
20	1	1	0	1	0
21	0	1	0	1	0
22	1	0	0	1	0
23	0	0	0	1	0
24	1	1	1	0	0
25	0	1	1	0	0
26	1	0	1	0	0
27	0	0	1	0	0
28	1	1	0	0	0
29	0	1	0	0	0
30	1	0	0	0	0
31	0	0	0	0	0
32	1	1	1	1	0

Figure 5-9. DELTA Radio Channel Selection Pattern

RANGR

The RANGR mobile radio can support Voice Guard operation in a manner similar to the DELTA S and SX radios. There are several significant differences which are listed below.

- Voice Guard interface circuitry is a standard part of the RANGR system board. To make Voice Guard operational, it is necessary to move several radio system board jumpers.
- RANGR is limited to 16 radio channels and 16 VG OA's.

- When used with an S990/S950 control unit, RANGR is download limited to four modes of 16 channels each.
- When used with an S550 control unit, RANGR is limited to one mode of 16 channels.

The selection pattern for the RANGR channel select leads (FB-1 through FB-4) is the same as shown in Figure 5-9 for the first 16 channels of DELTA with FB-5 being ignored.

DUAL CONTROL

It is permissible to use Voice Guard with an S550 control unit in a dual control configuration, so long as only one Voice Guard unit is utilized. The VG unit can be associated with either control unit or, it can be located between the junction box and the radio thus permitting Guarded mode operation from either control unit. NOTE: Two separate VG units associated, one each, with each control unit is not an available configuration.

PORTABLE

MPS

The MPS portable is a synthesized hand carried radio capable of supporting up to 64 individual transmit and receive channels. When equipped for Voice Guard operation, a 2 by 5 inch, multilayer printed circuit assembly is added to the radio. It is mounted in an extended back cover, which increases the overall thickness of the radio approximately 0.4 inches. The Voice Guard module is connected to the MPS radio by means of a flex circuit.

The Voice Guard equipped MPS can support one cryptographic key and channel selectable OA's. It is available with either the DES or VGE encryption algorithm. It is also available with a number of optional configurations however, because of the limitation on the number of control switch positions on the control cap of the radio, some combinations of functions are incompatible. Option configuration and incompatibilities are detailed in the MPS Product Index.

The MPS radio channel and VG personality information is programmable with a TQ-2310 programmer. Cryptographic key information is loaded with a 19A148910 key-loader.

M-PD

The M-PD portable is synthesized hand carried radio capable of supporting up to 64 individual transmit and receive channels. Voice Guard capability is included on the main system board of the M-PD. The Voice Guard equipped M-PD can support up to seven cryptographic keys and is available with either the DES or VGE encryption algorithm.

The M-PD Voice Guard personality PROM can be programmed to support the following list of VG functions on a per channel basis.

- Individual TX and RX OA's.
- Any one of seven cryptographic keys.
- Enable/disable VG operation.
- TX and RX data polarity.

The M-PD radio channel and personality information is programmable with an IBM PC or compatible having at least 512 kilobytes of RAM and running the M-PD VG programming software package TQ-3319. Cryptographic keys are loaded with a 19A148910 keyloader.

SYSTEM CHECKOUT

After a Voice Guard station has been installed, especially if added to an existing clear mode only system, it is essential that the outside addresses as discussed in the Chapter 3 and the data inversions as discussed in the Chapter 4 all be configured to properly satisfy the system requirements. This section addresses how to make simple measurements and observe the GETC or station shelf LEDs to assure that the station is set up correctly and will support proper system operation.

MOBILES AND PORTABLES

The first step in configuring an operational Voice Guard system is to assure that the mobiles and portables to be used in the system are programmed with the correct RF transmit and receive frequencies as well as proper VG outside address (OA) and data polarity on each channel to be used. Also verify that the mobiles and/or portables can communicate in both the clear and guarded modes on a simplex basis.

If the mobiles have been shipped from the factory with default programming, channels 1 through 16 should have both TX and RX OA's set for 55 (hex) and the data inversion matched to the band and split of radio to meet the data polarity standard described in the Chapter 4.

If the portables have been shipped from the factory with default programming, all channels should be programmed with both TX and RX OA's equal to 55 (hex) and the data inversion matched to the data polarity standard described in the Chapter 4.

Should there be any problem in setting up a VG system, the contents of the personality PROM of at least one of each configuration of equipment being employed (i.e., RANGR, MPS, M-PD, DELTA etc.) should be examined to insure that some other OA or data inversion information is not present.

VOICE GUARD STATION SHELF - Options 9780 & 9781

The GETC or Voice Guard station shelf as employed in Remote, Repeat, Remote/Repeat, Voted Remote Repeat, satellite receiver and voter receiver applications can be set for any one of 256 separate receive OA's. In those applications that also support non-voted repeating of a Voice Guard transmission, the OA as repeated can also be set for any of the available 256 OA's, independent of the received OA.

In the case of remote or voted-repeat applications, the Voice Guard station shelf passes the received OA on through and provides no means of modifying it. In voted applications, the Voter Selector does not look at the received OA at all, nor does it provide for any modification of the OA of the voted output.

All applications of the GETC or station shelf provide the capability for separately inverting or not inverting the data on the operational radio and/or telephone line paths.

Status Display

In order to minimize the potential confusion concerning the setting of the GETC or VG station shelf switches, a capability of displaying a summary of these switches (S1, S2 and S3) has been included in the shelf software.

A 2400 baud computer terminal configured for SIMON testing (see LBI-31593) connected to GETC of VG station shelf connector TB-8, will display a complete summary of the switch settings immediately after each power-up or

depression of the shelf reset button. Since the shelf switches are read by the software only at code initialization, it is necessary to push the shelf reset button after each switch change to get it read. This also results in the shelf displaying the switch summary again.

After getting the switch summary to agree with the system requirements, remove the display terminal cable from the shelf, reconnect the system cable if the shelf is a voter receiver or selector. Once again, depress the shelf reset button to assure that the shelf is operating properly.

Receiving Function

LED Observation

The LEDs on the front of the GETC or VG station shelf will indicate the status of a Voice Guard signal being processed. The "Digital SYNC" light or L7 will be lit whenever a proper addressed VG signal of proper data polarity is being received. The remaining LEDs L6 through L1 are associated with transmitting functions of the shelf and will not light if the shelf is in the satellite receiver mode or is in the remote station mode and the VG signal is arriving via the radio port.

When first checking out a GETC or VG station shelf operationally, a VG signal should be applied to the activated ports (port 0 = radio path and port 1 = telephone line path). If the OA and data polarity are correct, the digital "SYNC" or L7 LED will light. If this LED does not light during the test transmission but does light briefly for one or two seconds after the VG test transmission is ended, the data being received is inverted from what the shelf is expecting. S3-1 inverts the polarity of the radio port (0) data that the shelf expects while S3-3 inverts the polarity of the telephone line port (1) data expected. The switches in the ON position denotes noninversion of the data while OFF denotes data inversion. See Figure 5-10.

If the L7 LED does not light at all and data is being received, the most probable cause is that the switch S1 and the received OA do not agree or all-call is not enabled. The OA's should be set up correctly before the data inversion switches are changed.

Should it become desirable to verify that data is actually being received on either of the shelf ports, it is possible to check with an oscilloscope at pin 19 of the appropriate MODEM IC on the shelf for the presence of a logic level (5 volt) data signal when the test source is transmitting. In the case of the radio port (0), U-4 is the proper IC. In the case of the telephone line port (1), U-19 is the proper IC.

In either case, the proper VG signal at pin 19 of the MODEM IC should be pseudorandom logic level data with a 104 microsecond bit period. With no VG signal being received on the radio port (0), logic level data with random period may be seen. This is the limited noise from the receiver discriminator. With no VG signal being received on the telephone line port (1), no logic signal may be noted or, if a 1950 Hz idle tone is being employed, a repetitive waveform at a 1950 Hz rate may be seen.

Interrupt Line Observation

Once it has been established that proper data is being received, it is possible to verify that the data polarity is correct and the OA's match by observing the appropriate MODEM IC interrupt line (pin 24) with an oscilloscope. If a proper VG signal with matching OA is being received, there will be a continuous string of negative going, logic level pulses occurring at an 833 usec rate. These will stop immediately upon termination of the VG transmission. If the VG signal being received on the port being examined has the data polarity inverted, pin 24 will display short, intermittent bursts of pulses. Moreover, when the VG transmission is terminated, there will be a 1 to 2 second continuous burst of interrupt pulses.

If the data polarity is correct but the OA's do not match, there will be a nearly continuous string of 833 usec interrupt pulses. Some interruptions or gaps will be seen, and there will be no burst after the VG transmission is terminated as there was with inverted data.

With no VG signal being received, only random noise, short bursts of interrupts may be seen. These will appear about the same as when the data is inverted.

When a shelf port is performing both a transmit and a receive function, such as when configured as a repeater, the receiving of a proper VG signal will cause appropriate LEDs on the shelf to light (see the TRANSMITTING FUNCTION section below) and also cause a second set of interrupts to appear on pin 24 of the port modem chip. The second set of interrupts are associated with the port transmitting function and are normal. If the port is only receiving, as in a remote only configuration, only one set of interrupts will be seen on pin 24 of the port modem chip.

Transmitting Function

If the GETC or VG station shelf is set up to provide a transmitting function, and a valid VG signal is provided on an active port, two additional LED's should light on the front of the shelf. These will be for a radio port (0) signal and remote,

repeat or remote/repeat modes: "Repeat PTT" or L1 and "F1" or L6. For telephone line port (1) and remote or remote/repeat modes: "Remote PTT or L2" and "F1 or L6" through "F4 or L3" depending on which frequency might have been selected by the telephone line controller. While a CIU is supplied for only one or two frequency operation, the VG (digital) mode can support up to four frequency operation. This would require additional control lines between the CIU and the console(s), and also an alternate clear mode frequency selection system to support four frequency operation.

VOTING RECEIVER

The "PWR or L7" LED on the voter receiver shelf actually serves a shelf ready function. This LED may blink periodically when the shelf software is executing a reset, after which the LED L7 will again be lit. Whenever the voter receiver shelf is receiving a valid VG signal with proper OA and polarity, the "SYNC or L6" LED will be lit. This indicates that the voter receiver is receiving a valid VG signal and that the digital voter selector will be so informed when ever it polls that voter receiver.

The "SEL or L5" LED will be lit only on the shelf that the voter digital selector has selected. Only one voter receiver can be validly selected at a time however, the selection may change as often as every VG frame (4 times per second).

Shelf switch S1 sets up the required received OA for the VG signal being received from its companion satellite receiver. This OA must always be set to the same value as set into the companion satellite receiver. See Figure 5-10.

Shelf switch S2 assigns the shelf address number that will be used by the digital voter selector during polling. Only the first five switches S2-1 through S2-5 are used. The last three are ignored and are not displayed on the terminal. Shelf switch S3 sets the mode and transmit line data polarity. Unused switches are ignored. See Figure 5-10. The shelf MODEM IC interrupt line observation technique described in the INTERRUPT LINE OBSERVATION section above also applies to the Voter Receiver.

To put a voter receiver shelf into the switch display mode requires the removal of the cable connector that busses all of the voter receivers to the digital voter selector from J8 and connect the SIMON cable from the terminal to J8. Then push the shelf reset button. The "PWR or L7" LED is not lit in the display mode.

The SIMON cable connector (J8) has pins 3 and 5 (and 6) tied together. This grounds an input to the micropro-

cessor that causes the shelf to switch into the display mode upon depressing the shelf reset button. At the completion of the display operation, remove the SIMON cable and replace the system cable. It is then necessary to press the voter receiver shelf reset button to get the shelf out of the display mode and also depress the digital voter selector shelf reset button to get the selector to again log the voter receiver back "on line".

VOTING SELECTOR

The "PWR or L7" LED on the digital voter selector shelf serves as a shelf ready light in much the same manner as was described for the voter receiver. When the selector has selected a frame of VG data from a voter receiver and is transmitting it to the phone line port, the "SEND or L6" LED will be lit. When the selector is not sending VG data but, is only repetitively polling voter receivers looking for valid VG data to operate upon, the "SEND or L6" LED is not lit.

Switches S1 and S2 are not used by the digital voter selector hence, they are ignored by the selector shelf in both the operational and display modes. Switch S3 establishes the operating mode for the shelf along with providing for phone line data inversion. The remaining unused switch sections of S3 are ignored. See Figure 5-10.

To put a digital selector shelf into the display mode, it is necessary to remove the polling bus cable connector from J8 and connect, in its place, the display terminal. Then push the shelf reset button. The "PWR or L7" LED is not lit in the display mode.

SIMON cable connector pins 3 and 6 (and 5) are tied together. This grounds an input to the microprocessor which, upon depressing the shelf reset button, causes the shelf to go into the display mode. Upon completion of the display operation, remove the SIMON cable and reconnect the system bus cable connector. Push the selector shelf reset button in order to get the shelf out of the display mode.

TELEPHONE LINE SETUP

Data Polarity Consideration

When setting up a VG system, it is essential that the data polarity standard discussed in section four be adhered to faithfully. This is because the inverting of an NRZ data signal effectively results in the appearance of a totally different NRZ data signal. Such a data signal can be inverted by passing the signal through an odd number of inverting amplifiers or logic gates.

A point often missed is that passing an NRZ modulated radio signal through an RF mixer employing highside L.O. injection will produce NRZ data inversion, while the same mixer employing lowside L.O. injection will not produce NRZ data inversion.

The GETC or Voice Guard station shelf has provisions for inverting or not-inverting the received and transmitted radio path (shelf modem 0) data as required. It should be noted however, that the data polarity standard has much less significance when dealing with the 19A705178 telephone line modems. These modems are 16 level, 9600 baud devices. This means that the 9600 baud, 2 level data is converted to 4 level - 4 phase data that then modulates a 1700 Hz subcarrier. This results in a 9600 baud NRZ input data signal having a spectral occupancy of flat from DC to 4800 Hz being converted to a 2400 baud complex data waveform having a spectral occupancy from 500 to 2900 Hz.

The data information is now contained symmetrically about the 1700 Hz subcarrier tone frequency. Therefore, passing this signal through any number of inverting amplifiers or through any configuration of mixers will have no effect on the data polarity. Because of this, there is no absolute definition for data polarity for circuits carrying telephone line modem data.

The phone line modem transmit data polarity may be arbitrarily selected at the one end of a control circuit, then at the other end of the control circuit, the receive data polarity be selected to make the circuit work properly.

Level Setting Criteria

Confusion occurs over what is the correct modem signal level to drive into a telephone line. There is no one correct level. There is, however, a definable criteria that should always yield satisfactory modem performance when utilizing the Voice Guard data modems.

Data modem criteria:

- RMS Test Tone Level - This is the rms value of a sinusoidal tone (typically 1 kHz). The peak value reflects the maximum signal level that a telephone channel can reliably support without producing distortion or channel overload. This level can vary widely and is usually specified by the telephone company or multiplex equipment manufacturer.

- **Signal-To-Noise Ratio** - The required S/N for adequate data modem bit error rate performance is defined by the modem manufacturer as being 26 dB for 1 bit error in approximately 2 million data bits and 24 dB for 1 bit error in approximately 50,000 bits. This is measured as the ratio of the rms magnitude of the modem signal to the rms noise at the receive end of the telephone circuit. The frequency band for this parameter is 300 to 3000 Hz.

There are two constraints that need to be applied when establishing the modem signal level to apply to any specific telephone line or its equivalent. These are:

- The ideal rms modem signal level into the telephone circuit should be 10 dB below the rms test tone level. Under no circumstance should it ever be greater than 6 dB below the rms test tone level.
- The rms modem signal level into the telephone circuit should be sufficient to produce at least a 24 dB signal-to-noise ratio at the receiver end as described above.

With a good data grade telephone circuit, it will be possible to meet both of the above criteria with a margin window of as much as 10 dB. If this is the case, choose a level about mid-way in the window. If two above criteria can not be met simultaneously, the telephone circuit is unacceptable and should be "fixed".

The receive level into the Voice Guard data modem can be monitored with an oscilloscope on the GETC or VG Station Shelf at the arm of potentiometer R1. The desired input level should be between 250 and 400 mV peak-to-peak, though adequate performance can be obtained with a receive signal level of as low as 25 mV P-P.

INTELLIGIBILITY - GENERAL

The present state-of-the-art method of digitizing a voice signal and passing it thru a 25 kHz mobile radio channel

does not permit this to be accomplished distortion free. Different digitizing schemes will degrade the voice quality in different ways. The design objective of any mobile radio voice privacy system is to maintain maximum voice intelligibility within the allocated transmission bandwidth.

In a continuing effort to improve voice intelligibility, both the VG-9600 and the M-PD circuitry has been modified. The frequency response of the CODEC transmit filtering in both the VG-9600's and M-PD portables has been changed. Also, in the M-PD units, the receive filtering has been changed.

VG-9600 units

All Revision "H" and later VG-9600's contain the revised filtering. The changes to earlier units can be made in the field. See appropriate Technical Services Bulletin for details.

When the VG-9600 is employed in a mobile application, it is essential that the mobile microphone be type 19B801499P1 for best voice intelligibility.

M-PD portables

A new M-PD VG printed wire board layout has been established to support the new filtering. A field modification kit is available for existing M-PD portables.

Console Applications

In some consoles, the received VG audio may sound somewhat muffled. In console applications, the received audio from a VG-9600 is passed on flat (not pre-emphasized). Where a problem of muffled console received VG audio appears to exist, the received audio can be pre-emphasized by moving jumper P10 to position 2-3 on the VG-9600 analog board. Also, jumper P19 position 1-2 provides a 6 dB/oct pre-emphasis while position 2-3 provides a 12 dB/oct pre-emphasis of the received VG audio. Select P19's position for best audio quality as judged by the user(s).

SWITCH #		1	2	3	4	5	6	7	8
STATION OPTION 9780	S1	Rx OA	Rx OA	Rx OA	Rx OA	Rx OA	Rx OA	Rx OA	Rx OA
	S2	Tx OA LSB	Tx OA	Tx OA	Tx OA	Tx OA	Tx OA	Tx OA	Tx OA MSB
	S3	MODEM 0 Rx POL.	MODEM 0 Tx POL.	MODEM 1 Rx POL.	MODEM 1 Tx POL.	ALL CALL ENABLE	MODE SEL LSB	MODE SEL	MODE SEL MSB
STATION OPTION 9781	S1	Rx OA LSB	Rx OA	Rx OA	Rx OA	Rx OA	Rx OA	Rx OA	Rx OA MSB
	S2	Tx OA LSB	Tx OA	Tx OA	Tx OA	Tx OA	Tx OA	Tx OA	Tx OA MSB
	S3	MODEM 0 Rx POL.	MODEM 0 Tx POL.	NOT USED	NOT USED	ALL CALL ENABLE	MODE SEL LSB	MODE SEL MSB	MODE SEL
VOTER RECEIVER	S1	Rx OA LSB	Rx OA	Rx OA	Rx OA	Rx OA	Rx OA	Rx OA	Rx OA MSB
	S2	SEL ADDR LSB	SEL ADDR BIT 1	SEL ADDR BIT 2	SEL ADDR BIT 3	SEL ADDR MSB	NOT USED	NOT USED	NOT USED
	S3	NOT USED	NOT USED	MODEM 1 Rx POL.	NOT USED	ALL CALL ENABLE	MODE SEL LSB	MODE SEL	MODE SEL MSB
VOTER SELECTOR	S1	NOT USED	NOT USED	NOT USED	NOT USED	NOT USED	NOT USED	NOT USED	NOT USED
	S2	NOT USED	NOT USED	NOT USED	NOT USED	NOT USED	NOT USED	NOT USED	NOT USED
	S3	NOT USED	NOT USED	NOT USED	MODEM 1 Tx POL.	NOT USED	MODE SEL LSB	MODE SEL	MODE SEL MSB

SHELF SWITCH ASSIGNMENT
FIGURE 5-10

(This Page Intentionally Left Blank)

CHAPTER 6

VG VOTING SYSTEMS

VOICE GUARD VOTING

INTRODUCTION

In many systems, particularly where low power portable radios are employed, talk-out coverage range is found to be significantly greater than the talk-in range. To alleviate this operational system problem, receivers are frequently geographically dispersed over the required coverage area so that at least one receiver can always receive signals from the low power radios wishing to talk-in. These several receivers are connected to a central point by microwave or radio paths or by telephone lines where they are all automatically compared and the best quality received signal is forwarded on to a dispatcher and/or repeater. The other unused received signals are ignored. Comparison of the received signals is usually performed dynamically so as to always be forwarding the best signal. The practice of continuously comparing and selecting one received path from an available field of several is generally called "VOTING" though it is sometimes referred to as "SWITCH DIVERSITY COMBINING".

ANALOG VOTING METHODOLOGY

In analog voice voting systems, the criterion for selection is typically based upon received signal-to-noise ratio. A channel IDLE tone (1950 Hz) is usually sent from each satellite receiver to the voter to indicate that the receiver is squelched. Channel activity detectors are also employed to provide recognition of speech as opposed to an unsquelched receiver that is only sending noise to the voter. Therefore, most analog voters will only work on a system that is handling unencrypted, analog voice. LBI-30002 contains a detailed description of the General Electric analog voter.

DIGITAL VOTING

In systems equipped with analog voting where digitized voice or other continuous, pseudorandom data is to be handled, additional problems arise. One of these problems is that if a data signal opens the squelch of a satellite receiver, the analog voter channel activity detector will interpret this as an unsquelched receiver with no modulation and will shut down the channel as having failed. Another is that no convenient frequency domain technique is available with which to establish the received data signal-to-noise ratio at the voter selector, thus there is no voting criterion on which to make an analog based selection.

In order to accomplish voting of a pseudorandom data signal, a new decision criterion is required. This can be based on looking at the analog characteristics of the received data such as amplitude distortion, crossover distortion or phase jitter, or based on information accuracy such as, bit error rate or word error rate. However, error rate measurement criteria are complicated if data scrambling is being employed.

VOICE GUARD VOTING METHODOLOGY

In Voice Guard end-to-end encryption systems with voting, the digital voting criterion is that the bit-error-rate (BER) of the unencrypted header portion of each VG data frame is calculated for each satellite receiver data path and the best BER path is selected on a frame-by-frame basis. Each VG data frame consists of 2152 bits of which the first 112 bits are unencrypted (see ref. Design and Performance of a Digital Voice System for Land Mobile Radio, G.D. Rose and S. Kappagantula contained in appendix of this manual).

VOICE GUARD SYSTEM HARDWARE

SATELLITE RECEIVER

Description

The high band or UHF satellite (auxiliary) receiver, option 9723, required for Voice Guard voting applications is a standard MASTR II auxiliary receiver, with the IFAS board modified in the same manner as for MASTR II station receiver applications, and a GETC or Voice Guard station shelf. A summary of these modifications are:

- Change C622 on the 19D432667G1 IFAS board from 0.47 uf to 10 uf. This is done to improve the receiver low frequency response in order to support VG data.
- Realign the receiver IF stages to provide the best possible data eye pattern at V/S high. This is done to give the best possible low signal level data performance.

In addition, the RUS run on the satellite receiver system board is cut and both leads brought out so that the VG station shelf can independently control the 1950 Hz busy tone generator and audio feed to the telephone line. LBI-31679 contains detailed information on end-to-end satellite (auxiliary) receivers.

The GETC or VG station shelf is the same as used in end-to-end station applications. The software required to support satellite receiver operation is resident in the PROM and is the same as used in the GETC and VG station shelves. The satellite receiver mode of operation is selected by setting the shelf DIP switch S3, sections 6, 7 and 8 to "1-0-1". See Figure 6-1 for a summary and LBI-31546 for a detailed discussion of shelf DIP switch settings.

Voice Guard digital voter hardware is connected in parallel with the GE-VSD analog voter hardware. The two share common, data grade, telephone lines and operate in parallel. When a valid VG signal is detected by the GETC or VG shelf, the analog voter is disabled and the voting is handled digitally; otherwise, the incoming signal is handled by the analog voter.

If a particular satellite receiver is located very near the voter, it is not necessary to use the telephone line modems. The interconnection between the satellite receiver and the digital voter can be by RS-232 link. It should be noted that this method of interconnection requires separate wire lines for the clear and data signals. See LBI-31679 for details.

Operation

The receiver recovers all on-channel RF signals of adequate strength. If a clear mode (unencrypted) signal with a correct Channel Guard (CG) tone is received, the 1950 Hz receiver idle tone will be removed from the telephone line and the audio (modulation) being recovered will be sent down in its place.

If a VG data signal containing the proper outside address (OA) is received, the GETC or VG shelf will recognize the data, reconstruct the digital data preamble and send the data to a telephone line modem where the 9600 baud NRZ data is converted to a 2400 baud, 16-level signal that is put on the same telephone line used for analog audio. The telephone line must be capable of supporting data signals. (See the Chapter 4 of this manual).

DIGITAL VOTER

Description

In a single channel VG voting system, one voter receiver shelf is required for each satellite receiver. One voter selector is connected to up to 32, co-located, voter receivers. Normally, the VG voting selector combination is shipped in either a 30-inch or 44-inch station cabinet, depending upon the

number of voter receiver shelves required. The 30-inch cabinet can house up to six voter receivers, a voter selector and power supply, while a 44-inch cabinet can house up to 12 voter receivers, a voter selector and power supply. The voter receiver hardware is very similar to the GETC or VG station shelf used with satellite receivers except that the PROM (19A149334) contains entirely different software. The voter selector shelf contains the same PROM code as the voter receivers but, has an additional hardware modification that adds a 1950 Hz oscillator to the hardware complement. See LBI-31680 for detailed information on the VG voter.

Operation

Each VG voter receiver, upon receiving a valid VG data signal from its corresponding satellite receiver, calculates the average bit error rate (BER) of the unencrypted data frame header. This BER is based on the known properties of the first 112 bits of each frame. There are ten categories of goodness of BER and each voter receiver determines the category of each valid frame header and makes this information available to the voter selector upon command.

All of the voter receivers and the voter selector are connected to a common asynchronous serial data bus. Each voter receiver has a shelf polling address between 0 and 31 assigned to it. This address is established by the setting of DIP switch S2, sections 1-5, on each voter receiver shelf. See Figure 5-10. No two shelves may have the same address. The VG voter selector polls each voter receiver shelf sequentially to determine if a) it has received a valid VG signal and if so, b) what is the BER category of that signal. The voter selector then determines which receiver will supply one frame (approximately 224 msec) of VG data. Should more than one voter receiver report that the BER was in the best available category, the voter selector will then select the voter receiver with the lowest (magnitude) polling address. By judicious assignment of polling addresses, the digital voting system can be weighted to provide selection preference to any given site.

The selected frame of data is then transferred to a buffer in the voter selector over the common bus at 19.2 kbaud where it is then clocked out at 9.6 kbaud. Before one frame has been completely clocked out of the buffer, the selector will have again polled all active voter receiver shelves and selected the one to transfer the next frame of data. This results in a smooth, continuous, 9.6 kbaud data train being forwarded from the selector, where each successive frame has been independently chosen from one of the available VG voting receivers.

If a VG voting receiver should fail at any time, the voting selector will take note on the next round of polling and it will remove the failed receiver from the polling list of available receivers. Upon being placed back in service, the voting receiver can be logged in by the selector as being available by depressing the reset button on the selector shelf. This causes the selector to reconfigure and recognize all available polling addresses.

INTERFACE ADAPTER

There is the need for several components to be added to the voter system when Voice Guard voting is overlaid on an GE-VSD analog voter. Since no place readily existed for these components, a new assembly was made to support them. This is called the Interface Adapter and is identified by PL19C336844G1. Only one Interface Adapter is required for 2 through 32 VG sites. See LBI-31680 for detailed information on the Interface Adapter.

The following functions are performed by the Interface Adapter.

- R3, D2 and C1 form a low current, shunt regulated 4.4 V power supply which provides the required pull-up voltage for several logic functions.
- R2 is the pull-up resistor for the voter PRE-DETECT bus.
- R1 is the pull-up resistor for the RKP INHIBIT line.
- D1 is an isolation diode for the analog voter MUTE line. It is essential that this diode be a low forward voltage drop type (i.e., Schottky barrier) as the MUTE line directly accesses the emitter-base junction of a transistor and the muting function must pull close enough to ground to prevent the transistor junction from conducting.
- K1 provides the very low forward voltage drop required by the digital voter COS input and the RKP RCVNG input.

VOTING STATION - DESCRIPTION

The PROM (19A149219) in the GETC or VG station shelf contains all of the required software modules to operate in any of several station modes. These are all discussed in LBI-31546 and in the VOICE GUARD STATION SHELVES section of Chapter 5 in this manual. When operating in the voted remote/repeat mode, the shelf operates in a nearly full duplex manner. The received VG data via the radio path is passed out the station control line transmit port to the VG voter, while the station control line receive port accepts voted VG data from the voter selector output and passes it on to the radio RF transmit port.

When a voter is being incorporated in a VG system, the GETC or VG shelf in the station should be set for the voted remote/repeat mode independent of whether the station is operating in the voted remote, voted repeat or voted remote/repeat application. See LBI-31546 and the VOICE GUARD STATION SHELVES section of Chapter 5 in this manual, for a detailed description of station shelf modes.

CONSOLE INTERFACE UNIT

Description

The Console Interface Unit (CIU) is required in end-to-end encryption systems to provide interconnection between 1 or more dispatch consoles and the station RF equipment. The CIU is comprised of the following hardware pieces:

- Control shelf consisting of:
 - Four Freq Tone Remote Control board 19A704686P6
 - Interface board 19D438302G1
 - Telephone line modem 19A705178P1
- Voice Guard shelf consisting of:
 - Voice Guard unit 19D438909P14,16,23
 - Power supply 19A149246P1
 - Keep alive supply (optional) 19B234781G2

The CIU is housed in a 30" indoor cabinet. One CIU must be employed for each radio channel in the system. One to four CIUs can be mounted in one cabinet. CIU versions to support either VGE or DES encryption algorithms are available. Also, DES, FS-1027 endorsed and non-endorsed versions are available.

Operation

At the beginning of a console initiated transmission, the AC tone control signaling format calls for a nominal 125 msec burst of high level 2175 Hz tone (called SECURIT tone) followed by a nominal 40 msec burst of function tone. Then a low level 2175 Hz continuous tone keeps the transmitter keyed on the air. One of four standard function tones determines the transmit frequency (channel) and the logical OR of the function tone detectors in the station generates "remote PTT".

The CIU houses the Voice Guard unit which, in turn, contains the operational cryptographic key. When a transmission is to be made in the CLEAR mode, the control tones from the console(s) are passed through the CIU and on to the station. When a transmission from the console(s) is to be encrypted, a different function tone is sent that is intercepted by the CIU which, in turn, interrupts the clear audio path to the station. The clear audio is redirected to the VG module while the VG module output is connected to a telephone line modem which then places its 16-level 2400 baud data on the control line to the station. The audio being sent to the CIU from one console is also looped to the other control line pair so that all other console operators may hear both ends of each conversation. The function tones and their assignment in a VG system are shown below:

- 1950 Hz	- F1 Clear mode
- 1850 Hz	- F1 Guarded mode
- 1350 Hz	- F2 Clear mode
- 1250 Hz	- F2 Guarded mode

When a Guarded mode transmission is being received from the station (toward the console(s)), the VG unit in the CIU recognizes the valid VG data and responds causing the receive audio path to the console(s) to be fed decrypted audio. In the case of a clear transmission, the station audio is passed through the CIU and on to the console(s).

An additional looping capability exists in the CIU when operating in a voted system. The information on the control line from the voter can be looped to the control line to the station to complete the voted repeat path.

Instruction books LBI-31760 and LBI-31761 will provide additional detailed information on the CIU.

REMOTE KEYING PANEL (RKP)

Function

A Remote Keying Panel (RKP) provides a means for a voter to initiate a station AC tone transmitter keying sequence for clear mode Repeat or Remote/Repeat transmissions. It is not required for Remote only operation. When applied to a Voice Guard voter, the RKP must be modified. These modifications are discussed in detail in LBI-31680 and are summarized below. The basic RKP is described in detail in LBI-4650.

When the voter is co-located with the station, it is possible to interconnect the voter directly to the station, not requiring an RKP or telephone line modems. Such interconnection involves a number of separate leads.

Modification Summary

For Repeat and Remote/Repeat Voice Guard voter applications, the RKP must be modified as follows.

a) Keying Logic card - 19D417452G2

Change R212 from 100 ohms to 2700 ohms.

This slows the turn-on charging of the (5 second) transmit hang timer by approximately 100 msec so that there is time to decide whether the transmission is Guarded and, if it is, have time to keep the transmitter from keying on in the clear mode. This is because the transmitter keys ON several hundred msec later if the transmission is digital. Turning the timer ON too soon will allow a digital data "burp" to occur at the start of each repeated, Guarded transmission.

b). Tone Control card - 19D417417G1

Unsolder U8-8 from the PWB and insert a hot-carrier diode between U8-8 and the PWB, with the cathode end soldered to the IC. Also add a 10k ohm resistor from TP-10 to the +5 volt bus on the card.

The tone mute bus was originally intended to be pulled low by only IC U8. In the VG voting application, it is necessary to be able to pull the tone mute bus low by either U8 or externally. Since U8 has a TTL active pull-up output device, it was not possible to just externally pull the output low without drawing excess current in IC U8. The diode in series with U8 output now allows the bus to be wire-ORed. The 10k ohm resistor is a pull-up to +5 volts on the now diode isolated bus.

c). RKP backplane

The backplane run labeled + CONTROL is cut free from terminal TB2501-6. A wire is added from TB2501-6 to J2504-C14. Add jumper between backplane H1 and H2.

The + CONTROL function is only used in DC control functions. Since an external termination was required for the tone mute bus described above, + CONTROL was selected. J2504-C14 is the card access to the bus.

The jumper between backplane H1 and H2 connects the PTT LED on the shelf power supply to the PTT input terminal on the backplane. This allows the LED to light when the PTT output is activated by the COS input to the RKP.

Operation

CLEAR - When a clear mode signal is being received, the analog voter causes the "RECEIVING" input (TB2502-5) on the RKP to go low (active). This activates the 5 second hang timer and then starts the limit timer on the keying logic card. This, in turn, activates the PTT output on the RKP terminal TB2502-9 and also lights the LED on the RKP shelf power supply. The external PTT signal is connected to the tone voter board on the digital voter selector and is used to remove the 1950 Hz idle tone from the phone line. Internally, the transmit tone control sequence is generated and appears on the phone line. After the tone control sequence is complete, the clear voted audio from the analog voter is applied to the phone line.

GUARDED - When a Voice Guard signal is being received, the RKP starts to key up just as in the clear mode but is subsequently inhibited by the "INHIBIT" input to RKP terminal TB2501-6. The digital signal as processed by the telephone line modem is applied to the phone line for delivery to the CIU and/or repeater station.

It is essential that the analog PTT line from the RKP not be allowed to "glitch" during the beginning of a digital sequence. This will cause the 1950 Hz tone on the phone line to be turned off too soon and a burst of digital noise will be propagated through the system. See OPERATION in the CONSOLE INTERFACE UNIT section of this manual.

SYSTEM CONFIGURATIONS

While there are a number of ways to configure a voting system, the basic building blocks are all the same. It is possible to configure only analog voting or only Voice Guard voting or overlay both voters on the same control lines. One or more console positions and a CIU may be employed in voted remote or voted remote/repeat systems or no consoles or CIU need to be employed in voted repeat only systems.

On a standard catalog basis, up to twelve (12) analog voter sites may be utilized. More than twelve site analog voting is attainable on a "specials" basis. Up to 32 Voice Guard voter sites may be utilized before special hardware and software modifications become necessary. Figure 6-1 depicts the block diagram of a typical four site, single frequency, VG/analog voted remote/repeat system with two consoles. To add voting sites, up to twelve, only additional VG satellite receivers and analog and Voice Guard voter receivers attached to the voting busses would be required.

When adding Voice Guard voting to the existing GE-VSD analog voter, it was most desirable that no modifications be required to the analog voter hardware. In order to make this happen, the few additional required components needed to overlay the two systems were placed on a small PWB that was then mounted on the back of the voter cabinet. This board assembly was called the Interface Adapter and is identified as PL19C336844G1. Details of this assembly are discussed in LBI-31680.

VOTED REMOTE

The interconnect diagram of a two site VG voted remote system is shown in Figure 6-2. It contains: an analog voter, a Voice Guard voter, an Interface Adapter, a MASTR II remote base station, a CIU and a console. To add voting sites, additional VG voter receiver shelves would be interconnected in the same manner as the two shown in Figure 6-2. LBI-30002 covers the details of adding analog voter sites to an existing system.

Analog Operation

Normally, all satellite receivers are applying a 1950 Hz tone to their phone lines to indicate that no RF signal is

being received. The VG voter selector is also generating a 1950 Hz tone which mutes the audio output of the CIU. When a unit on the RF channel transmits a clear mode signal, the 1950 Hz tone is removed from the output of each satellite receiver receiving the signal. All satellite receiver audio outputs are brought by telephone line, radio or microwave link to a central point where the analog voter selects the receiver audio having the best signal-to-noise ratio.

The analog voter "RCVNG" lead, TB7-6, goes high when a clear signal is being received. This causes the reed relay on the interface unit in the voter cabinet to operate which, in turn, grounds the wired-OR COS line, TB10-8, and the tone disable line, TB10-1, in the VG voter selector shelf. This advises the VG selector that a clear mode transmission is in progress and removes the 1950 Hz tone from the voter output line. The RKP inhibit line, TB10-9, from the VG voter selector remains high and the analog voter mute line, TB7-8, remains above +0.65 volts. The selected analog path is indicated by the green lamp on the corresponding analog voter card being lit.

At the completion of an analog transmission, 1950 Hz is reapplied to the inputs of all of the analog voter receiver modules by their corresponding satellite receivers. Also, the VG voter selector, upon detecting that the COS line has again gone high, reapplies 1950 Hz tone to the voter output control line. This mutes the audio output from the CIU.

VOICE GUARD OPERATION

When a unit on the RF channel transmits in the Voice Guard mode and is received by one or more of the satellite receivers, the 1950 Hz tone is again removed from the output of each active satellite receiver. However, the VG shelf at each active satellite receiver determines that a valid VG signal is being received and proceeds to put 16-level data modem output on the telephone line. Immediately upon detecting that the 1950 Hz tone is missing on any of its inputs, the analog voter starts to process the VG data as an analog signal. The corresponding Voice Guard voter receiver detects the presence of valid VG data. This causes the VG voter selector RKP INHIBIT lead, TB10-9, to go low. This, in turn, pulls the analog voter MUTE line, TB7-8, down to less than +0.50 volts which causes the analog voter output to be muted. The 1950 Hz tone from the VG voter selector is again removed and VG data modem signal is applied to the voter output telephone line. The CIU output is unmuted, and the VG data is decrypted in its VG unit.

It should be noted that the analog voter MUTE line directly accesses the emitter-base junction of a transistor. When this transistor is turned ON, the measured voltage drop

will be the classic 0.6 to 0.7 volts. To keep the transistor from turning ON, it is necessary to clamp the MUTE line to less than 0.5 volts. See LBI-31680 for additional information on the Interface Adapter.

It should also be noted that about 30 seconds into every Voice Guard transmission, each analog voter receiver module that is receiving a VG modem data input will normally indicate failure and its respective RED lamp will light. This is normal because the VG data signal looks like an unsquelched radio receiver to the analog voter hence it indicates failure. This is not a problem because the analog voter output is muted during a VG transmission anyway. As soon as the VG transmission ends, the failed indication immediately clears itself and the analog voter is ready to process an analog transmission.

VOTED REMOTE/REPEAT

A voted remote/repeat system as depicted in Figures 6-1 and 6-3 are similar to a voted remote system as described in the VOTED REMOTE section of this manual except that the voted signal modulates the base station transmitter as well as being delivered to the CIU. Logic is included in the CIU that allows a console originated signal to preempt a mobile originated transmission. In addition to the complement of equipment required for voted remote operation, a voted remote/repeat system also generally requires a remote keying panel or RKP. The RKP accepts voted audio and a control signal from the voter and generates the transmitter tone keying sequence and places it on the telephone line to the CIU. In the voted remote/repeat mode, the CIU is strapped so as to loop the voted audio, either VG data or clear voice, onto the transmit control line from the CIU to the base station transmitter.

The RKP RECEIVING input (TB2502-5) and the INHIBIT input (TB2502-6) are low impedance circuits that are not readily driven from transistors. Therefore, the analog voter COR board (19B219964G1) is used to provide the switching interface to the RKP. The COR is not required for the voted remote only configuration.

A point of further note for voted remote repeat systems is that the RKP will send a burst of SECURIT tone to the console(s) at the beginning of each activation of the RKP. To prevent this burst of 2175 Hz tone from being heard, each console must be equipped with a 2175 Hz suckout filter. Such filters are generally available.

Analog Operation

When a unit on the RF channel transmits a clear mode signal, each satellite receiver receiving the signal will remove the 1950 Hz tone from its output. One or more analog voter receiver units detecting the loss of 1950 Hz tone input will result in the analog voter output "RCVNG" (TB7-6) lead going high. This causes the reed relay on the Interface Adapter to operate which, in turn, makes the COS input to the VG voter selector go low.

The COR relay (19B219964G1) on the analog voter is held in the normally operated state during periods of no activity or during clear mode operation. Therefore, the analog voter "RCVNG" signal also is delivered to the RKP (TB2502-5). When the "RCVNG" signal goes high, the 5 second hang timer and transmit limit timer are set and the transmit tone sequence is started. The RKP PTT output also goes low. This is connected to VG voter selector TB10-1 and performs the function of removing the 1950 Hz tone from the output of the voter, which then allows the CIU to unmute and pass clear audio to the console(s). Refer to LBI-4650 for detailed operation of the RKP.

Voice Guard Operation

When a unit on the RF channel transmits in the Voice Guard mode and is received by one or more satellite receivers, the 1950 Hz tone is removed from the output of each active satellite receiver. However, the GETC or VG shelf at each active satellite receiver determines that a valid VG signal is being received and proceeds to put 16-level data modem output on the telephone line to the voter. Immediately upon detecting that the 1950 Hz tone is missing on any of its inputs, the analog voter starts to process the VG data as an analog signal. The corresponding Voice Guard voter receiver detects the presence of valid VG data. This causes the RKP INHIBIT output (TB10-9) of the VG voter selector shelf to go low (ground). The RKP INHIBIT lead going low causes the analog voter MUTE line (TB7-8) to drop below +0.5 volts which mutes the analog voter and lets the COR on the analog voter release. This removes the RKP keying signal and also pulls the RKP INHIBIT input to ground which serve to halt the transmitter tone keying sequence and to reset the timers inside the RKP.

The 1950 Hz tone on the output of the voter selector is again removed and the voted VG data from the 16-level data modem is connected to the voter output telephone line and on to the CIU. The CIU output is unmuted, and the VG data is decrypted in its VG unit. The VG telephone line modem data is also looped to the telephone pair going to the transmitter

where it processed by the GETC or VG shelf in the station and then modulates the station transmitter.

The characteristics of the analog voter MUTE line and analog voter receiver fault indication during VG transmissions as discussed in the VOICE GUARD OPERATION section above apply to voted remote/repeat applications as well.

VOTED REPEAT

A voted repeat system is one in which no consoles or CIU are employed but, the voted signal is used to key ON and modulate a base station transmitter. Such a system configuration is depicted in Figure 6-4. It functions identically to a voted remote/repeat configuration except that the control circuit from the voter output is connected directly to the repeater transmitter input instead of to a CIU. The base station used in a voted repeat application must be configured identical to the base station used for voted remote/repeat systems. That is because the control input to either configuration is by wire line and appears the same to the station independent of whether it originated from a CIU or voter.

UNIQUE CHARACTERISTICS

Voted systems have certain unique limitations that are not shared with the non-voted counterpart system configurations. Two significant such limitations are described below:

a) In voted repeat and remote/repeat configurations the station VG shelf cannot change the transmitted OA relative to the OA that is received. This is because the VG station shelf software only reads the TX OA switch S2 when the VG signal comes in via the radio port. In voted applications, the voted signal to be transmitted enters the shelf via the control line port, not the radio port. The software is structured to not change the OA and to not read switch S2, if the signal enters via the telephone line port. While the voted remote/repeat shelf software allows the station receiver to receive a VG signal, it treats it as a satellite receiver and sends the received VG data to a voter receiver input.

b) In voted operation, the CG MONITOR function does not open up the channel so that it can operate in a no CG mode. Also, the receive OA is not opened up to pass all OA's, independent of S1. This is because the station CG MONITOR function is not normally conveyed to the satellite receiver locations. Hence, even though the station CG MONITOR function may actually be enabled, the satellite receivers don't know about it and remained squelched.

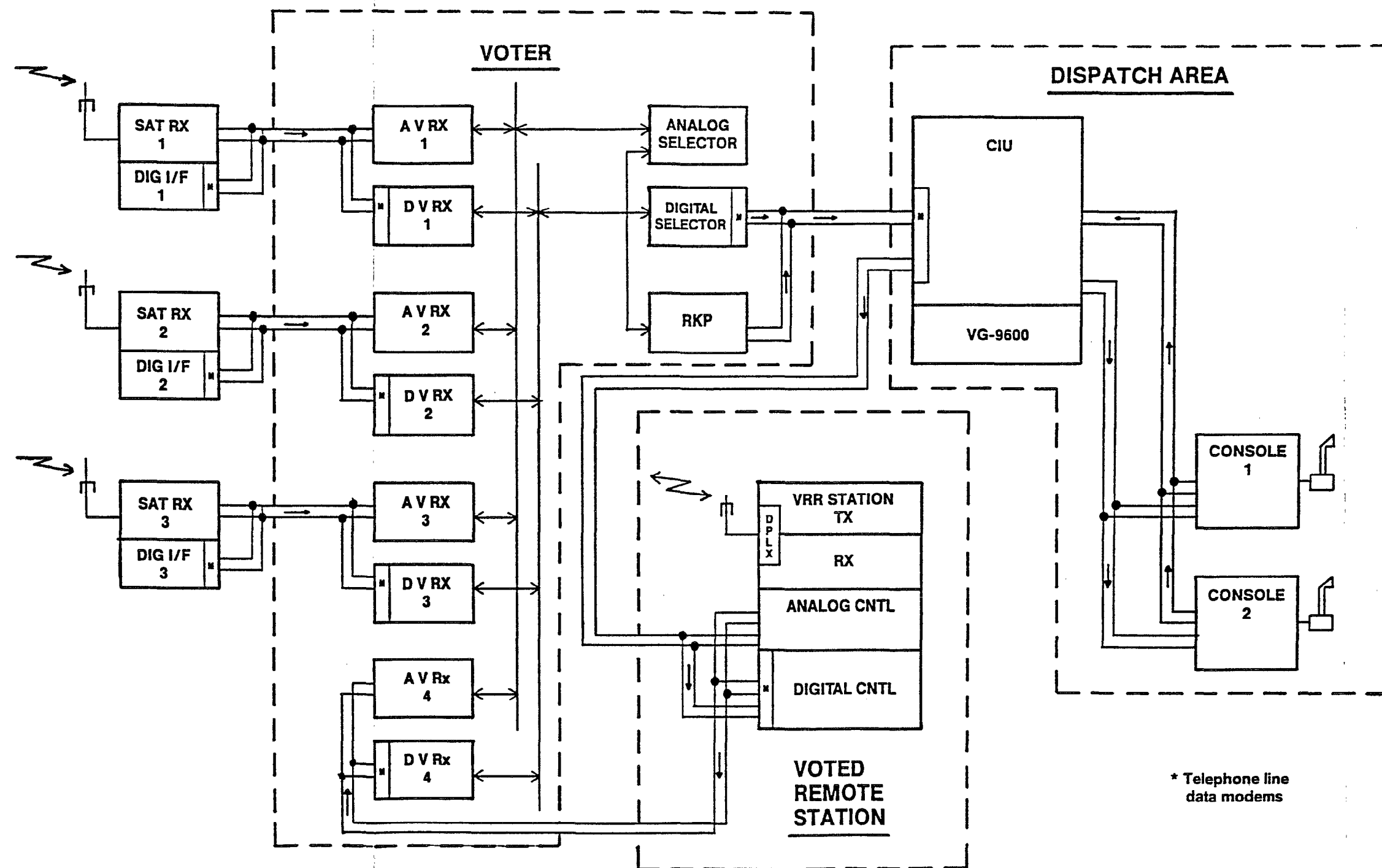


Figure 6-1. Voted Remote/Repeat



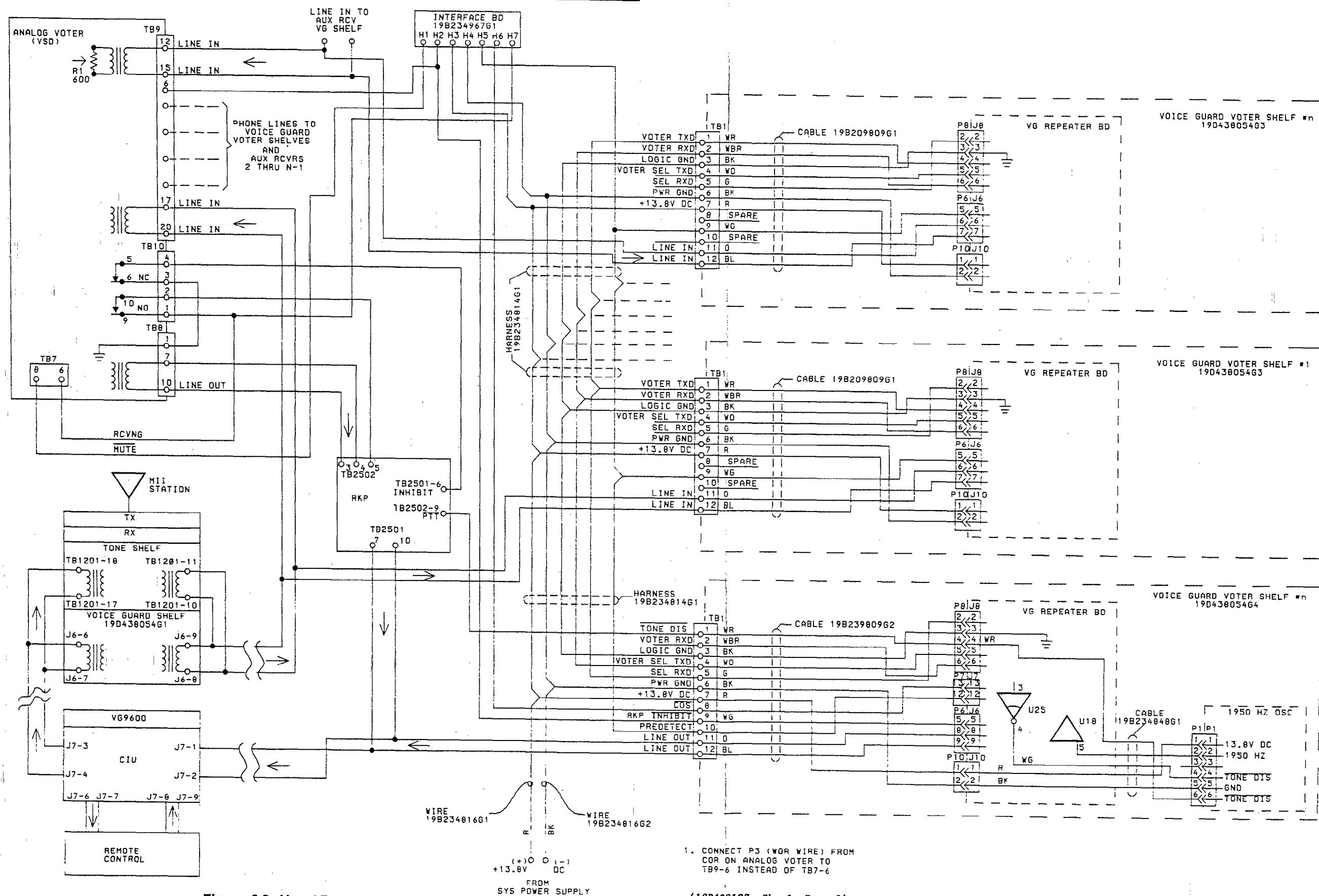


Figure 6-3. Voted Remote/Repeat

(19D438127, Sh. 1, Rev. 2)

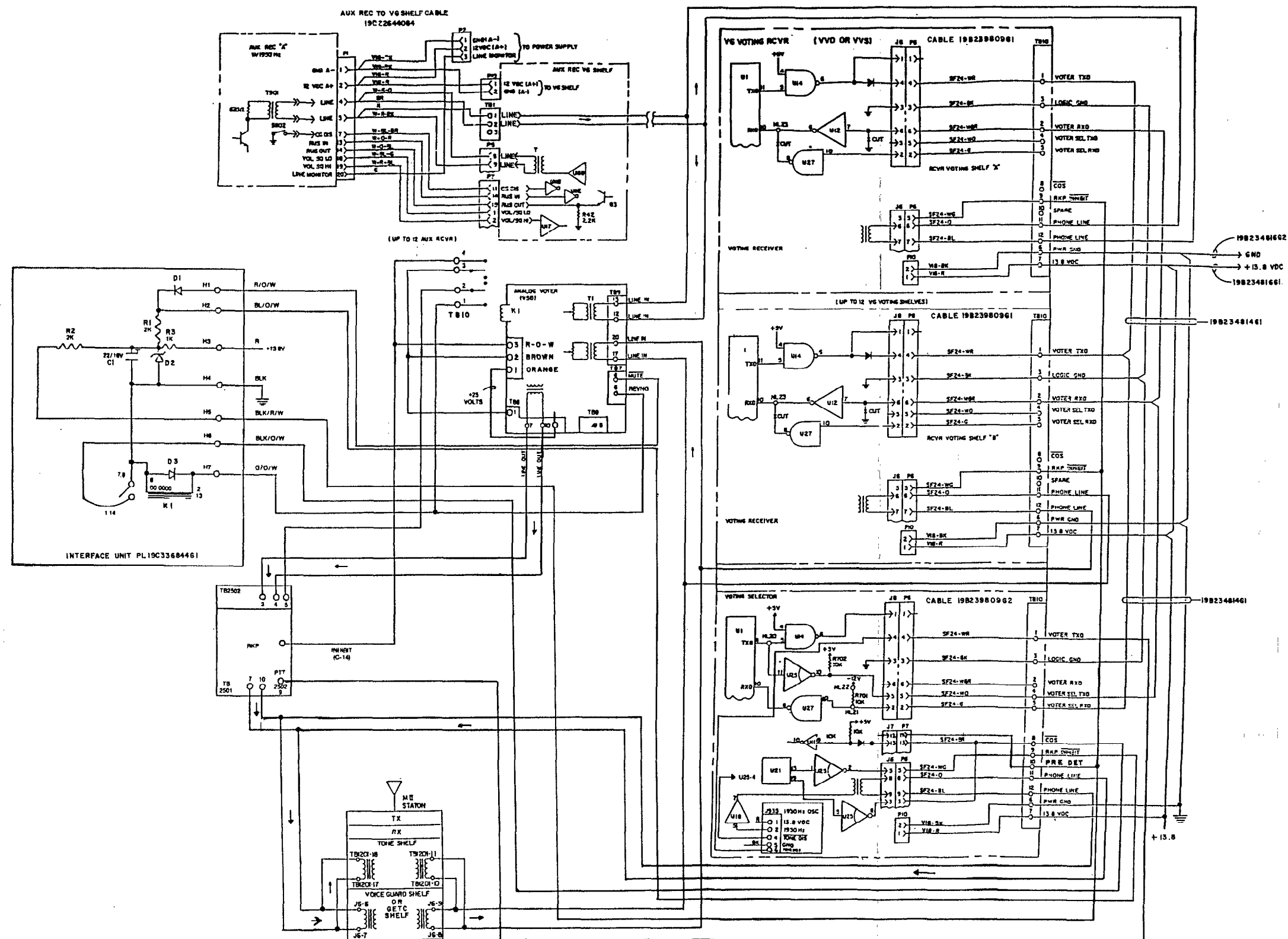


Figure 6-4. Voted Repeat

(This Page Intentionally Left Blank)

CHAPTER 7

VOICE GUARD PUBLICATIONS

APPLICATION	PUBLICATIONS FOR:		
	DES ALGORITHM	VGE ALGORITHM	DES & VGE
MASTR CONTROLLER Maintenance Manual 2-Frequency Option	LBI-31531	LBI-31740	LBI-31688
KEY LOADER Operator's Manual Maintenance Manual	LBI-31541 LBI-31544	LBI-31685 LBI-31684	
DELTA/RANGR MOBILES & STATIONS Operator's Manual	LBI-31520 ¹ LBI-31697 ²	LBI-31697	
Installation Manual Maintenance Manual "SIMON" for the VG module	LBI-31521 LBI-31522	LBI-31698 LBI-31683	LBI-31550
END-TO-END ENCRYPTION STATIONS Maintenance Manual <i>Service Section</i> "SIMON" for the shelf			LBI-31532 <i>LBI-31546</i> LBI-31593
ENCRYPT/DECRYPT (E/D) STATIONS Operator's Manual	LBI-31520 ¹ LBI-31697 ²	LBI-31697	
Maintenance Manual Remote Only <i>VG control board</i> <i>VG 9600 module</i>	LBI-31661 <i>LBI-31665</i>	LBI-31681 <i>LBI-31674</i>	<i>LBI-31664</i>
Remote/Repeat (shelf) <i>VG control board</i> <i>VG 9600 module</i>	LBI-31662 <i>LBI-31665</i>	LBI-31682 <i>LBI-31674</i>	<i>LBI-31664</i>
"SIMON" for the VG module "SIMON" for the shelf			LBI-31550 LBI-31593
AUXILIARY/SATELLITE RECEIVER Maintenance Manual Opt. 9723 (w/VG shelf) Opt. 9730 Opt. 9729 (w/VGE module) "SIMON" for the shelf "SIMON" for the VG module	LBI-31679 LBI-31699, LBI-31665	LBI-31674, LBI-31687	LBI-31593 LBI-31550
VOTING SELECTOR/RECEIVER Maintenance Manual "SIMON" for the shelf			LBI-31680 LBI-31593
CONSOLE INTERFACE UNIT (CIU) Maintenance Manual <i>VG Module</i> <i>4 Freq. Remote Board</i>	LBI-31760 <i>LBI-31665</i>	LBI-31761 <i>LBI-31674</i>	<i>LBI-31552</i>

¹ For FS-1027 (mechanical key locks)² For non FS-1027 (DES algorithm but no key locks)*Manuals shown in italics are sent as part of the manual shown above it.*

CON'T

APPLICATION	PUBLICATIONS FOR:		
	DES ALGORITHM	VGE ALGORITHM	DES & VGE
MPS PERSONAL VG RADIO Operator's Manual Maintenance Manual <i>Service Section</i>	LBI-31613 <i>LBI-31614</i>	LBI-31723 <i>LBI-31724</i>	LBI-31612
MPD SCAN VG RADIO Operator's Manual Maintenance Manual (VHF) Maintenance Manual (UHF) <i>Maintenance Section</i> <i>Service Section</i>	LBI-31912 LBI-31914 LBI-31915 <i>LBI-31945</i> <i>LBI-31918</i>	LBI-38207 LBI-31947 LBI-31946	
MPD SYSTEM VG RADIO Operator's Manual Maintenance Manual (VHF) Maintenance Manual (UHF)	LBI-31913 LBI-31916 LBI-31917	LBI-38208 LBI-31951 LBI-31949	
PROGRAMMING VG-9600 modules & MPS radio (for use with TQ-2310) MPD Personal VG Radio (for use with PC)	LBI-31523	LBI-31776	TQ-3319
MISCELLANEOUS Voice Guard Systems Manual "SIMON" Level Interface Cable for VG-9600 Modules Hump Mount Kit (for VG-9600 Modules) Eye pattern adapter Digital test generator			LBI-31600 LBI-31700 LBI-31747 LBI-38118 LBI-38204

¹ For FS-1027 (mechanical key locks)² For non FS-1027 (DES algorithm but no key locks)*Manuals shown in italics are sent as part of the manual shown above it.*

36th IEEE VEHICULAR TECHNOLOGY CONFERENCE



86CH2308-5

20-22 May, 1986

Dallas, Texas

Technology On The Move

**Sponsored by the
IEEE Vehicular Technology Society**

**Host
Dallas Section, IEEE
and the
Dallas Chapter, Joint VTS/COMSOC Society**

DESIGN AND PERFORMANCE OF A DIGITAL VOICE PRIVACY SYSTEM FOR LAND MOBILE RADIO

G.D. Rose and S. Kappagantula

General Electric Company, Mobile Communications Division, Lynchburg, VA 24502.

This paper presents the design and performance characteristics of a 9600 bits/sec digital voice privacy system. The system has been applied in commercially available mobile radio products. Various aspects of the design including speech bandwidth compression, encryption and radio engineering will be discussed. The resulting performance from a radio frequency standpoint is presented. Performance characteristics will show that certain limitations of previously available commercial mobile radio voice privacy products are overcome in this design.

I INTRODUCTION

Land-mobile radio systems have become a vital tool for efficient operation of many of today's business and governmental organizations. Frequently, the nature of the communications carried by these systems is of a sensitive nature to these organizations. However, radio communications are not private since most of them can be received on available monitors. To overcome this security problem, many mobile radio users are beginning to require some form of voice privacy or scrambling. Voice privacy techniques for land-mobile radio can be divided into two categories, analog and digital. Generally digital approaches provide a much higher level of protection than analog techniques. In digital voice privacy implementations, the analog speech to be transmitted is first digitized. This string of ones and zeros representing speech information is then scrambled in accordance with a predetermined algorithm and then, after appropriate frequency domain filtering, modulates a radio transmitter. The transmitted pseudorandom stream has all the characteristics of white noise when monitored by a standard receiver. Furthermore, there is no perceived change in the noise-like modulation whether there is any analog information being processed or not. In digital scrambling, the only information to be gained by an adversary is that a scrambled transmission is in progress.

In this paper we present the design and performance of a digital voice privacy system that utilizes a data rate of 9600 bits/sec. Section II describes the digital coding of speech, section III with the data encryption technique. Data format design is discussed in Section IV and the operational performance of the radio in Section V.

II DIGITAL ENCODING OF SPEECH

The maximum data rate that can be reasonably supported by a mobile radio channel is influenced by regulatory constraints. Thus a standard 25 KHz channelization cannot carry telephone quality PCM speech using 2-level modulation schemes. Multilevel modulation schemes have the disadvantage of a more rapid performance degradation than 2-level schemes on a Rayleigh fading channel. Furthermore data filtering for bandwidth restriction usually translates into intersymbol interference at the receiver. This causes the received error rate to be increased generally as a function of filter bandwidth and the transmitted data rate. For instance, the bandwidth limits set by FCC regulations (1)

mean that the maximum 2-level modulated data rate that can be reliably supported on a standard channel is around 12-16 kilobits/sec. This is based on typical characteristics of transmitter and receiver data filters. Therefore speech bandwidth compression techniques for such bit rates are required.

Generally speech coders can be divided into two classes: Waveform coders and Speech vocoders. Waveform coders attempt to preserve the transmitted waveform by coding at the transmitter and reconstructing it at the receiver. Examples are PCM, CVSD (Continuously Variable Slope Delta modulation) and SBC (Sub Band Coding). Vocoders operate on an analysis-synthesis basis by the extraction of perceptual parameters of the input speech. An example is the U.S Government standard LPC-10 algorithm. Such coders are generally more bandwidth efficient with respect to the data rate required for a given subjective speech quality but are invariably more complex than waveform coders. Waveform coders can also withstand the bit error rates encountered on a mobile radio channel better than vocoders. The problem is usually solved in vocoders by the use of FEC (Forward Error Correction). However this adds substantially to the complexity of the processing required. Therefore waveform encoding techniques are better suited to mobile radio channels.

The use of linear delta modulation techniques for speech compression have been extensively investigated (2,3). Variants of the concept such as CVSD (Continuously Variable Slope Delta modulation) have proven especially suitable for a mobile radio channel. Figure 1 shows a typical CVSD coder block diagram. The output bit rate is the same as the sampling rate of the input speech. The output of the one bit quantizer is a 0 or a 1 depending on the output of the quantizer for a finite number of previous samples. The adaptation logic generates step sizes which are a function of the variations in the speech signal. The subjective quality of CVSD speech at bit rates of between 12 and 16 Kilobits/sec is acceptable as communications quality. CVSD is a low complexity encoding scheme and its hardware implementation is relatively simple. The disadvantage of CVSD is that lowering the bit rate below 12 Kbps degrades the speech intelligibility substantially. Secondly 12 or 16 Kbs/s data rate is non standard for conventional data modems and UARTS. Lastly these data rates may require wider I.F bandwidths.

Subband coding has been recognized as a suitable coding technique for mobile radio channels. The primary advantage of SBC (Sub Band Coding) is that a lower bit rate is required to produce communications quality speech. This means that a standard data rate such as 9.6 Kbs/s can be used for the speech transmission. SBC is also robust in a Rayleigh fading channel. Zinser et al. (4) have designed and evaluated two such coders for a fading channel. The coder used in our system is derived from the above designs. The block diagram of the coder is shown in Figure 2. The input speech signal is digitized by a standard 8-bit u-law PCM codec after low pass filtering. The codec produces a digitized full band signal. This signal is then split into 4 sub bands, each of which are decimated down to the respective base bands. The band splitting is achieved by a Quadrature Mirror Filter (QMF) bank which yields an octave-spaced band structure. The subsequent data compression is achieved by a combination of APCM (Adaptive PCM) (5) and BCPCM (Block Companded PCM) quantizers. The bandwidth compression data rate from the coder is 9244 bits/sec. Frame synchronization and signalling information are inserted before transmission. This information accounts for 356 bits/s making the channel data rate 9.6 Kbs/s.

The resulting speech quality was evaluated for intelligibility using DRT (Diagnostic Rhyme Test) scores on the speech at various signal levels. The DRT (6) is designed to test the general intelligibility of speech and provides data for the intelligibility of the six elementary phonetic features of speech. In general communications quality speech coders score in the range of 80-90. The range 70-80 is termed 'fair'

and all scores below 70 indicate speech of unacceptable quality. Figure 3 shows the comparative performance of CVSD and Subband coded speech in a Rayleigh fading environment. As can be seen the degradation in intelligibility for the CVSD system is more rapid with worsening signal levels. The reasons for this is a fundamental limitation which will be described in the next section.

III DIGITAL ENCRYPTION OF DATA

The Data Encryption Standard (DES) algorithm has been accepted as a Federal standard encryption technique (8) since 1977. The DES algorithm is also required mandatorily by most Federal agencies for transmission of unclassified but sensitive National Security related information. The use of the DES algorithm has become widespread due to the advances in VLSI technology. A number of vendors now offer single IC DES devices. The DES algorithm which is described in detail in (7) is shown in Figure 4. The algorithm is intended to encipher/decipher 64-bit blocks of data using a 56-bit key. The security of the algorithm lies in the large number of choices of the key variable. The only known technique to attack the algorithm is by an exhaustive search of all possible key combinations. For a 56 bit key there are over seventy quadrillion combinations which ensures a high level of security even if an adversary is well equipped (8).

The DES algorithm is a block cipher algorithm. Data is enciphered in 64 bit blocks. Decryption is the reverse of encryption. The data block encryption/decryption is a function of a complex key schedule calculation. The general security requirements for Telecommunication equipment using DES are defined by the Federal Standard 1027 (9). The DES algorithm can be used for data encryption in a number of modes of which two have become popular with mobile voice privacy systems. These are the Cipher Feedback (CFB) and the Output Feedback (OFB) modes of operation.

The CFB mode of operation also referred to as n -bit CFB produces cipher stream by feeding back n bits of ciphertext per round of encryption. The process is shown in Figure 5(a) for $n=1$. In the 1-bit CFB mode of operation an initialization vector (IV) is first encrypted as a block. The plaintext data is then XORed with one bit of the output register. The ciphertext bit is then shifted into the input register. The next round of encryption is initiated and one bit from the output register is used to encrypt the next plaintext bit and the process continues in this way. It can be noted that since the CFB mode depends only on the ciphertext it is a self-synchronizing mode of operation. Despite its simplicity the CFB mode suffers a serious disadvantage on a mobile radio channel. First a single bit error in the transmitted ciphertext will result in the corruption of 50% of a 64 bit block of recovered plaintext. This propagation of errors tends to reduce the effective communication range substantially. This explains the steep drop in the intelligibility scores of the system referred to in Figure 3. This is a fundamental limitation of the CFB mode of operation.

The OFB mode of the DES algorithm operates as follows. A 64-bit initialization vector (IV) is first encrypted by the transmitting unit. The output vector is bitwise XORed with the plaintext data stream. The output vector or some known function of it is now fed back into the DES algorithm for another round of encryption. In the general case of this mode of operation n bits of the 64 bit output are used to encipher n data bits before the vector is fed back. Figure 5(b) depicts the OFB mode where $n=64$. Clearly the OFB mode is data independent i.e. the encryption vector is local to both the transmitter and receiver. This implies that bit errors in the transmitted ciphertext will not be propagated through the recovered plaintext as in the CFB mode. The OFB mode requires that the transmitter and receiver

start with the same IV to be in sync. This imposes an overhead in the data stream which translates to a lowering of available bits to carry voice information. The non-error propagation characteristics of the OFB mode however, outweigh the overhead requirements which will be described in section V.

IV DATA FORMAT FOR THE R.F. CHANNEL

The IV used throughout an encrypted transmission provides for cryptographic sync. Reliable decoding of the transmitted speech data depends on the proper maintenance of cryptographic sync. This implies that the IV has to be protected against fades and dropouts on the R.F. channel. The voice privacy system was intended for use in the VHF, UHF and 800 Mhz regions. Each of these frequency regions are affected by fades of varying characteristics. For instance at 850 Mhz, the average fade duration at a vehicle speed of 20 MPH is about 2 milliseconds at a signal threshold of 15 dB below the mean signal strength (10). In this case signal exists under the threshold for about 2 percent of the time. At lower carrier frequencies or lower vehicle speeds the fade durations are longer and less frequent. At VHF frequencies typical fade lengths are about 30-50 msec. Hence the data format should be able to ensure correct reception of the IV under these conditions.

The data format that was designed meets the following objectives :

- o Greater than 99% probability of correct acquisition at an average channel error rate of 3%.
- o Protection of data from fades of 50 msec in length.
- o Late entry or 'rejoin' capability for a receiver that enters the conversation after a transmission has already begun. This implies that recurring sync and IV bursts will be transmitted at regular intervals in the data stream.
- o A very low probability of false cryptographic sync detection.

The preamble contains bit sync, word sync, signalling and cryptographicsync information. The data UART used by the system requires bit and word sync information. The UART is designed to recognize a 11-bit Barker code word. Signalling information included in the preamble is used for repeater accessing and for group access functions. The transmitted data stream contains the following:

- o A 11-bit Barker code word transmitted in the preamble and every subsequent data frame. A data frame duration is about 225 msec.
- o Continuous digital signalling for repeater or group access within a carrier frequency. This field is called the Outside Address (OA) field. This information is transmitted both in the preamble and in data frame headers.
- o SBC voice encrypted by the DES algorithm operating in the Output Feedback (OFB) mode.

Preamble Format

Figure 6(a) shows the preamble transmitted at the start of a voice transmission. The preamble begins with a burst of bit sync information which is a 'dotting' pattern (101010...). This burst allows the receiving UART to acquire bit sync. The dotting burst is followed by a burst of word sync and digital signalling information. A word sync burst consists of 12 repeats of a 48 bit packet. The packet consists of a Barker code word, two bytes of OA and a packet position number. The receiving unit acquires word sync when it detects the Barker code word. The OA performs a validation function such that only units with corresponding OAs can communicate on a given frequency. The redundancy of 12 was chosen such that word sync is reliably acquired with a signal level close to the 12 dB SINAD level of the radio. The position number is used to establish the boundary between the word sync/signalling burst and the following cryptographic sync information. The OA bytes are complements of each other in the preamble. The OA validation requires that the two bytes perfectly match when a Barker code word is detected.

The cryptographic sync burst referred to in Figure 6 consists of a 64 bit IV and a 16 bit null information field repeated 9 times along with a fade protection field which forms the IV group. The fade filler time Tfg is 60 msec. The IV information accounts for 75 msec. Each IV group is preceded by a 64-bit guard band (GB). The receiver performs a 5 of 9 majority vote on the IV information. The interleaving of the GB information allows the burst to withstand fades upto 45 msec in duration. Figure 7 shows the performance of preamble acquisition with respect to average bit error rate and received signal strength.

Data Frame Header

A frame header is transmitted every 225 msec. The header consists of 14 bytes of information. Figure 6(b) shows the composition of the frame header. The header is made up of 2 bytes of the Barker code word and fill bits, 2 bytes of OA and 10 bytes for IV information. The OA bytes are copies of each other unlike their counterparts in the preamble. This is used to distinguish the preamble acquisition from acquisition of a data frame. A receiving unit that has missed the preamble or has lost data sync will attempt to resync with the data stream. The frame header provides the resync information. A unit which attempts to resync or 'late enter' will do so by detecting one frame header and probability matching the IV of that frame with the IV of the next successive frame. The updating of the IV from frame to frame is a function of the DES algorithm. This makes the probability of false detection of the IV virtually negligible.

V IMPLEMENTATION AND PERFORMANCE

Voice Guard is the name that has been applied to the digital voice security system described in this paper. The system has been applied to mobile, station and personal (hand-held) equipment. The Voice Guard signal requires an overall baseband that is essentially flat from 10 Hz to 4.8 KHz thus requiring direct FM modulators in products equipped with Voice Guard, but without any special IF circuitry.

The mobile and personal products are synthesized and provide constant deviation over the required frequency range. The modulation approach is to split the Voice Guard signal so as to allow the low frequency components to modulate the reference oscillator and the high frequency components to modulate

the synthesizer loop. The logic level serial digital Voice Guard signal is passed thru a GMSK (Gaussian Minimum Shift Keying) filter in order to minimize the required spectral occupancy of the modulated signal. The input to the FM modulator is switched between the output of the GMSK filter when operating in the voice private mode, or the Post Limiter Filter when operating in the clear voice mode. Figure 8 shows the block diagram of a Voice Guard unit. Figures 9(a) and (b) show the transmitted and received eye-patterns of the data stream.

Two base station types are available. The first is an end-to-end security version and requires no cryptographic equipment at the base station (repeater) site. Furthermore, in remote base station applications, encryption/decryption can be accomplished only at the control point hence, the control path is also encrypted. The base station or repeater receiver regenerates the Voice Guard data and sends it down to the control point in the case of remote operation and, to the transmitter in the case of repeater operation. Only one type of Voice Guard station unit is required in this system for remote, repeat and remote/repeat operation. The mode of operation of the station can be reconfigured in the field by the simple operation of setting a DIP-switch. The second type of base station provides only R.F. security i.e. point-to-point encryption. This type of base station requires cryptographic equipment at the station/repeater site. Communication between the station and the dispatch console/controller are carried on over standard voice grade telephone lines using available telephone modems.

The high band station exciter is a phase lock multiplier that can easily support the filtered Voice Guard digital signal. The input to the modulator is switched between the output of a GMSK filter for private operation and the Post Limiter Filter for clear voice operation. For UHF operation, the direct FM oscillator-multiplier exciter is to be employed. Modulation is applied directly to the FM oscillator. It is steered between the GMSK filter and the Post Limiter Filter just as in the previously described equipments.

Spectral Occupancy

As is mentioned earlier, the FCC radio Rules and Regulations, Part 90, defines the maximum spectral occupancy characteristic that a radio not having a modulation limiter and post limiter filter can possess. Figure 10 shows the spectrum occupied by a Voice Guard signal along with the FCC limits for operation above 450 Mhz. The FM deviation is set at 3 Khz.

Range Performance

As the RF signal-to-noise ratio degrades while operating in the clear, background noise becomes increasingly noticeable. At such levels there is no degradation in the recovered digital audio. At noise levels which are high enough to cause bit errors, Voice Guard yields a warbling characteristic to the recovered voice. Under some conditions, it is possible that the private mode is more intelligible than the clear mode. Laboratory and field tests have shown the range of clear and private modes of operation to be essentially equal. Figure 3 shows the DRT test results for clear and private operation as a function of clear mode SINAD.

Capture Ratio

.....

Capture ratio is a measure of on-channel interference tolerance of a receiver to another signal. A standard FM mobile radio operating in the clear at about 18 dB SINAD will be captured by another on frequency signal that is 5 dB stronger than the reference signal. Similarly, no significant interference is noticed when the interfering signal is 5 dB weaker than the reference (18 dB SINAD) signal. The Capture Ratio is then 5 dB. When operating in the encrypted mode, the capture ratio is found to be 4 dB.

Adjacent Channel Interference

.....

Even though the Voice Guard data is filtered prior to modulating the transmitter, there is a classic (SIN X)/X distribution of spectral energy which is still present in the adjacent channel even though the FCC spectral occupancy requirements have been met. An examination of several radios showed that the energy in the adjacent channel is 27 to 30 dB higher when operating in the encrypted mode than when operating in the clear with a one KHz tone in hard audio limiting.

VI CONCLUSION

We have described a digital voice privacy system which has been applied in commercially available products. The GE-Voice Guard system is now available in both mobile and handheld radios. The performance discussed in the body of the paper shows that the Voice Guard system achieves an acceptable voice quality with no loss of range as compared to clear mode operation (13). In addition, use of SBC with the OFB mode of DES have allowed continuous digital signalling. This offers features analogous to using CTCSS in the clear mode. The 9600 bits/s data rate allows unmodified radio IFs and modulators to be used, as well as inexpensive modems for land line interface. The system addresses a major need for voice privacy on land mobile channels. Furthermore limitations present in previously available privacy products have been eliminated in this design.

ACKNOWLEDGEMENTS

The authors would like to thank Mr. C. Szczutkowski for his suggestions and encouragement in the writing of this paper. The effort of Mrs. F. McConville in typing the paper are gratefully acknowledged.

REFERENCES

- (1) FCC Radio Rules and Regulations, Part 90.
- (2) M.R. Karim, "An Investigation of Delta Modulation of Speech for Mobile Radio", IEEE Trans. Veh. Tech., pp.158-165, Nov. 1982.

- (3) P.M. Petrovic, "Digitized Speech Transmission at VHF Using Existing FM Radios", IEEE Trans. Veh. Tech., pp. 76-88, May 1982.
- (4) R.L. Zinser et al., "A Robust 9.6 Kb/s Subband Coder Design for the Rayleigh Fading Channel", Proc. ICC, Amsterdam, 1983.
- (5) P. Cumminskey et al., "Adaptive Quantization in Differential PCM Coding of Speech", BSTJ, Vol. 52, pp. 1105-1118, Sept. 1973.
- (6) W.D. Voiers, "Diagnostic Evaluation of Speech Intelligibility", in Speech Intelligibility and Speaker Recognition, Dowden, Hutchinson and Ross, Stroudsburg, Pa., 1977.
- (8) FIPS-PUB 46, "Specifications for the Data Encryption Standard", Jan. 1977.
- (9) H. Beker and F. Piper, "Cipher Systems", Wiley Interscience, 1982.
- (10) FED-STD 1027, "General Security Requirements for Equipment Using the Data Encryption Standard", April 1982.
- (11) G.A. Arredondo et al., "Voice and Data Transmission", BSTJ, Vol. 58, pp. 97-122, Jan. 1979.
- (13) D. Bishop, "GE encryption scheme improves coverage, reduces bandwidth", Mobile Radio Technology, August 1985.

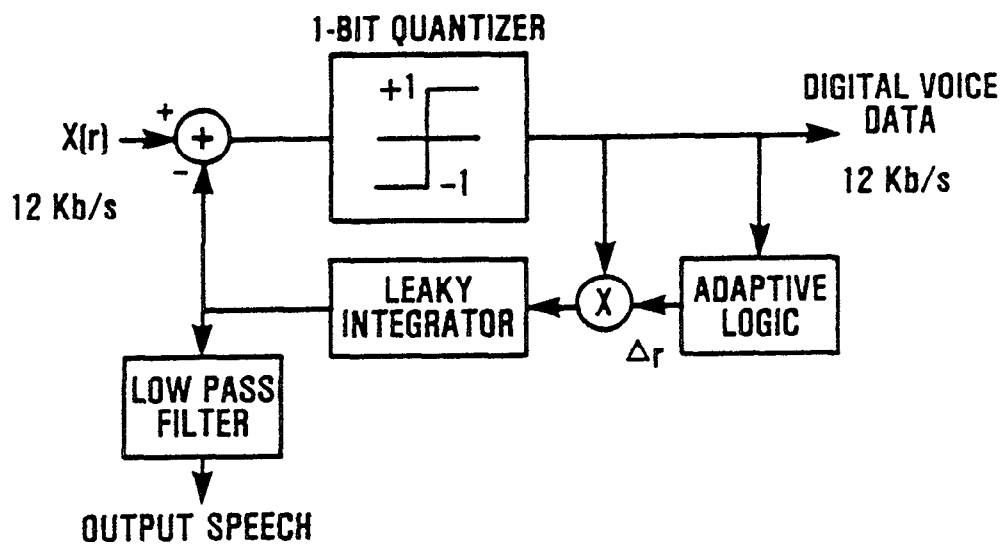


Fig. 1 Block Diagram of a 12 Kb/s CVSD Coder

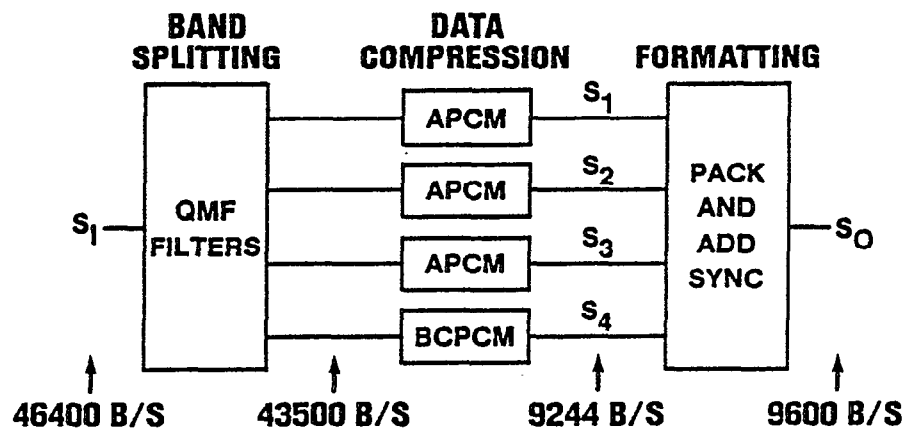


Fig. 2 Sub Band Coder: Block Diagram

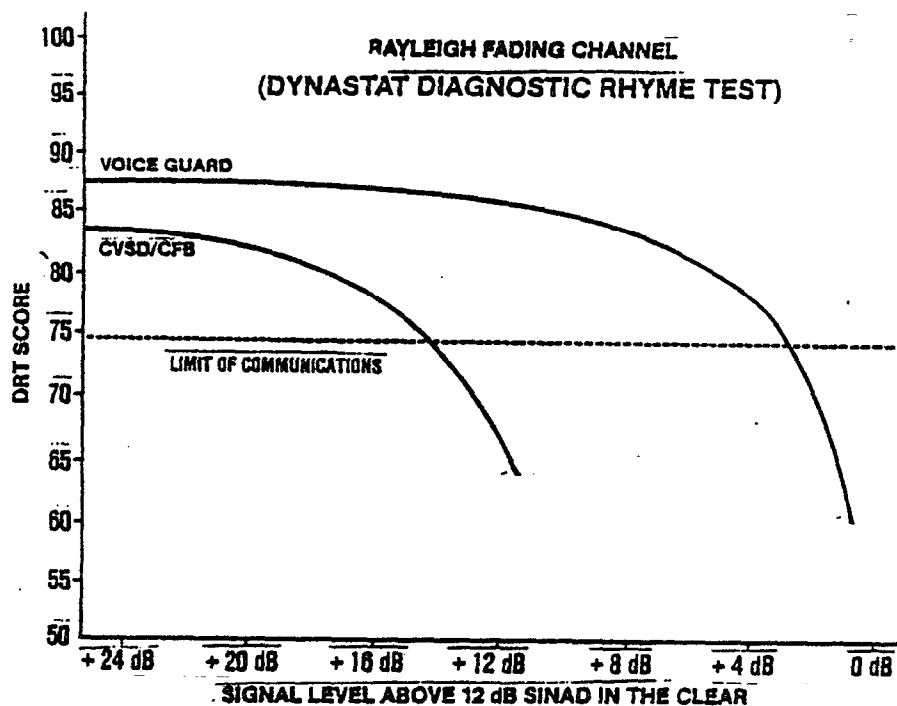


Fig. 3 Comparison of Voice Quality with Signal Level for the SBC and CVSD Systems

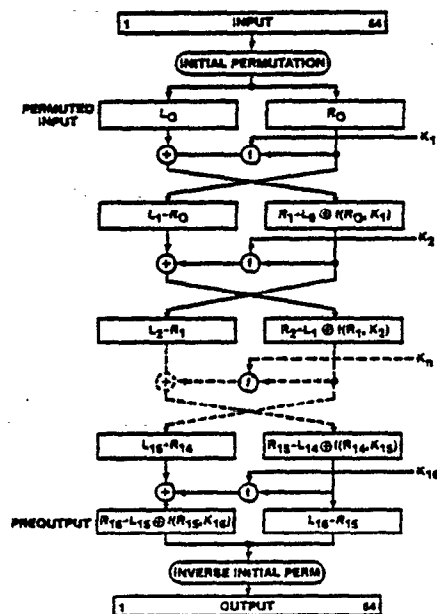


Fig. 4 Block Diagram of the DES Algorithm

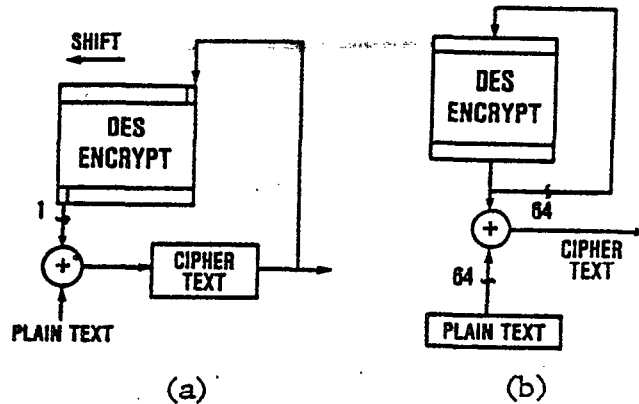


Fig. 5 The CFB and OFB Modes of the DES Algorithm

PREAMBLE:

DOTTING	SYNC SEQUENCE	IV FIELD (9 REPEATS)	VOICE GUARD FRAMES
Tx turn on	Sync/OA/S# (12 repeats)	64 Bit IV + Fade protection field	Subband Coded Encrypted Data Frames

Fig. 6(a) Preamble Data Format

VOICE GUARD FRAMES:

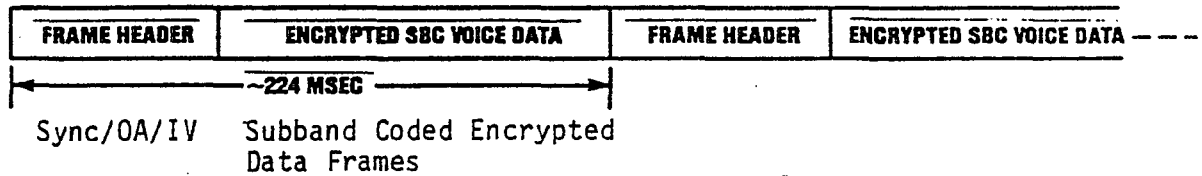


Fig. 6(b) Frame Header and Voice Frame

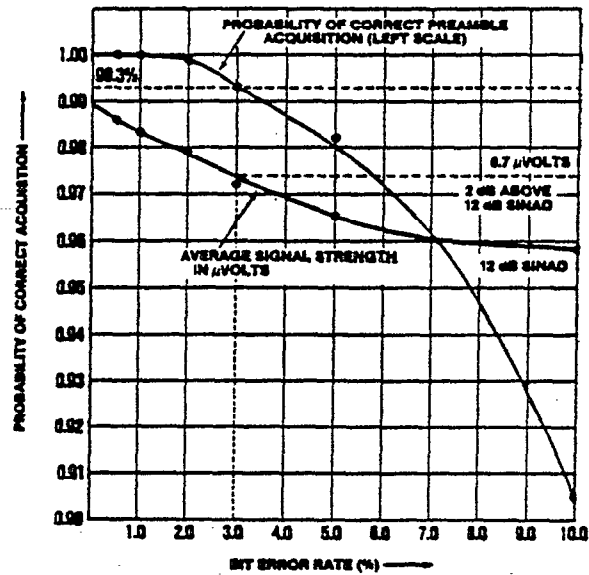


Fig. 7 Preamble Acquisition Performance

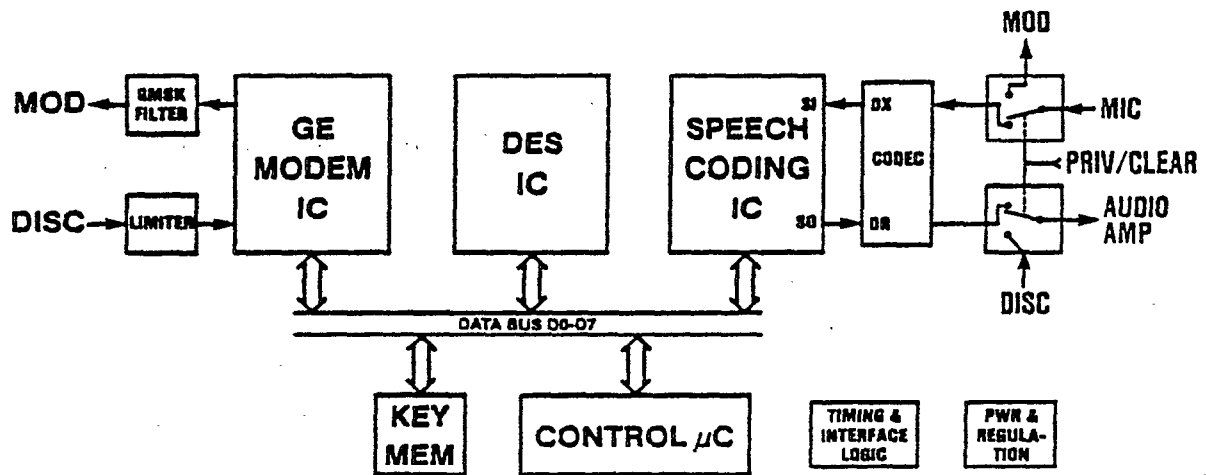


Fig. 8 Block Diagram of a Voice Guard Unit

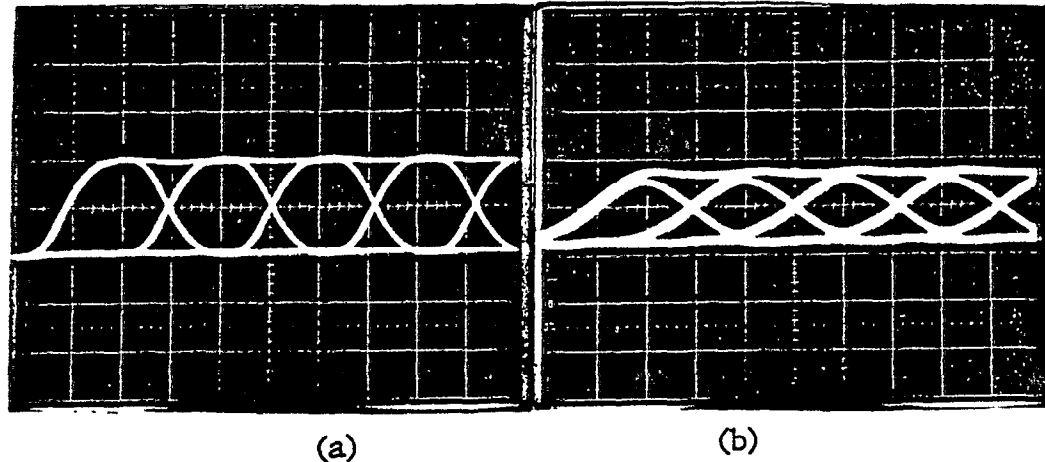


Fig. 9 Transmitted and Received Eye Patterns

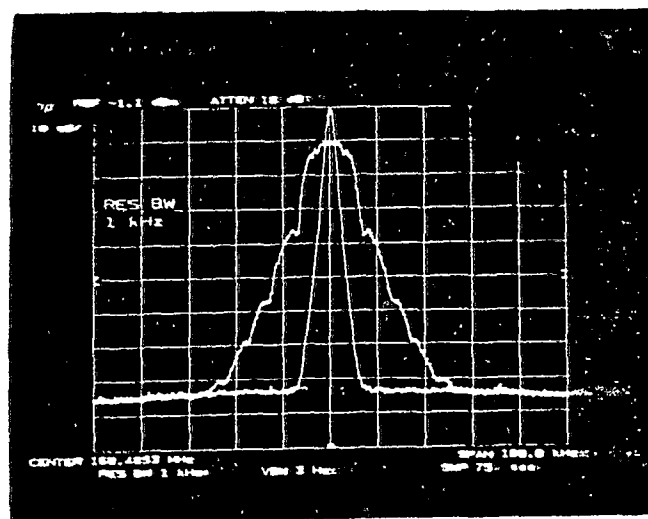


Fig. 10 Spectral Occupancy of the Transmitted Voice Guard Signal

APPENDIX

SUPPLEMENTAL SECURITY REQUIREMENTS FOR THE APPLICATION OF FEDERAL STANDARD 1027 TO DES-PROTECTED COMMERCIAL VOICE RADIOS

Exceptions and Clarifications to Federal Standard 1027. The following exceptions and clarifications to Federal Standard 1027 are approved for handheld, mobile, and fixed station commercial radios using the DES algorithm.

1. Mobile and Fixed Station Radios. The following exceptions or clarifications to Federal Standard 1027 apply to the degree stated in this paragraph for mobile and fixed station commercial radios which embody the DES algorithm. Paragraphs referenced below are those of Federal Standard 1027 unless otherwise stated.

a. Paragraph 3.1.1 and 3.1.4. - The radio need not have the locks required by this paragraph. If the radio does not have integral locks, the radio, when installed, must be lockable by an external mechanism which precludes unauthorized access to the key variable entry controls and other controls (see Paragraph 3.7) critical to the security of the radio.

b. Paragraph 3.1.2 - Protection against theft and undetected substitution of the radio is required and can be provided by a lockable mounting mechanism external to the radio as described in Paragraph 3.3.1.a. of this specification. If an external mechanism is used, it shall be made available by the radio manufacturer.

c. Paragraph 3.1.3 - In vehicular applications, the lock which prevents unauthorized return of the radio to operational status, shall be in addition to the normal vehicle ignition lock.

d. Paragraph 3.2.1.2.1 - 3.2.1.2.4 - In instances where a key variable loader already exists or in cases where the specified interface cannot be incorporated into an existing radio without substantial redesign, alternate mechanical and electrical interfaces for an externally connected key variable loader are permitted, providing that the key variable loader can enter printed keying material in the format described in Paragraph 3.2.1.1. and Table 2 of Federal Standard 1027.

e. Paragraph 3.2.4 - The requirement to retain the key variable with an independent back-up energy source, applies only when the primary power source is interruptable under normal operating conditions.

f. Paragraph 3.3 - A new IV is required only for each push-to-talk operation of the radio in lieu of the conditions stated in the third sentence of this paragraph.

g. Paragraph 3.4.1 - The Cipher Feedback, Cipher Block Chaining, and Output Feedback modes are approved for single channel voice radio applications.

h. Paragraph 3.4.2.3 - Performing the checkword test for each push-to-talk operation is an acceptable frequency of testing for this function.

i. Paragraph 3.4.3.1 and 3.4.3.2 - These paragraphs do not apply.

j. Paragraph 3.4.3.5 - Only the last sentence applies.

k. Paragraph 3.7 - The POWER ON/OFF function is also optional for this application. If the ALARM RESET and TEST MODE functions are performed automatically as a result of some related action by the radio operator, separate controls are not required.

l. Paragraph 3.8 - The POWER ON indicator is not required. The radio shall in some manner (visual or audible) indicate the following status conditions: DES BYPASS, TEST, ALARM, AND PARITY.

m. Paragraph 3.9 - If the primary power source for the radio is interruptable under normal operating conditions, then critical storage shall be held with an independent back-up energy source during these periods of interruption.

n. Paragraph 3.10 - Alternate EMI/EMC criteria which are similar to those of MIL-STD-461B may be used if prior approval is obtained. The EMI/EMC concerns are focused on spurious radiation from the radio and conducted emanations on the protected voice signal.

2. Handheld Radios. The security requirements contained in Paragraph 1 of this Annex also apply to handheld radios except in those cases noted in this paragraph. The following paragraphs of Federal Standard 1027 apply to the degree stated for commercial handheld radios.

a. Paragraph 3.1.1 and 3.1.4. - Physical locks are not required on the equipment.

b. Paragraph 3.1.2 - Equipment is not required to have a mounting technique to deter theft or substitution.

c. Paragraph 3.1.3 - Standby modes, if used, need not be guarded by a physical lock.

d. Paragraph 3.7 - The standby mode control is optional.

e. Paragraph 3.9 - The radio shall be capable of holding critical storage for at least 30 seconds to facilitate changing of the radio's battery with minimum disruption in secure radio operation.



Ericsson GE Mobile Communications Inc.
Mountain View Road • Lynchburg, Virginia 24502

Printed in U.S.A.

FEDERAL STANDARD

TELECOMMUNICATIONS: GENERAL SECURITY REQUIREMENTS
FOR EQUIPMENT USING THE DATA ENCRYPTION STANDARD

This standard is issued by the General Services Administration pursuant to the Federal Property and Administrative Services Act of 1949, as amended.

1. Scope

1.1 Description. This standard specifies the minimum general security requirements that are to be satisfied in implementing the Data Encryption Standard (DES) algorithm in a telecommunications environment. The DES itself specifies an algorithm used for cryptographically protecting certain U.S. Government information. (This algorithm is described in Federal Information Processing Standards Publication 46). The requirements defined in this standard affect the security of equipment implementing the DES algorithm. Other security requirements, which relate to the interface and interoperability of DES cryptographic equipment with associated terminal equipment (e.g., narrative text, automatic data processing, digital facsimile, digital voice, etc.), will be addressed in other Federal telecommunication standards.

1.2 Security Objectives. This standard addresses the following security objectives:

- a. To prevent inadvertent transmission of plain text.
- b. To prevent theft, unauthorized use, or unauthorized modification of DES cryptographic equipment while installed.
- c. To prevent unauthorized disclosure or modification of key variables while in DES cryptographic equipment.
- d. To provide interoperability between key variable loaders and DES cryptographic equipment, and facilitate the use of standardized keying material for U.S. Government applications of the DES algorithm.
- e. To prevent data encryption when a critical cryptographic failure condition exists, and to generate an alarm upon detection of a critical cryptographic failure.

1.3 Purpose. This standard prescribes security requirements for implementation of the DES in telecommunication equipment and systems used by the departments and agencies of the U.S. Government.

1.4 Application. This standard applies to all DES cryptographic components, equipment, systems, and services procured (including lease) by U.S. Government departments and agencies for the encryption of digital information in the telecommunications environment. This includes stand-alone DES cryptographic equipment as well as any Data Terminal Equipment and Data Circuit-terminating Equipment utilizing the DES algorithm for digital encryption. When DES cryptographic equipment is integrated into Data Terminal Equipment (DTE) or Data Circuit-terminating Equipment (DCE), this standard applies to those portions of the DTE or DCE design which implement the security requirements of this standard. The same degree of protection is required whether DES cryptographic equipment is in stand-alone units or is physically embedded in associated equipment. Guidance to facilitate the application of this standard, with respect to degradation of its security by improper implementation or use, will be provided for in a revision to Federal Property Management Regulation 41, Code of Federal Regulations 101-35.3.

1.5 Verifying Conformance. Procedures for verifying that DES cryptographic equipment conform with this standard are available from the preparing activity.

1.6 Definitions and Conventions. The following definitions, conventions, and terminology apply in this standard.

- a. Bypass: A condition which allows plain text to pass through equipment unaltered, with or without some delay.
- b. DES: The Data Encryption Standard algorithm specified in Federal Information Processing Standards Publication 46.
- c. DES Cryptographic Equipment: Equipment embodying one or more DES devices and associated controls, interfaces, power supplies, alarms, and the related hardware, software, and firmware used to encrypt, decrypt, authenticate, and perform similar operations on information.

- d. **DES Device:** The electronic hardware part or subassembly which implements just the DES algorithm specified in Federal Information Processing Standards Publication 46, and which is validated by the National Bureau of Standards.
- e. **Initializing Vector (IV):** A vector used in defining the starting point of an encryption process within a DES device.
- f. **Key Generator:** A DES device plus those additional cryptographic functions required to implement: (1) a particular mode of encryption; (2) combining of plain text or cipher text with DES device output; (3) the initializing vector; and (4) associated alarms and self-testing.
- g. **Key Variable:** A 64-bit input to DES cryptographic equipment, with 8 bits used for parity checking and 56 bits used in the DES device for encryption or decryption. Unless otherwise stated, reference to a DES key variable means a key variable in its unencrypted form.
- h. **Key Variable Loader:** An electronic, self-contained unit which is capable of storing at least one 64-bit DES key variable and transferring that key variable, upon request, into DES cryptographic equipment.
- i. **Message:** A generic term used to describe, in the broadest sense, information to be transferred which is represented by a digital sequence. This sequence should be numbered 1, 2, . . . , N, where 1 represents the information unit transmitted first.
- j. **Physical Key:** A device used to operate a mechanical lock.
- k. **Pseudorandom Binary Process:** A deterministic technique for producing a sequence of binary digits which satisfy the statistical properties of a random bit stream.
- l. **S-Box:** A nonlinear function which substitutes four output bits for six input bits within a DES device to make the DES algorithm a nonlinear process (see Federal Information Processing Standards Publication 46).
- m. **Zeroization:** A method of erasing an electronically stored DES key variable by removing electrical power from the electronic storage, by overwriting that storage with an all ONES or ZEROS pattern, or by otherwise irrevocably altering the contents of the DES key variable storage.

2. Referenced Documents

- a. Federal Information Processing Standards Publication 46: DATA ENCRYPTION STANDARD. January, 1977. (Copies of this standard are available from the National Technical Information Service, U.S. Department of Commerce, 5285 Port Royal Road, Springfield, VA 22161.)
- b. Federal Information Processing Standards Publication 81: DES MODES OF OPERATION. December, 1980. (Copies of this standard are available from the National Technical Information Service, U.S. Department of Commerce, 5285 Port Royal Road, Springfield, VA 22161.)
- c. Federal Standard 1031: TELECOMMUNICATIONS: GENERAL PURPOSE 37-POSITION AND 9-POSITION INTERFACE BETWEEN DATA TERMINAL EQUIPMENT AND DATA CIRCUIT-TERMINATING EQUIPMENT. (Copies of this standard are available from GSA, Specifications and Consumer Information Distribution Branch (WFSIS), Bldg. 197 (Washington Navy Yard), Washington, DC 20407.)
- d. Military Standard 461B: ELECTROMAGNETIC EMISSION AND SUSCEPTIBILITY REQUIREMENTS FOR THE CONTROL OF ELECTROMAGNETIC INTERFERENCE. (Copies of this standard are available from the Naval Publications and Forms Center, 5801 Tabor Avenue, Philadelphia, PA 19120.)
- e. Military Standard 462: MEASUREMENT OF ELECTROMAGNETIC INTERFERENCE CHARACTERISTICS. (Copies of this standard are available from the Naval Publications and Forms Center, 5801 Tabor Avenue, Philadelphia, PA 19120.)
- f. National Bureau of Standards Special Publication 500-20: VALIDATING THE CORRECTNESS OF HARDWARE IMPLEMENTATIONS OF THE NBS DATA ENCRYPTION STANDARD. September, 1980. (Copies of this publication are available as SN 003-003-01861-9 from the Superintendent of Documents, U.S. Government Printing Office, Washington, D.C. 20402.)
- g. National Bureau of Standards Special Publication 500-61: MAINTENANCE TESTING FOR THE DATA ENCRYPTION STANDARD. August, 1980. (Copies of this publication are available as SN 003-003-02225-0 from the Superintendent of Documents, U.S. Government Printing Office, Washington, D.C. 20402.)
- h. Proposed Federal Standard 1026: TELECOMMUNICATIONS: INTEROPERABILITY AND SECURITY REQUIREMENTS FOR USE OF THE DATA ENCRYPTION STANDARD IN THE PHYSICAL AND DATA LINK LAYERS OF DATA COMMUNICATIONS; dated June 1, 1981.

3. Requirements

3.1 Physical Security. DES cryptographic equipment shall be designed to restrict physical access to internally stored DES key variables and to deter theft, unauthorized use, or unauthorized modification of the equipment when installed. The level of physical security provided shall be such that unauthorized attempts at access or use will either be unsuccessful or will have a high probability of being detected during penetration or subsequent to penetration. The installation design must minimize the possibility of penetration which cannot be visually detected.

3.1.1 Locks. At least one lock shall be used to limit access to the key variable entry controls. When the Cipher Block Chaining mode is used and the Initializing Vector (IV) is externally entered into DES cryptographic equipment, access to the associated controls shall be limited by the same lock which protects the key variable entry controls. In addition, certain other controls shall be operated by means of a physical key-operated selection switch or shall be accessible only upon opening or removing a locked cover (see section 3.7). The physical key used to operate or access these controls shall be different from the physical key used to limit access to the key variable entry controls. Note that the two locks previously described may be used in conjunction with each other ("two person control") when protection against the possibility of unauthorized use is considered necessary. All locks shall be of the pick-resistant variety (MEDECO or equivalent).

3.1.2 Mounting. A means shall be provided to protect against theft and substitution of DES cryptographic equipment when installed (with or without a key variable present). A solution such as a mounting mechanism accessible only from the interior of the locked equipment shall be used to deter removal of the equipment by any means other than determined force.

3.1.3 Standby Periods. DES cryptographic equipment shall be designed so that operating personnel can conveniently make it inoperable (while retaining the key variable) during periods when the equipment is in standby, and not in operation. This shall be implemented in such a manner as to prevent unauthorized use, for example, by reapplication of power. Once placed in standby, equipment shall not be capable of being restored to operation without the operation of at least one lock.

3.1.4 Equipment Enclosure. DES cryptographic equipment enclosures shall be designed such that a physical lock must be operated in order to disassemble the equipment to an extent that would permit undetectable access to internal circuitry. Also, all holes placed in the outside surface of the equipment during manufacture shall be located such that undetectable access to key variable storage and processing circuitry, as well as undetectable disassembly of the equipment, are not possible using these holes.

3.2 Key Variables. The security provided by DES cryptographic equipment is dependent upon the DES key variable. The same DES key variable must be inserted into equipment in a link or network to make a grouping of equipment cryptographically unique and compatible. A DES key variable consists of 64 bits (K1 through K64), 56 bits of which are randomly or pseudorandomly derived and 8 bits of which are odd parity check bits. Each bit of odd parity is computed individually on its preceding seven-bit group of random or pseudorandom bits according to the convention shown in table L.

3.2.1 Key Variable Entry. Two approved methods of entering unencrypted DES key variables into DES cryptographic equipment are described below. All DES cryptographic equipment shall utilize at least one of these two methods of key variable entry. This is required to perform one or more of the following: (1) to enter DES key variables for normal encryption and decryption, (2) to provide the capability to enter a key variable to decrypt encrypted and electronically transmitted key variables, and (3) to facilitate maintenance. Ciphertext output shall be inhibited during transfer of key variables into DES devices. A means of permitting operating personnel to either conveniently correct errors made during manual key variable entry or to reenter the entire key variable shall be provided. When a DES key variable is assembled into a single 64-bit sequence, the bits shall be ordered in the following manner: K1, K2, . . . , K64. This numbering corresponds to the numbering of key variable bits defined in Federal Information Processing Standards Publication 46.

3.2.1.1 Method 1. DES cryptographic equipment may contain an integral capability to manually enter DES key variables from printed form. The printed DES key variables shall consist of a sequence of 16 symbols (V1, V2, . . . , V16) entered starting with the left-most symbol (V1). Each printed symbol represents a four-bit binary word corresponding to four bits of the DES key variable, as defined in table 2. Manual entry can be accomplished by any technique which provides relatively easy, reliable loading (e.g., keyboard, rotary switches, thumbwheel switches, etc.). If a DES key variable is displayed electrically or mechanically, all visual residue of the DES key variable shall be removed automatically after it is accepted as valid (see section 3.2.4).

3.2.1.2 Method 2. DES cryptographic equipment may accept key variables in electronic form from an externally connected key variable loader in accordance with the electrical and mechanical interface requirements of this standard. When the 64-bit DES key variable sequence is transferred serially, the order of transfer is as listed in section 3.2.1, with K1 being the first bit transferred. After a DES key variable has been entered into a key variable loader and verified by the key variable loader (successful parity check), there shall be no visual or mechanical residue of the key variable available to a person having access to the key variable loader. The key variable loader shall have a zeroize capability controlled by operating personnel.

3.2.1.2.1 Key Variable Transfer Operation. Electronic key variable transfer into DES cryptographic equipment from a key variable loader is initiated by the DES cryptographic equipment under control of operating personnel. Operating personnel shall initiate the key variable transfer by some manual action to the DES cryptographic equipment which will result in a REQUEST indication being sent by the DES cryptographic equipment to the key variable loader. Upon receipt of REQUEST indication, the key variable loader will provide a 64-bit serial key variable on the DATA circuit and an associated 64 cycles of clock on the CLOCK circuit. The timing involved in this DES key variable transfer is shown in figure L.

3.2.1.2.2 Interface Circuits. The DES key variable transfer interface shall consist of nine circuits: GROUND, REQUEST, DATA, CLOCK, VDD, and four undesignated circuits. The functional relationship of the REQUEST, DATA, and CLOCK circuits is shown in figure L.

- a. **GROUND.** This circuit is connected to logic ground within DES cryptographic equipment. In many equipment, this circuit will also be connected to chassis ground, internal to the equipment.
- b. **REQUEST.** This circuit is normally OFF (high). It turns ON (low) as a result of an action by operating personnel to initiate a key variable transfer. REQUEST is generated by DES cryptographic equipment.
- c. **DATA.** In response to a REQUEST indication, the DATA circuit conveys the 64 bits of DES key variable to the DES cryptographic equipment. The DATA circuit may also be used, under control of the undesignated circuits, for other purposes. DATA is generated by the key variable loader.
- d. **CLOCK.** In response to REQUEST indication, the CLOCK circuit sends 64 clock cycles synchronously, and in a specified phase relationship with respect to the key variable bits on the DATA circuit. The CLOCK circuit may also be used for other purposes, under control of the undesignated circuits. CLOCK is generated by the key variable loader. DES cryptographic equipment shall respond to only the first 64 clock cycles (and ignore any additional clock cycles) associated with a given DES key variable transfer in response to a REQUEST indication.
- e. **VDD.** This circuit is connected to a regulated 5 ± 0.5 volt power supply within the DES cryptographic equipment. VDD provides a positive logic voltage reference for key variable loaders with floating ground and negative internal logic (such as the KOI-18).
- f. **Undesignated Circuits.** Use of the four undesignated circuits is optional, and they can be used for any function associated with key variable management and/or equipment control. The electrical parameters of these undesignated circuits, if used, must conform to the general electrical requirements contained in section 3.2.1.2.3 and table 3 of this standard. Specifically, undesignated output and input circuits shall meet the requirements of sections 3.2.1.2.3.a and 3.2.1.2.3.b of this standard, respectively. DES cryptographic equipment shall be capable of accepting key variables from key variable loaders which do not have or use the undesignated circuits.

3.2.1.2.3 Electrical Interface Characteristics. The electrical characteristics in this section apply at the DES cryptographic equipment connector used for electronic key variable entry. All electrical measurements are with respect to GROUND. Logic levels for the circuits are defined in table 3 and are compatible with commercially available 4000-series CMOS digital integrated circuits operated from a five-volt power source. The logic levels in table 3 shall be met for the following load conditions:

- a. **REQUEST.** The output voltage levels in table 3 shall be met when driving loads greater than 50 kohms with shunt capacitances less than 200 pF.
- b. **DATA and CLOCK.** These input circuits shall function properly when the input voltage levels in table 3 are applied to input loads greater than 200 kohms with shunt capacitances less than 50 pF.

3.2.1.2.4 Mechanical Interface Characteristics. DES cryptographic equipment shall be physically connected to a key variable loader via a cable, not to exceed one meter in length, using the type of nine-position connector specified in Federal Standard 1031 (based upon Electronic Industries Association standard RS-449). DES cryptographic equipment shall provide, via front panel access (under lock control), the female nine-position connector with latching blocks, for electronic key variable entry. The cable from the key variable loader shall use a matching male nine-position connector: one capable of latching. The position assignments for this connector are contained in table 4.

3.2.2 Parity. The parity of unencrypted DES key variables shall be verified during entry, whether manual or electronic, and during any subsequent transfer within DES cryptographic equipment, to ensure that no accidental single-bit modification of a key variable has occurred. Each group of eight bits shall be of odd parity, as defined in Federal Information Processing Standards Publication 46.

3.2.3 Zeroization. Any detected attempt to gain access to the internal components of DES cryptographic equipment, through disassembly of the equipment (e.g., removal of case), shall automatically zeroize the key variable and, in the Cipher Block Chaining mode, the Initializing Vector. All key variable storage locations, except those containing test key variables and encrypted key variables, must be capable of being zeroized. The ability to inhibit the zeroization feature shall be provided in the interior of equipment for maintenance. This inhibit feature must not be accessible until the equipment has been opened for maintenance. A means shall be provided to automatically disengage the internal inhibit

feature and zeroize the maintenance test key variable in the DES device before DES cryptographic equipment is returned to the operational mode. A means shall also be provided to ensure that DES cryptographic equipment is not able to encrypt and decrypt when in the zeroized state.

3.2.4 Key Variable Storage. After initial key loading, all unencrypted key variables shall be stored inside DES cryptographic equipment, in order to receive the protection associated with the security requirements of this standard. A means must be provided to assure that unencrypted key variables cannot visually or electrically be read out of DES cryptographic equipment. If key variables are read out of DES cryptographic equipment for purposes of transmission, they must be encrypted first. Key variables must be stored in erasable electronic storage (e.g., random access memory, shift registers, the DES device, etc.). DES cryptographic equipment must also have the ability to maintain their key variables whenever primary power is interrupted. Except for key variables residing in "final" locations (actual use or protection against power interruption) within DES cryptographic equipment, the appearance of a key variable in any intermediate storage location within DES cryptographic equipment must be only temporary (e.g., as a part of the key variable entry or testing process) and all such temporary storage locations must be zeroized upon transfer of the key variable to one of its "final" locations. The DES key variable, when routed internally within DES cryptographic equipment, shall be routed in such a manner as to prevent external access to the key variable, either inadvertently or due to the single failure of an electronic component.

3.3 Initializing Vector (IV). Initializing vectors can be produced using the DES algorithm, a key variable, and input data generated internally; or they can be derived from another random or pseudorandom source. New IV's shall be derived such that all possible IV's (N bits long) are equally likely (i.e., have a probable occurrence of 2^{-N}). A means shall be provided to assure the introduction of new initializing vectors following the loading of new key variables, return of primary power after a power interruption (except for in the Cipher Block Chaining encryption mode), or upon start-up after the DES device has been zeroized or reset (e.g., when the device is first brought into service or after a battery change). The following IV requirements also apply:

- a. An IV shall be used to initiate every ciphertext chain (see proposed Federal Standard 1026).
- b. When the Cipher Feedback encryption mode is used, the IV shall contain a minimum of 48 bits, may be transmitted unencrypted, and shall be newly generated for every ciphertext chain.
- c. When the Cipher Block Chaining encryption mode is used, the IV shall contain 64 bits, shall be encrypted prior to transmission, and need be newly generated only when a new key variable is entered into a DES device.
- d. When the Output Feedback encryption mode is used, the IV shall contain 64 bits, and may be transmitted unencrypted.

3.3.1 Initializing Vector Retention. Except in the Cipher Block Chaining mode, the last initializing vector used should be retained in storage during an interruption of primary power, if it is to be used to generate a new initializing vector upon resumption of operation. In the Cipher Block Chaining mode, the initial IV should be retained for reuse to eliminate the need to retransmit it securely.

3.4 Encryption Function and Alarms

3.4.1 Modes. Four modes of implementing the DES have been approved. These modes are described in detail in Federal Information Processing Standards Publication 81. The Cipher Feedback and Cipher Block Chaining modes are intended for encryption of narrative text and Automatic Data Processing (ADP) data, for transmission over communications channels. The Output Feedback mode is intended for applications where error extension due to encryption/decryption cannot be tolerated. The Electronic Codebook mode is approved for the encryption and decryption of Data Encrypting Keys (DEK's) and IV's, for transmission over telecommunication systems. Use of the Electronic Codebook mode for other purposes, and use of other encryption/decryption modes, shall be approved by the responsible U. S. Government agency, as designated in section 1.4.

3.4.2 Encryption Tests. DES cryptographic equipment shall be designed to provide for automatic testing of the encryption function, in addition to any other self-testing methods that are provided. To ensure that DES cryptographic equipment is not used to encrypt messages after it has failed, one of the following two methods shall be employed:

3.4.2.1 Method 1. Two DES key generators shall be used to do the same encryption of plaintext data. Their outputs shall be compared. Any difference between the outputs shall generate an alarm and shall cause the ciphertext output to immediately cease until operating personnel eliminate the error condition, or take such other action as may be prescribed by approved operational procedures. A means to automatically test the comparator circuits and associated inhibiting circuits (e.g., cause an intentional error) shall be provided.

3.4.2.2 Method 2. An acceptable alternative to the continuous comparison of the outputs of two key generators operating in parallel is the use of a single key generator whose integrity is verified by both of the following two tests (or just the S-box test if it is run at the frequency prescribed for the DES checkword test). These tests do not strictly meet the security objective stated in section 1.2.e, but they do serve to limit the transmission of data under critical failure conditions.

3.4.2.2.1 S-Box Test. This test consists of loading one or more known key variables (test variables) and one or more known 64-bit inputs into the transmit DES device and operating the DES key generator until all S-box entry combinations for each S-box have been applied. The final output(s) are then compared with all 64 bits of the known correct result(s) (determined previously, off-line, and stored in the equipment). If they fail to compare, an alarm shall be automatically generated and all ciphertext output shall be inhibited until operating personnel eliminate the error condition, or take such other action as prescribed by approved operating procedures. A means of automatically testing the comparator circuits and associated inhibiting circuits (i.e., cause an intentional error) shall be provided. (Descriptions of several S-box tests are contained in National Bureau of Standards Special Publications 500-20 and 500-61).

3.4.2.2.2 DES Checkword Test. After a new DES key variable is loaded into the DES cryptographic equipment, and after the S-box test has been performed, a known 64-bit input word is encrypted in the new key variable and the resulting 64-bit checkword is stored. This checkword shall be retained in storage and used until the new key variable is superseded. The DES checkword test consists of encrypting the known 64-bit input word in the current DES key variable and comparing the result with all 64 bits of the checkword. If they fail to compare, an alarm shall be automatically generated and the ciphertext output of the DES cryptographic equipment shall be inhibited until operating personnel eliminate the error condition, or take such other action as prescribed by approved operating procedures. A means of automatically testing the comparator circuits and associated inhibiting circuits (i.e., cause an intentional error) shall be provided. The S-box test may be used in place of the DES checkword test, if advantageous. When this is done, the S-box test must be run at the frequency prescribed for the DES checkword test.

3.4.2.3 Frequency of Testing. When two DES devices are operated in parallel (see section 3.4.2.1), the self-checking is continuous. When only one device is used with the S-box and DES checkword tests (see section 3.4.2.2), testing of the DES device is not continuous. In such an instance, the S-box test shall be accomplished to ensure correct operation of the device at the time of key variable entry, and the DES checkword test shall be accomplished prior to each use of an initializing vector. Automatic testing of the comparator circuits used in implementing method 1 or 2 (see sections 3.4.2.1 and 3.4.2.2) shall be performed when practical, but no less frequently than upon each DES key variable entry into the DES device.

3.4.3 Other Tests

3.4.3.1 Control Field Recognition. In automatic data processing and narrative text telecommunication applications, provision shall be made to verify that stand-alone DES cryptographic equipment can recognize implicit or explicit control fields signalling the start of encryption (e.g., START OF TEXT). A means of automatically testing the above-mentioned functions (i.e., cause intentional errors) shall be provided. When the control field recognition functions are tested, failure of DES cryptographic equipment to recognize and act upon these fields shall inhibit operation in the secure mode and generate an alarm. Provision may be made internal to DES cryptographic equipment to conveniently override this feature to facilitate maintenance. When the DES cryptographic equipment function is integrated into Data Terminal Equipment (DTE), and data is encrypted as a consequence of being processed within the DTE, the requirement to check the ability to recognize these control fields may not be necessary. In these cases, where the DTE provides but does not check the control field recognition function(s), the DTE design shall assure that data intended for encryption will always be encrypted and will never be transmitted unencrypted.

3.4.3.2 Chain Identification (CID), Manipulation Detection Code (MDC) and Message Authentication Code (MAC). In systems which utilize the CID, MDC, or MAC fields, an alarm shall be generated when the received MDC, CID, or MAC mismatches (i.e., does not compare) with the expected value. When DES cryptographic equipment is generating and checking the CID, MDC, or MAC fields and mismatch occurs, the DES cryptographic equipment shall generate an alarm. CID's shall not be repeated for a given key variable period. When DES cryptographic equipment is generating the CID, the equipment shall generate an alarm when the CID counter reaches its maximum value. In full-duplex and multidrop applications, provision must be made to assure that CID's are not duplicated by the various terminals. Details of the CID, MDC, and MAC fields are described in proposed Federal Standard 1026. DES cryptographic equipment (or a DTE or DCE providing the CID, MDC, or MAC functions) must also be capable of testing the comparator(s) used to compare a received CID, MDC, or MAC with the expected or locally derived value (e.g., cause an intentional error). If a CID, MDC, or MAC comparator fails its test, an alarm shall be generated, and operation in the secure mode shall cease.

3.4.3.3 Other Ciphertext-Inhibit Tests. In addition to the conditions described in section 3.4.2 and previous paragraphs in section 3.4.3, ciphertext output of DES cryptographic equipment is also inhibited by: (a) transfer of a DES key variable into a DES device, (b) zeroization of DES cryptographic equipment, (c) use of the test mode, and (d) use of a DES device for a function other than the encryption of plaintext data (e.g., generating an IV, computing an MAC). DES cryptographic equipment shall be capable of testing that the conditions described in (a), (b), (c), and (d) above are capable of inhibiting ciphertext output.

3.4.3.4 Parity Check Verification. DES cryptographic equipment and key variable loaders shall be capable of testing that DES key variables with improper parity can be detected.

3.4.3.5 Frequency of Testing. The ability of DES cryptographic equipment (and DTE's or DCE's providing the CID, MDC, or MAC functions) to recognize the control fields described in section 3.4.3.1, to perform the comparisons described in section 3.4.3.2, and to generate an alarm when an error or mismatch resulting from the use of these functions is detected, shall be checked at the same frequency required for the DES checkword test (see section 3.4.2.3). The MAC comparator shall be checked once per authenticated message. The tests described in sections 3.4.3.3 and 3.4.3.4 shall be performed at the same frequency as the S-box test.

3.5 Fail-Safe Design Requirements. DES cryptographic equipment design shall not contain potential single failures which could compromise DES key variables, or affect the initialization process. Specifically, DES cryptographic equipment design shall not permit potential single failure conditions which could result in: (1) transmission of the key variable, or any portion thereof, or (2) transmission in depth (reuse of the same IV) due to faulty or insufficient randomization. When firmware techniques are used to control the cryptographic functions described above, sufficient safeguards shall be incorporated to ensure proper operation of the firmware. (Note: Other critical areas (such as plain text handling, alarms, and alarm checks) that may be affected by undetected failures also deserve special consideration in design).

3.6 Test Mode. DES cryptographic equipment shall have a test mode which, when used, will assure that the equipment is operating as intended. At a minimum, the test mode shall perform an S-box test, when using Method 2 (see section 3.4.2.2), and test all security alarm circuitry. In the test mode, a test DES key variable(s) shall be used. The ciphertext output of DES cryptographic equipment shall be inhibited while in the test mode. However, a means may be provided for maintenance personnel to override the ciphertext output inhibit feature from inside the equipment. If the ciphertext inhibit override feature is implemented, a means shall be provided to automatically disengage the ciphertext inhibit override before DES cryptographic equipment is returned to the operational mode. DES cryptographic equipment shall prevent the test key variable from being used for encryption/decryption of actual plaintext/ciphertext data.

3.7 Control Functions. DES cryptographic equipment shall provide for the following controls under the conditions listed:

<u>NAME</u>	<u>FUNCTION</u>	<u>CONDITIONS</u>
POWER ON/OFF	Turns primary power (and internal battery) ON or OFF and causes zeroization of critical storage when in the OFF position. (See section 3.9.)	Optional feature. Lock not required.
STANDBY MODE	Provides the capability to render the DES device inoperable during unattended periods, without zeroizing the key variable. (See section 3.1.3.)	Required when equipment is not in continuous 24-hour a day operation. Must be under control of a lock.
ALARM RESET	Provides the capability to clear alarms after a fault has been corrected by repeating those security checks which could have generated the alarm condition. Performance of the security checks must be successful (i.e., the condition causing the alarm must have been corrected) before the alarm state can be exited. The ciphertext output shall be inhibited until the alarm state is exited.	Required on all equipment. Must be under control of a lock.
TEST MODE	Causes DES cryptographic equipment to perform tests contained in section 3.6 of this standard.	Required on all equipment. Must be under control of a lock.
LAMP TEST	Provides assurance that indicators are operable.	Optional feature. No lock required.
KEY VARIABLE ENTRY	Provides for external entry of DES key variable(s), either manually or automatically. (This does not include "down-line loading".) Ciphertext output shall be inhibited during entry of the key variables if the DES key variables are automatically placed in a DES device as a result of entry.	Required if external key variable entry devices are used. (See section 3.1.1)
BYPASS MODE	Provides the capability for bypassing the DES device and transmitting plain text when DES cryptographic equipment is in an alarm condition or other malfunction condition.	Optional feature. Must be under control of a lock.

SECURE MODE	Provides capability to transmit and receive cipher text.	Optional feature. Must be under control of a lock.
ZEROIZE	Provides capability to zeroize all unencrypted key variables (and IV in CBC mode).	Required feature on all equipment. No lock required.

NOTE: It is not necessary to provide individual locks for each control function. They may, for instance, be collocated (within the constraints of section 3.1.1 of this standard) behind a locked cover or gated by a physical key switch.

3.8 Status Indicators. DES cryptographic equipment shall provide for display of the following indications of status under the conditions listed below.

NAME	FUNCTION	CONDITIONS
POWER ON	Indication that proper electrical power is available for equipment operation.	Required only when power ON/OFF switch is used.
DES BYPASS	Indication that the equipment is not in the encipher/decipher state.	Required when BYPASS control is implemented.
TEST	Indication that DES cryptographic equipment is in a test mode, as opposed to an operational mode.	Required on all equipment.
BATTERY	Indicates whether the internal battery is operating properly and is capable of retaining critical storage.	Required when a battery is used as a backup energy source.
ALARM	Indication that an error in operation of the DES cryptographic equipment has occurred or that attempted tampering has been detected. Ciphertext output must be automatically and immediately disabled when an alarm occurs, if not in the bypass condition.	Required on all equipment.
AUDIBLE ALARM	Same as ALARM.	Optional feature. Not a front panel indicator. A dry contact relay type of interface shall be used and should be available on the rear of the equipment.
PARITY	Indication that an error in parity has occurred during DES key variable entry or during internal transfer of the key variable. Further internal key variable transfers shall be inhibited until the condition which caused the error is corrected and a correct key variable has been entered.	Required on all equipment.

3.9 Retention of Critical Storage. Critical storage (e.g., key variable final storage location(s), CID's, IV's, and test data) in DES cryptographic equipment shall be retained during primary power interruptions. DES cryptographic equipment shall have a means of determining whether critical storage has been properly maintained during interruption of primary power.

3.10 EMI/EMC Requirements. DES cryptographic equipment shall be designed and constructed to meet the Electromagnetic Interference/Electromagnetic Compatibility (EMI/EMC) requirements of MIL-STD-461B for class A-3 equipment. Good EMI design practices should be followed in all aspects of the DES cryptographic equipment design. DES cryptographic equipment shall comply with the test requirements of MIL-STD-462 as specified below in all operating modes:

<u>TEST</u>	<u>REQUIREMENT</u>
CE01	Narrowband measurements only required; limits specified in figure 4-1, curve 1, for Direct Current (DC) and Alternating Current (AC) power leads and control and signal leads.
CE03	Figure 4-4, curve 1, broadband, and figure 4-3, curve 1, narrowband, apply for DC and AC power leads and control and signal leads.
RE01	Figure 4-11 applies with the following modification: The limit from 3 kHz to 50 kHz shall be 60 dB above 1 pT.
RE02	Figure 4-12, narrowband, and figure 4-13, broadband, apply.

4. Deviations and Changes to Federal Standard 1027. When a Federal Agency considers that this standard does not provide for its essential needs, a statement citing inadequacies shall be sent in duplicate to the General Services Administration (GSA), Washington, DC 20405. The General Services Administration and the preparing activity, in accordance with Federal Property Management Regulations 41 CFR 101-29.3, will determine the appropriate action to be taken and will notify the agency. Manufacturers and suppliers may contact the preparing activity for information regarding procedures for requesting approval for equivalent methods to be used, to meet the requirements of this standard. Supplementary guidance concerning requests for such approval is being provided in a revision to Federal Property Management Regulation 41, Code of Federal Regulations 101-35.3.

PREPARING ACTIVITY:

Communications Security Organization
National Security Agency
9800 Savage Road
Fort George G. Meade, MD 20755

MILITARY INTERESTS:

Military Coordinating Activity NSA -- NS

Custodians
Army -- SC
Navy -- EC
Air Force -- 02

Review Activities

Army -- AD, CR
Navy -- AS, OM
Air Force -- 90
DCA -- DC
TRI-TAC -- TT
DLA -- DH

User Activities Navy -- SH, MC

This document is available from the General Services Administration (GSA), acting as agent for the Superintendent of Documents. A copy for bidding and contracting purposes is available from GSA Business Centers. Copies are for sale at the GSA Specification Unit (WFSIS), Room 6039, 7th and D Streets S.W., Washington, D.C. 20407; telephone (202) 472-2205. Please call in advance to arrange for pickup service.