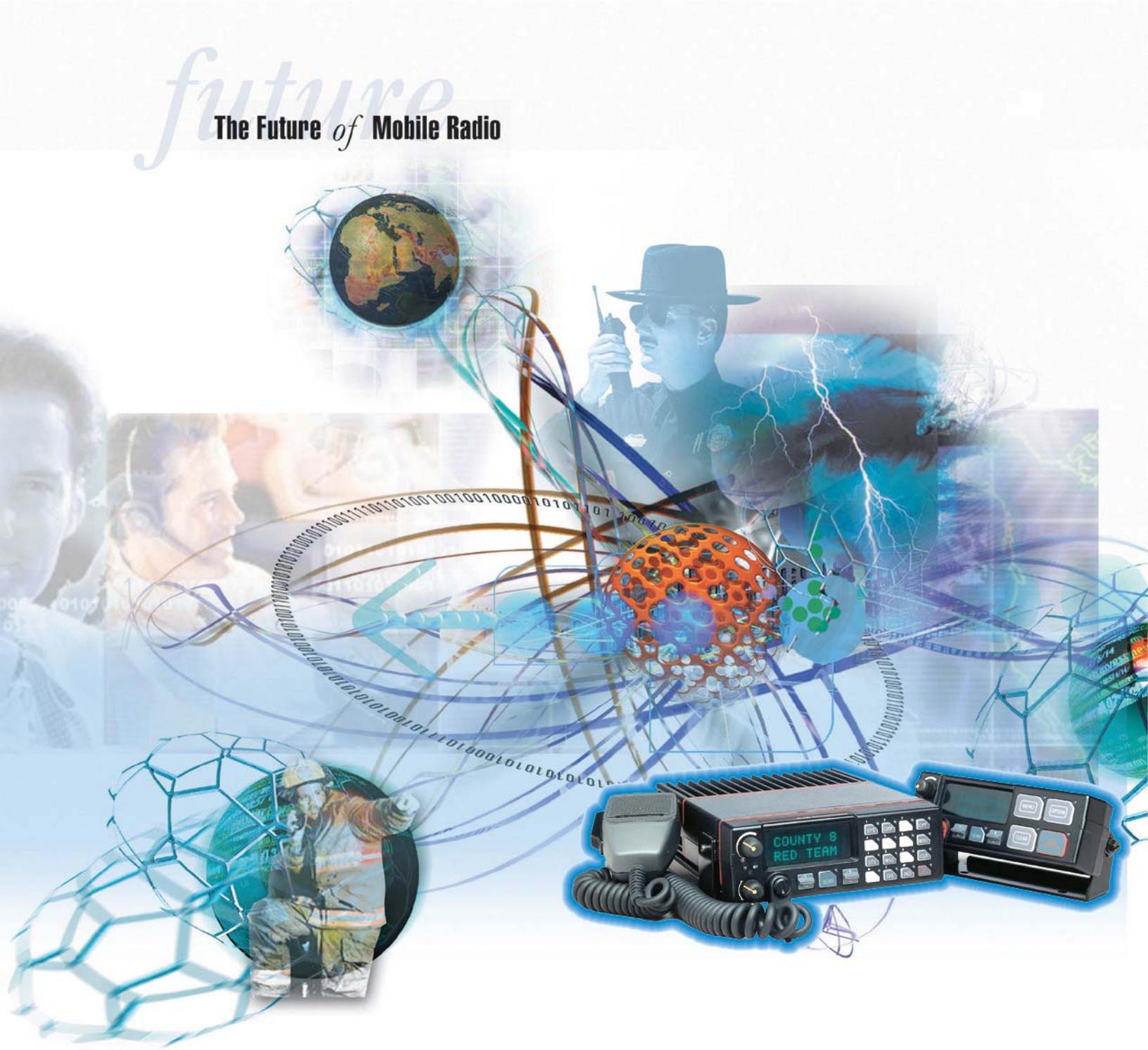


EDACS® ProVoice™ Orion™ System/Scan Mobile

Two-Way FM Radio, 806-870 MHz

tyco Electronics

M/A-COM

The voice coding technology embodied in this product is protected by intellectual property rights including patent rights, copyrights, and trade secrets of Digital Voice Systems, Inc. The user of this technology is explicitly prohibited from attempting to decompile, reverse, engineer, or disassemble the Object Code, or in any other way convert the Object Code into human-readable form.

NOTICE!

This manual covers M/A-COM, Inc., products manufactured and sold by M/A-COM, Inc.

EDACS and Voice Guard are registered trademarks and ProVoice and Orion are trademarks of M/A-COM, Inc.

IMBE is a trademark of Digital Voice Systems, Inc.

TORX is a registered trademark of Textron, Inc.

This manual is published by **M/A-COM, Inc.**, without any warranty. Improvements and changes to this manual necessitated by typographical errors, inaccuracies of current information, or improvements to programs and/or equipment, may be made by **M/A-COM, Inc.**, at any time and without notice. Such changes will be incorporated into new editions of this manual. This manual may be reproduced in its entirety and without modifications for informational purposes only.

TABLE OF CONTENTS

Page

1. INTRODUCTION 4

2. SCOPE 5

3. CRYPTOGRAPHIC BOUNDARY 6
3.1 C57 Digital Signal Processor (DSP) 6

4. PHYSICAL SECURITY 7

5. MODULE DESCRIPTION 8
5.1 MODULE COMPONENTS 8

6. SOFTWARE/FIRMWARE CAPABILITIES 10
6.1 RADIO CONTROL PROCESSOR (RCP) 10
6.2 INTERRUPT CONTROL PROCESSOR (ICP) 10
6.3 C57 DSP (ADI) 10
6.4 FIRMWARE 10

7. ROLES AND SERVICES 11
7.1 CRYPTO-OFFICER ROLE 12
7.2 USER ROLE 12
7.2.1 Transmit/Receive 12
7.2.2 Zero DES keys 12
7.2.3 Display DES key index 12
7.2.4 Bypass Mode 13
7.3 STATUS FUNCTIONS 14
7.4 KEY MANAGEMENT 14
7.5 TABLE OF SERVICES 14

8. SECURE OPERATION 16
8.1 CLEAR, DIGITAL, AND PRIVATE OPERATION 16
8.1.5 Clear Mode (Analog) 16
8.1.6 Digital Mode (IMBE) 16
8.1.7 Private Mode (IMBE DES) 17
8.1.8 Receiving An Encrypted Call 17
8.1.9 Transmitting An Encrypted Call 17

9. SELF TESTS 18
9.1 ERROR MESSAGES 19
9.2 RESUMING NORMAL OPERATION 22
9.3 OPERATOR INTERVENTION 22
9.4 STATUS 23
9.5 CRYPTOGRAPHIC TEST 23
9.6 CRITICAL FUNCTION TEST 26

10. GLOSSARY 27

1. INTRODUCTION

The ProVoice™ Orion™ System/Scan Mobile Two-Way FM radios (hardware version D28LPXE (12W) and D28MPXE (35W); firmware version LZY 213 773/91 Rev. 43A) are high-quality, high performance FM radios. Both radios (System and Scan) are identical except in the control head attached to the front of the radio. The System version has a 16-key keypad and Liquid Crystal Display (LCD) while the Scan version has a 4-key keypad and LCD. The purpose of this document is to provide the required documentation to the validating agency for FIPS 140-2, Level 1 validation. The Orion radio is a multi-chip stand-alone module.

The Orion radio is synthesized and operates in both trunked (EDACS®) and conventional communications systems. Trunked mode allows selection of either a communications group or an individual radio within a system. Both the selected group and the individual radio are secured through IMBE™ digital signaling and DES encryption.

Trunked operation is a set of radio frequency channels used by multiple user groups. By using high-speed digital data, the radio goes to an unused channel when a call is initiated and will only respond to calls in the same user group. In this way, conversation privacy between user groups is assured. This operation is very similar to a cellular phone call.

Conventional operation is communicating on radio channels allocated for conventional use. Conventional operation is allocating a radio channel (transmit/receive) for conventional (non-trunked) use that can be manually selected by the operator. The user selects a channel and directly communicates on that channel. A channel is a transmit/receive radio frequency pair. This could be considered the “Walkie-Talkie” mode.

A trunked group consists of several users with a common group identification (GID). A radio may have several groups but the selected group determines whom the unit can call at any specific time.

In trunked mode, a set of groups, which communicate on a set of channels, is called a system. In conventional mode, a system is a set of channels. A system can consist of all trunking groups and channels, all conventional channels, or a mixture of both trunked and conventional.

2. SCOPE

This document defines the security policy for the Orion System/Scan mobile radio. This policy defines the cryptographic module, crypto-officer roles, user roles, and key management functions.

3. CRYPTOGRAPHIC BOUNDARY

The cryptographic boundary of the Orion radio is defined as the entire radio. This includes the physical housing, Control Unit, and Control Logic Board CMC-682. The Synthesizer/Receiver/Exciter, Power Amplifier, PA Interface, and IF sections are only used to transmit and receive and perform no cryptographic functions. Thus, they are excluded from the security requirements.

The Control Logic Board, CMC-682, includes CMOS Microprocessors IC701 and IC702, which are part of a microcomputer circuit. For a circuit overview refer to Maintenance Manual LBI-39072. For detailed circuit analysis of the microcomputer, including memory devices and major functions, refer to Maintenance Manual LBI-38902.

3.1 C57 Digital Signal Processor (DSP)

Circuit analysis of IC710, the C57 Digital Signal Processor (DSP), is not in the detailed analysis in the maintenance manual but is provided here as follows:

DSP chip IC710 performs speech digitization, IMBE speech compression, and optional decryption for ProVoice-equipped Orion radios. The DSP communicates with the H8/532 microcomputer IC701 through its 8-bit port D0-D7, which is connected to the data bus. The WR, RD, DSP CS, DES CS, and REGSEL signals control access to the ADP registers. The DP PWR and DP RST inputs are controlled by digital signals from the ASP. Setting DP RST low resets the ADSP chip. Setting DP PWR low places the ADSP chip in a low power state during the standby mode. The FLOAT output provides an active-low interrupt to the H8/532 microprocessor when speech data is available in the transmit mode or requested in receive mode.

Microphone audio from the ASP is applied to VG TX where it is digitized by the analog-to-digital converter within the ADSP. Received digital audio is converted to audio by a digital-to-analog converter within the ADSP and output differentially on the SPKR1 and SPKR2 output pins.

DSP IC710 contains both ***R***ead-***O***nly-***M***emory ***(ROM)*** and ***R***andom-***A***ccess-***M***emory ***(RAM).*** At power-up, the H8/532 loads the DSP RAM. This software is stored separately in the Flash E^2PROM along with the H8/532 operating software and radio personality. The software installed in Flash E^2PROM is specific to the encryption algorithm installed *(including un-encrypted IMBE),* and must match the options enabled in the software feature data for proper operation.

4. PHYSICAL SECURITY

The Orion radio is a Multi-Chip Stand-Alone module. This was concluded because the Orion radio consists of five modules: Control Unit, Synthesizer/Receiver/Exciter, Power Amplifier, PA Interface, and Control Logic/IF Board. The Control Unit (System or Scan) provides control functions and status information for the radio. Control is provided through a keypad, rotary channel switch and volume control with an off/on switch. Status information is provided by the LCD, LEDs, and keylights. The Synthesizer/Receiver/Exciter is a printed circuit board which has multiple IC chips interconnected to provide transmit and receive functions for the radio. The Power Amplifier and PA Interface provide power to the Orion radio. The Control Logic/IF Board is a printed circuit board, which has multiple IC chips interconnected to provide control logic (software driven) and intermediate frequency support for the transmit/receive functions. The Control Logic board has four interfaces, one to the synthesizer, one to the PA, one to the Option and Remote Control Connector (ORCC), and one to the Control Unit. All of these component parts, synthesizer, PA, ORCC, and Control Unit interfaces are enclosed for protection inside of the radio housing. This arrangement clearly meets the requirements for a multi-chip stand-alone module as described in the fundamental characteristics of physical embodiments as stated in the FIPS 140-2 vendor requirements document. The Orion radio module is intended to meet the security Level 1 approval.

The physical security mechanisms include:

- Passivation - All IC chips used in the Orion radio are standard devices of production-quality and commercial-grade specifications to meet M/A-COM's requirements. M/A-COM's requirements equal or exceed typical passivation specifications for power, temperature, reliability, shock/vibration, etc.
- Enclosure - or radio housing consists of a Control Unit (or Front Cover for Remote Type), Synthesizer/Receiver/Exciter Top Cover, Bottom Cover, and shields. The Covers are removable by backing out four captive screws. This procedure requires the use of a TORX® screwdriver *(M4)*.
- Tamper Protection - No critical security data *(cryptographic keys)* are accessible or downloadable as a result of tampering.
- Probe-Protected Ventilation Holes - The radio is sealed with no ventilation holes available for a probe to penetrate.
- Environmental Protection - The Orion radios are designed to meet MIL-810D & E specifications for wind driven rain. All access to the Orion radio is protected from water entry by suitable gaskets and seals. However, degradation due to use or disassembly during repairs, can affect the integrity of the seals as provided by factory assembly. A maintenance procedure is provided in the Service Section to assure that the radio housing will continue to meet the weatherproof features as designed.

5. MODULE DESCRIPTION

The Orion DES mobile radio can be divided into five main modules; Control Unit, Synthesizer/Receiver/Exciter, Power Amplifier, PA Interface, and Control Logic/IF Board. These are described in the following sections.

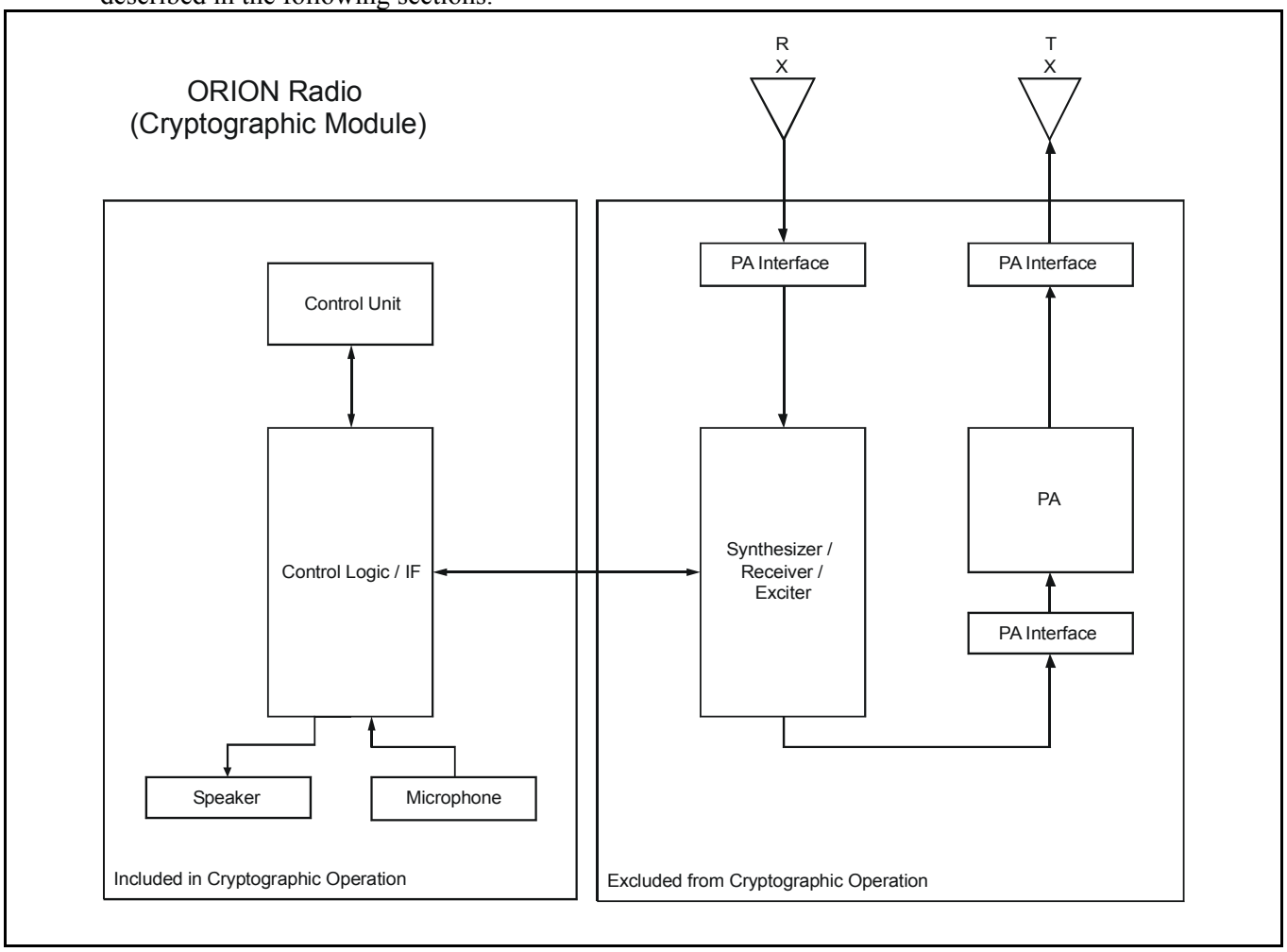


Figure 5-1: Orion Block Diagram

5.1 MODULE COMPONENTS

The Orion contains five modules; Control Unit, Synthesizer/Receiver/Exciter, Power Amplifier, PA Interface, and Control Logic/IF Board. The function of each will be described below:

Control Unit – the Orion has a SCAN and System Control Unit available. The Control Unit provides the user interface to the product. It allows input via keys, switches, and knobs. It provides output via the LCD and keylights. This unit is included as part of the cryptographic operation because it is the only mechanism for the User and Crypto-Officer to control the radio and receive status.

Control Logic/IF Board – this board is used for logic control, IF, and audio circuits. This module contains the H8 microcomputers, which run the main software for the radio, the ADI DSP, which performs the DES operations, the EEPROM, which stores the DES keys, microphone audio input, and

speaker audio output. This unit is included as part of the cryptographic operation because it performs all of the DES algorithms, stores keys, and provides all of the radio audio.

Synthesizer/Receiver/Exciter – this board provides circuits for the synthesizer, receiver, and transmitter. This board generates the frequencies that allow the Orion to operate at VHF, UHF, or 800 MHz. Even though this board is part of the Orion radio, it is being excluded from the cryptographic operation because it has nothing to do with the DES operation. This board allows the radio to transmit and receive signals but it has no knowledge of the content of those signals.

Power Amplifier – the PA provides transmit output power for the Orion. The exciter located on the Synthesizer/Receiver/Exciter board provides a low-level input to the PA. The PA will then generate anywhere from 12 to 110 watts of output power depending on the type of Orion and frequency band. . Even though this module is part of the Orion radio, it is being excluded from the cryptographic operation because it has nothing to do with the DES operation. This module provides transmit output power for the Orion and has no knowledge of the content of the signals it is amplifying.

PA Interface – this module is a board that provides numerous connections for the Orion. These connections include power, speaker, and other interconnections between boards. Even though this board is part of the Orion radio, it is being excluded from the cryptographic operation because it has nothing to do with the DES operation. This board connects signals between Orion modules but it has no knowledge of the content of those signals.

6. SOFTWARE/FIRMWARE CAPABILITIES

The Orion contains numerous firmware and software components. All of the associated hardware can be found on the schematics.

6.1 RADIO CONTROL PROCESSOR (RCP)

The RCP S/W is the main Orion S/W, which resides both in ROM and FLASH memory. This S/W controls the entire operation of the radio. It is the master while all other S/W components are slaves. This S/W controls the User Interface, Transmitting and Receiving, Keyloading, Private Mode, Zeroizing Keys, and numerous other functions.

6.2 INTERRUPT CONTROL PROCESSOR (ICP)

The ICP S/W is the slave S/W that responds to RCP commands. It controls such functions as read/write digital and analog I/O, serial port control, keypad scanning, synthesizer loading, and channel guard encode/decode. It is very low-level hardware control that notifies the RCP via interrupts whenever something happens. This S/W is not essential to the cryptographic module and its' operation.

6.3 C57 DSP (ADI)

The ADI S/W resides in the DSP ROM and RCP FLASH memory. The FLASH portion is downloaded at power up to the DSP RAM memory. This S/W, under the control of the RCP, performs A/D and D/A conversions on the user's voice for transmit and receive operations. The A/D and D/A conversion is performed using an algorithm known as IMBE. Also, the DSP S/W executes the DES algorithm on the digital voice to encrypt or decrypt. It receives the encryption key from the RCP. The DES algorithm has already been validated and received FIPS approval.

6.4 FIRMWARE

The ASIC (Modem), Audio Signal Processor (ASP), and Control Head are considered firmware. The S/W in these devices is very low-level hardware control that is performed via latch, relay, and register reads and writes. This S/W is not essential to the cryptographic module and its' operation.

7. ROLES AND SERVICES

There are two separate roles in the operation of the Orion DES radio: Crypto-Officer and User. The Orion DES radio can be used by anyone requiring secure two-way dispatch communications. This would include police officers, firemen, utility workers, etc. The group purchasing the radios would be the users and someone within the group would be designated as the technical liaison (Crypto-Officer). For example, the local police department buys 500 Orion DES radios. The police would have a Crypto-Officer program all 500 radios and load the appropriate DES encryption keys. The radios would then be installed into 500 Police cars (Users). The Crypto-Officer may setup DES talkgroups for Undercover work, Narcotics, Traffic Control as well as a global DES talkgroup so everyone can communicate together.

The User and Crypto-Officer do not require authentication to operate the Orion radio. Anyone can be a User or Crypto-Officer. It is strictly up to the owners of the product to control.

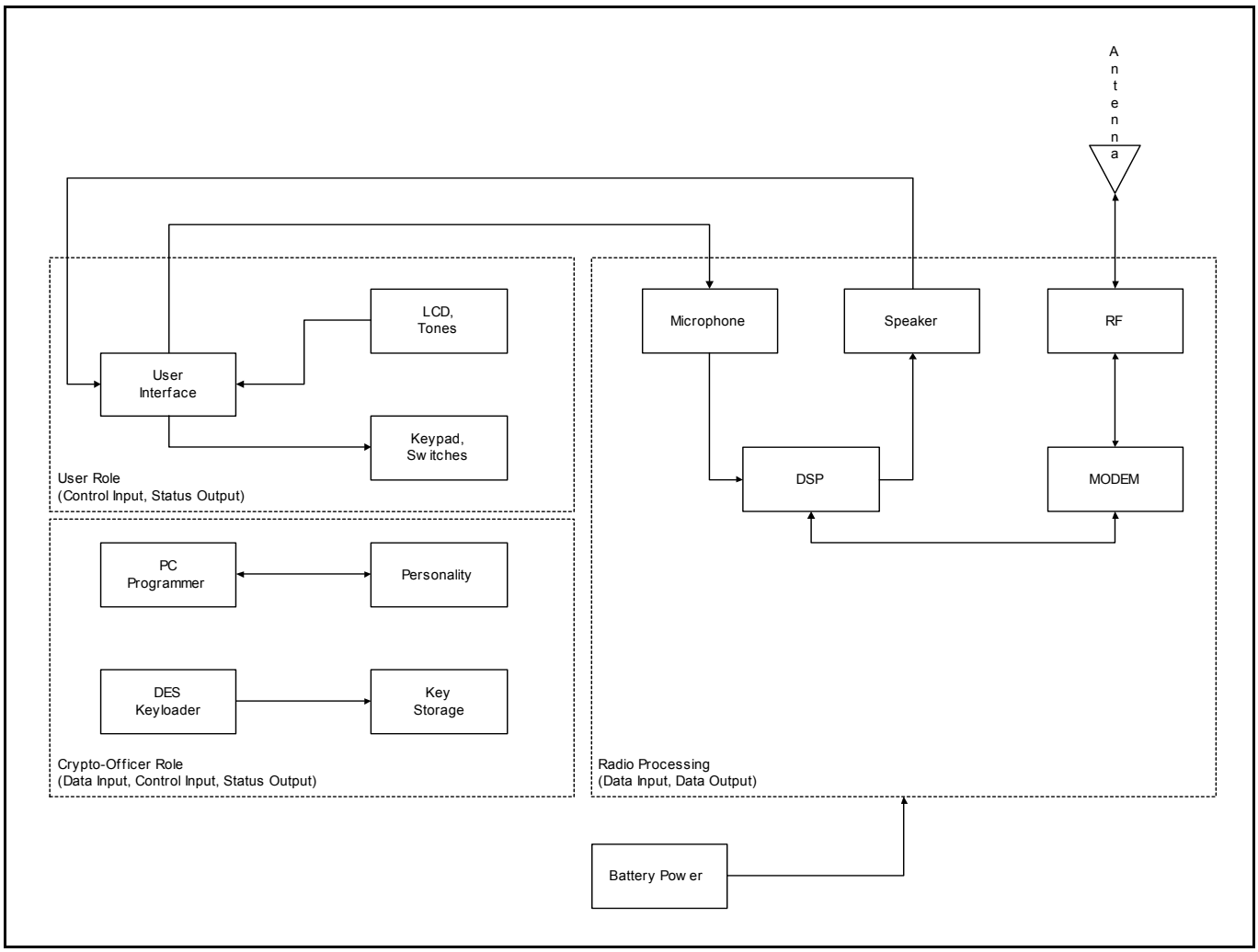


Figure 7-1: User and Crypto-Officer Roles

7.1 CRYPTO-OFFICER ROLE

A Crypto-Officer can perform the following services:

- Program Radio Personality
- Program DES Encryption Keys

The Orion DES Radio Personality is created on a PC using the program, *EDACS4* or *PC Programmer*. This personality contains numerous items including which talkgroups will be clear, IMBE-clear, and IMBE DES. It defines what encryption keys will be used on what systems and groups. Basically, it defines everything from the default system to protocol timeouts. The personality can be read or written to the Orion through the serial port connector.

The DES Encryption Keys are created and loaded into the radio using the DES Keyloader. This is a separate device, which programs the keys into the Orion's EEPROM through the serial port connector. The keys are 8 bytes long and must contain the correct parity. They can't be read out of the radio once they are programmed. DES radios require a DES Keyloader (Option V4025 with software version 3.N or later).

7.2 USER ROLE

A User can perform the following services:

- Transmit Conventional Clear/Private
- Receive Conventional Clear/Private
- Transmit EDACS Clear/Private
- Receive EDACS Clear/Private
- Zeroize Encryption Keys
- Display Encryption Key Index
- Bypass Private Mode

7.2.1 Transmit/Receive

The User must first select the system they will be communicating on; conventional or EDACS trunked. Next, they select the talkgroup they will be communicating with. When a call on that group is received it will automatically be heard in the speaker. To transmit a call, the user presses PTT (Push to Talk) button and speaks into the microphone. For a complete description of transmitting and receiving clear or private calls see section ***SECURE OPERATION.***

7.2.2 Zero DES keys

The user can zeroize the encryption keys at anytime by pressing the CLR (Clear) button and the OPT (Option) button on the radio keypad simultaneously. The user first hears a warning tone indicating the keys are about to be zeroized and then a solid tone is heard indicating the keys are now zero.

7.2.3 Display DES key index

The user can display the current encryption key index in use by the talkgroup and system. The Orion stores the DES encryption keys in banks. There are 8 banks possible with 7 keys per bank for a total of

56 DES keys, which can be stored in the radio. The bank and key index are set via radio personality. The user can display the current key index, 1-7, but not the actual key data.

7.2.4 Bypass Mode

The user can bypass crypto processing by turning off private mode. Private mode means the radio is ready for crypto processing and is indicated by the PVT keylight. The user can turn off private mode by pressing the PVT radio button and watching the PVT keylight turn off. In bypass mode, the transmitted microphone audio is digitized using the IMBE vocoder but no crypto processing is performed. Bypass mode can be specified using radio personality for a particular communication group, individual, or system. When the radio is configured to operate on one of these groups, the PVT keylight automatically turns off enabling bypass mode.

Mode Transition:

Figure 7-2 shown on page 13 indicates how the radio changes from crypto (or private) mode into bypass mode. First, the user initiates the change by pressing the PVT button or changing the system, group, or channel. Then, a second check is made to make sure crypto mode is not forced and that auto selecting the mode is allowed.

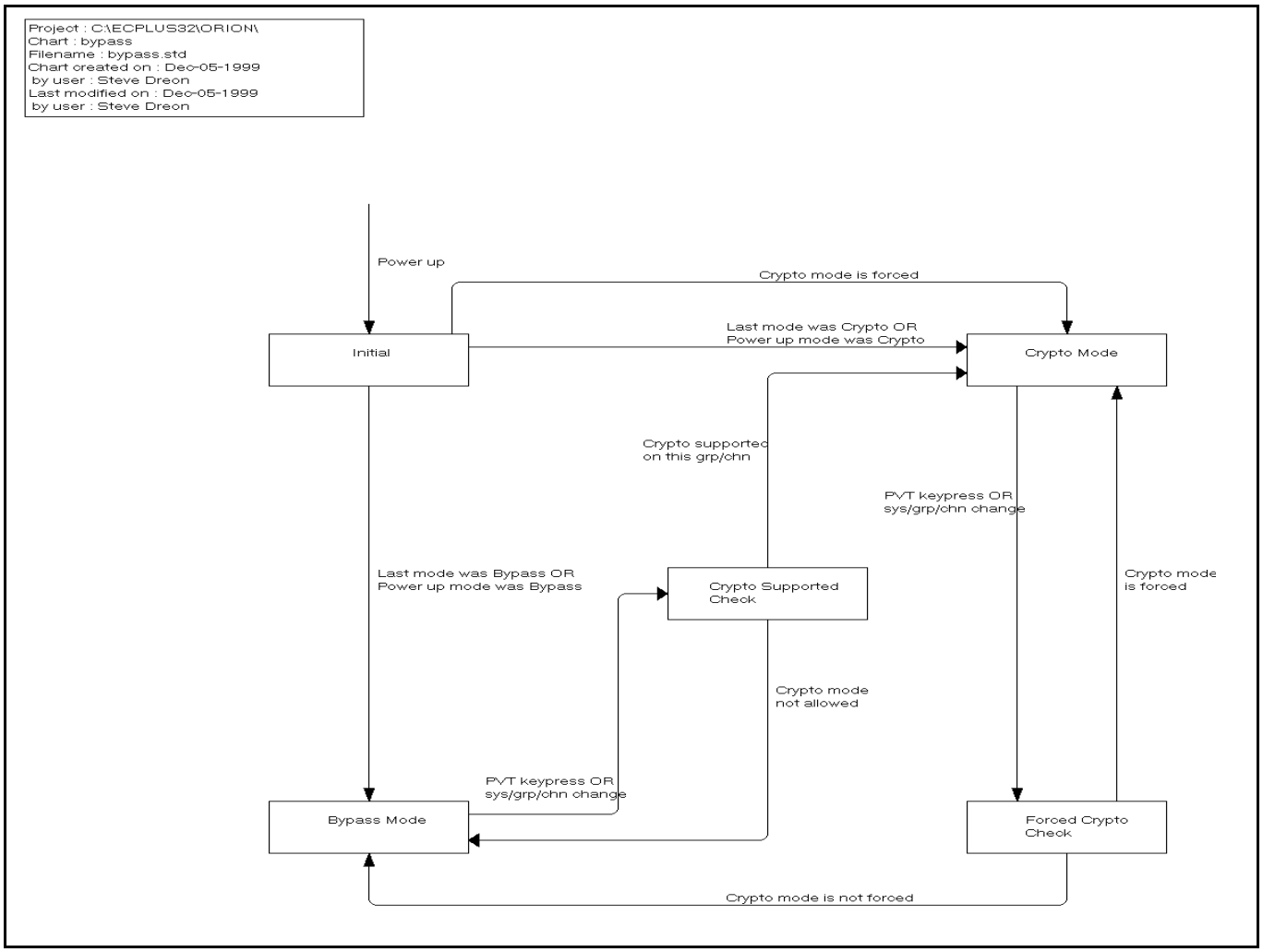


Figure 7-2: ByPass Mode

7.3 STATUS FUNCTIONS

Status information is displayed to both the Crypto-Officer and User via the 2x8 LCD, keylights, and alert tones. Refer to the EDACS Orion Mobile Radio Operator's Manual for details.

7.4 KEY MANAGEMENT

As stated under the Crypto-Officer Role, the DES keys are loaded into the radio in plaintext using a DES keyloader by the Crypto-Officer. The Crypto-Officer performs the following steps to load DES encryption keys:

- Connect the keyloader to the radio via the extended options connector.
- Turn the radio on and use the menu to select KEYLOAD.
- The Orion will display KEYLOAD, BANK=1 on the LCD. Use the arrows keys to select bank 1-8.
- The keyloader can transfer 1 key or all 7 keys to the selected bank.
- After the keys are loaded, disconnect the keyloader and press the CLR (Clear) button to resume normal operation.

The keybanks provide additional security to the users. For example, the Orion might be programmed with two EDACS trunked systems; EA and EB. EA could use bank 1 and EB could use bank 2. EA and EB are actually the same system on the same frequencies. The users could alternate between the two systems on a daily basis or permanently switch to EB if they felt EA was no longer secure.

The DES keys are 8 bytes long and are stored in EEPROM with a 2 byte CRC for a total length of 10 bytes per key. The keys are stored in plaintext but hidden with a random pattern every time the keyloader is attached. This technique makes it very difficult to determine the exact location of the keys in EEPROM.

7.5 TABLE OF SERVICES

SERVICES	INPUTS	OUTPUTS	USER	CRYPTO-OFFICER
Encryption	PTT, microphone audio, encryption key	Encrypted speech and messages	X	
Decryption	Received encrypted message, encryption key	Speaker audio	X	
Key Entry	Keyloader device, key selection	Encryption keys stored in radio		X
Key Zeroization	CLEAR/CLR and OPTION/O buttons	Encryption keys erased in radio		X
Audit Key Entry	Key selected during key loading	Encryption key with *"odds-one"* parity		X
Status: Active Role	Operational state of radio, radio personality, encryption keys	Transmit/receive (TX/BSY), private mode (PVT) keylight, communication group and system	X	
Status: Cryptographic State of Module	Radio personality, encryption keys, power up test	"DSP ERR" if power up test failed, "NO KEY" if encryption key error, otherwise no indication is given if crypto module is fully	X	

		operational		
Status: Error State	Power up test	See errors above	X	X
Status: Bypass	Radio personality, operational state of radio, radio PVT button	PVT keylight on indicates bypass mode is off, PVT keylight off indicates bypass mode is on	X	
Cryptographic Bypass	Radio personality, operational state of radio, radio PVT button	Transmit and receive audio and messages without encryption when bypass mode is active	X	

8. SECURE OPERATION

8.1 CLEAR, DIGITAL, AND PRIVATE OPERATION

Each system *(trunked or conventional)* is programmed for either ProVoice or Voice Guard (VG) communications. VG is an earlier generation algorithm that was replaced by IMBE and is only mentioned in this document because it appears in the Radio Personality as an option. IMBE programmed systems have three different voice modes: Clear *(analog),* Digital (*IMBE, not private*), and Private (*IMBE DES*). The voice modes are programmed on a per-group basis within each trunked system and on a per-channel basis within each conventional system. The following table shows the Transmit/Receive Mode compatibility:

GROUP/CHANNEL PROGRAMMING (TRANSMIT)	CLEAR RECEIVE	DIGITAL RECEIVE	PRIVATE RECEIVE
CLEAR	Yes	No	No
DIGITAL	Yes	Yes	No
PRIVATE	Yes	No	Yes (with proper cryptographic key)

8.1.5 Clear Mode (Analog)

Clear mode is when the radio transmits and receives only clear *(analog)* voice signals. These analog signals are non-digitized and non-encrypted. Clear mode transmissions can be easily monitored by unauthorized persons. Groups or channels programmed for clear operation cannot transmit or receive Digital or Private messages. In this mode, the radio is operating in cryptographic bypass mode.

8.1.6 Digital Mode (IMBE)

Digital mode allows the radio to transmit and receive digitized voice signals. IMBE digital signals provide improved weak signal performance and cannot be easily monitored with a standard receiver. Groups and channels programmed for IMBE digital operation transmit only digital signals. Private calls cannot be received or transmitted when the radio is in the Digital mode because the radio does not know the cryptographic key used. Message trunked group calls and individual calls will be answered back in the mode they were received, assuming the call or hang time is still active. Individual, phone, broadcast, and emergency calls will be transmitted clear if Digital mode is disabled or inoperative.

1. If receiving an analog message trunked call, the radio will respond in the analog mode during the hang time on the working channel.
2. If receiving an analog individual call (I-Call), the radio will respond in the analog mode during the hang time.
3. When using the "WHC" feature to respond to an I-Call (after the hang time has timed out), the call will be transmitted in the mode defined by the system mode as programmed for the current system if the ID being called is not in the I-Call list. If the ID is in the I-Call list, then the call will be transmitted as defined by the I-Call mode programmed in the list for that ID. For example, if you receive an I-Call from someone already stored in your Orion's Personality, you will call them back in the mode (Clear, Digital, Private) they are configured for in your radio. If they are not stored in your Orion's Personality, you will call them back in the mode your current system is configured for.

In this mode, the radio is operating in cryptographic bypass mode.

8.1.7 Private Mode (IMBE DES)

Private (cryptographic) mode allows the radio to transmit IMBE DES encrypted messages and receive clear or private transmissions. The radio will transmit private if the group/channel is programmed for private operation and forced operation is pre-programmed.

If the radio was pre-programmed for autoselect, the radio will transmit in the following modes:

- Private mode enabled, transmission always in private mode.
- Private mode disabled and private call received. Reply transmission will be private mode if made during scan hangtime. If reply transmission occurs after scan hangtime, transmission will be in clear mode.

When operating on a group or channel programmed for private mode, all transmissions will be private transmissions and the radio will receive clear and private signals. The PVT keylight (System Model) or OPTION keylight (Scan Model) turns ON when the private mode is enabled. If the selected group or channel is programmed for autoselect capability, the mode may be toggled between private and clear with the PVT button (System Model) or OPTION button (Scan Model). Radios programmed for forced private operation do not allow a change of the transmit mode. The user will see the message "FRCD PVT" indicating that forced private operation is active.

8.1.8 Receiving An Encrypted Call

When receiving, the radio automatically switches between clear or private operation. If the transmission being received is an encrypted transmission, it will be decrypted, the PVT keylight (System Model) or OPTION keylight (Scan Model) will flash, the receiver will unsquelch and the message will be heard in the speaker. For this to occur, the selected group or channel must be programmed for private operation and the correct cryptographic key must be loaded into the radio.

8.1.9 Transmitting An Encrypted Call

1. Select the desired group or channel.
2. Place the radio in private mode by pressing the PVT button (System Model) or OPTION button (Scan Model). When private mode is enabled, the PVT keylight (System Model) or OPTION keylight (Scan Model) will be ON.

   If the last state of the radio was private mode, the private mode will be enabled on power up. Also, the private mode will be enabled if forced operation has been programmed in the radio.

   If a group or channel is not programmed for private mode operation, "PVT DIS" will be displayed if an attempt is made to enable private transmit mode. It is not possible to operate on this group/channel in private mode.

   If the radio is programmed for forced private transmit operation, "FRCD PVT" will be displayed if an attempt is made to disable private transmit mode. It is not possible to transmit on this group/channel in clear mode.

   If the radio does not have the correct encryption key loaded, "NO KEY #" will be displayed and the call will not be transmitted.
3. Continue with standard transmission procedures. A private mode access tone will be heard when the PTT button is pressed.

9. SELF TESTS

All of the tests below are mandatory. There are no optional tests. Also, the only conditional tests are associated with the encryption keys. When the keys are manually entered into the Orion, they must pass a parity test. When the stored keys are used in the Orion, they must pass a CRC test.

Power-up tests

Software/Firmware tests

- 8k/32k RAM test
- 32k ROM Cyclic Redundancy Check (CRC)
- 256k/512k FLASH CRC

ADI S/W tests

- ADI File CRC is verified as stored in the Orion FLASH memory
- ADI program memory checksum is calculated at power up
- ADI data memory checksum is calculated at power up
- DES Known Answer Test (KAT) is performed at power up

BIOS Driver tests

- ASIC initialization
- ICP initialization
- ASP initialization
- E^2PROM initialization
- CHDOUT initialization
- CHDIN initialization
- RADIO initialization
- MODEM initialization
- EXTIO initialization
- SCI initialization
- ADI initialization

Critical Function tests

- Radio Personality is present with correct CRC
- Synthesizer is locked
- S/W Feature data is present with correct CRC
- Bypass Test

Conditional tests

- DES keys have a CRC that is verified as stored in the Orion EEPROM memory
- Manual entry of the DES keys requires passing a parity test
- DES keys require the algorithm to pass a Known Answer Test (KAT) before they are loaded

Error codes are divided into two categories:

1. Fatal operational error codes. These errors are displayed during normal radio operation or on the radio power up (Fatal System Errors). These errors will cause the radio to reset.
2. Non_fatal operational error codes. These errors are displayed during the normal radio operation or on the radio power up. The radio will not reset.

System Errors:

- Fatal system errors will cause the radio to display error message/code and then reset the radio to its starting operation. The reset condition will remain until the fatal error is corrected.
- Non fatal errors are displayed for a short period (about two seconds) then normal radio operation will resume.

9.1 ERROR MESSAGES

The errors are displayed on the radio display as follows:

message ERR=xxxx

where xxx is the error code and message is one of the messages listed below

ERROR MESSAGE	DESCRIPTION
HARDWARE	ROM errors
SOFTWARE	General software failure
TRACKING	tracking data fatal error
NO LOCK	Synthesizer not locking
FREQDATA	frequency data fatal error
PERSDATA	Radio Personality errors
	Non Fatal Errors
UNKNOWN	
FEAT ERR	S/W Feature data error
DSP ERR	DSP error

If either of the following error messages are displayed the radio was either programmed incorrectly or needs servicing:

DSP ERR ***ERR=XXXX***

DSP ERR

If the DSP H/W circuit is not responding, the following error message will be displayed and the radio needs servicing:

HARDWARE ***ERR= 30***

ROM Fatal system errors

ROM fatal errors may be corrected by cycling the radio power (turn it off then on). When the power cycle does not correct the problem the radio must be serviced.

ERROR NAME	MESSAGE	CODE	DESCRIPTION	ACTION
FATAL_RAM_ERROR	HARDWARE	2	8k RAM test error.	Return radio for service
FATAL_ROM_CHKSUM	HARDWARE	3	32k ROM CRC error	Return radio for service
FATAL_FLSH_CHKSUM	HARDWARE	4	Flash CRC error	Return radio for service
FATAL_ASIC_LOAD	HARDWARE	10	ASIC driver failed initialization	Return radio for service
FATAL_ICP_LOAD	HARDWARE	11	ICP driver failed initialization	Return radio for service
FATAL_ASP_LOAD	HARDWARE	12	ASP driver failed initialization	Return radio for service
FATAL_EE_LOAD	HARDWARE	13	EEPROM driver failed initialization	Return radio for service
FATAL_ICP_PORTINIT	HARDWARE	14	ICP digital I/O initialization failed	Return radio for service
FATAL_INTOUT_LOAD	HARDWARE	15	Standard input/output driver failed initialization	Return radio for service
FATAL_INTIN_LOAD	HARDWARE	16	Standard input driver failed initialization	Return radio for service
FATAL_RADIO_LOAD	HARDWARE	17	RADIO driver failed initialization	Return radio for service
FATAL_MODEM_LOAD	HARDWARE	18	MODEM driver failed initialization	Return radio for service
FATAL_EXTIO_LOAD	HARDWARE	19	External I/O driver failed initialization	Return radio for service
FATAL_SCI_LOAD	HARDWARE	20	Serial communication interface driver failed initialization	Return radio for service
FATAL_ICP_CHKSUM	HARDWARE	21	ICP prom checksum	Return radio for service
FATAL_ADI_NOACK	HARDWARE	30	ADI did not respond to command	Return radio for service
FATAL_ADI_QUNDERFLOW	HARDWARE	31	ADI rx circular queue underflowed	Return radio for service
FATAL_LCD_NOACK	HARDWARE	40	LCD did not ack message	Return radio for service
FATAL_LCD_HARD_FAIL	HARDWARE	41	LCD hardware is invalid	Return radio for service
FATAL_ICP_NOACK	HARDWARE	60	ICP did not ack message	Return radio for service
FATAL_EXTIO_ICPFAIL	HARDWARE	70	ICP failed in a fork	Return radio for service
FATAL_RADIO_ASPWRT	HARDWARE	80	Radio driver could not write to ASP	Return radio for service

Operational software Fatal system errors:

ERROR NAME	MESSAGE	CODE	DESCRIPTION	ACTION
RADC_PITD_ERROR	TRACKING	200	Radio Personality tracking data error.	Reprogram the tracking data
RADC_PIHW_ERROR	PERSDATA	201	Radio Personality hardware data error.	Reprogram the radio personality
RADC_FREQ_ERROR	FREQDATA	202	Radio Personality frequency data error.	Reprogram the radio personality
RADC_PITD_MALLOC_ERROR	SOFTWARE	203	Radio Personality tracking data malloc error.	Reprogram the tracking data
RADC_PITD_CKSUM_ERROR	SOFTWARE	204	Radio Personality tracking data checksum error.	Reprogram the tracking data
DACS_NO_LOCK	NO LOCK	300	Synthesizer did not lock or became unlocked.	Check the frequencies in the PC programmer and re-program the radio personality.
DACS_MODEM_FATAL_ERROR	SOFTWARE	301	Unable to correctly configure the modem for EDACS operation.	Reprogram the radio personality
CONV_NOLOCK_ERROR	NO LOCK	401	Synthesizer became unlocked.	Check the frequencies in the PC programmer and re-program the radio personality.
CONV_PERS_ERROR	PERSDATA	407	Conventional radio personality error.	Reprogram the radio personality
PI_NOPERS_ERROR	PERSDATA	500	Radio Personality data is not present.	Reprogram the radio personality
PI_CRC_ERROR	PERSDATA	501	Flash radio personality CRC did not match EEPROM.	Reprogram the radio personality
PI_DESC_CRC_ERROR	PERSDATA	502	Crucial radio personality data has in-correct CRC.	Reprogram the radio personality
UI_FATAL_DEVICE_NOTSUPPORTED	PERSDATA	609	I/O device type (from personality) not supported.	Reprogram the radio personality
AEGIS_KEYLOAD_ERROR	SOFTWARE	804	General keyload error has occurred.	Reprogram the radio personality
AEGIS_KEYLOAD_NOTABL	SOFTWARE	806	No key table was found in eeprom.	Reprogram the radio personality
AEGIS_KEYLOAD_BADSIZE	SOFTWARE	807	Key table is wrong size in eeprom.	Reprogram the radio personality

AEGIS_KEYLOAD_CORRUPT	SOFTWARE	808	Key table has been corrupted.	Re-program the personality and reload encryption keys.

Operational software Non-Fatal system errors:

ERROR NAME	MESSAGE	CODE	DESCRIPTION	ACTION
PIFEAT_SNR_ERROR	FEAT ERR	550	S/W Feature Data - Cannot read radio ROM serial number.	Service radio and replace SNR.
PIFEAT_READ_ERROR	FEAT ERR	551	Radio Personality S/W feature data read failure or data not available.	Service radio and replace SNR.
PIFEAT_CRC_ERROR	FEAT ERR	552	Radio Personality S/W feature data CRC failure.	Re-program the radio personality.
RI_DSPDOWN_NOATTEMPT	DSP ERR	850	DSP not found. Radio does not support private operation.	Re-program the ADI file.
AEGIS_ADIDOWN_NOTFOUND	DSP ERR	851	DSP file not found.	Re-program the ADI file.
AEGIS_ADIDOWN_CRCFAIL	DSP ERR	852	DSP file is corrupted.	Re-program the ADI file.
AEGIS_ADIDOWN_ENCERR	DSP ERR	853	S/W feature data does not match DSP file.	Re-program the radio personality.
AEGIS_ADIDOWN_PMFAIL	DSP ERR	854	DSP file is corrupted or hardware failure	Re-program radio or power cycle the radio.
AEGIS_ADIDOWN_DMFAIL	DSP ERR	855	DSP file is corrupted or hardware failure.	Re-program radio or power cycle the radio.
AEGIS_ADIDOWN_BIOSERR	DSP ERR	856	Hardware failure.	Service the radio.
AEGIS_KEYLOAD_NOBANKS	DSP ERR	860	Radio Personality did not assign banks for the keys.	Re-program the radio personality.
AEGIS_PVT_NONE	FEAT ERR	870	Private is not S/W feature enabled.	Re-program the radio personality.

9.2 RESUMING NORMAL OPERATION

The error tables listed in above contain the suggested action to clear the error and resume normal operation. As previously stated, FATAL errors will cause the radio to reset every 2 seconds until the error is fixed. Non-Fatal errors are displayed when they occur and do not stop the radio from operating. In either case, the only action that can be taken to clear the error condition is for the crypto-officer to use the PC Programmer and reprogram the radio. If this does not work or if the error is hardware related, the radio must be sent back to the manufacturer for repair.

9.3 OPERATOR INTERVENTION

The only requirement for the operator is to turn the radio on.

9.4 STATUS

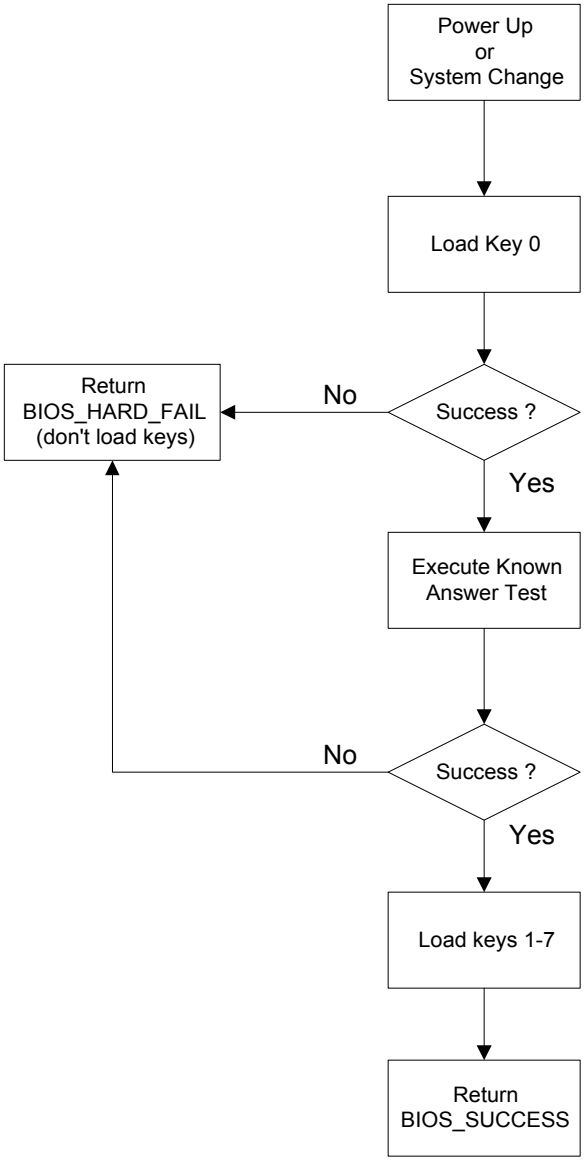
Upon completion of the power-up test, the radio provides a short beep *(if enabled)* to indicate the radio is ready for operation. The Control Head LCD indicates *(if programmed to do so)* the last selected system name on line one and the last selected group or channel on line 2 (Refer to Operator's Manual LBI-38888H, page 22, "TURNING THE RADIO ON").

9.5 CRYPTOGRAPHIC TEST

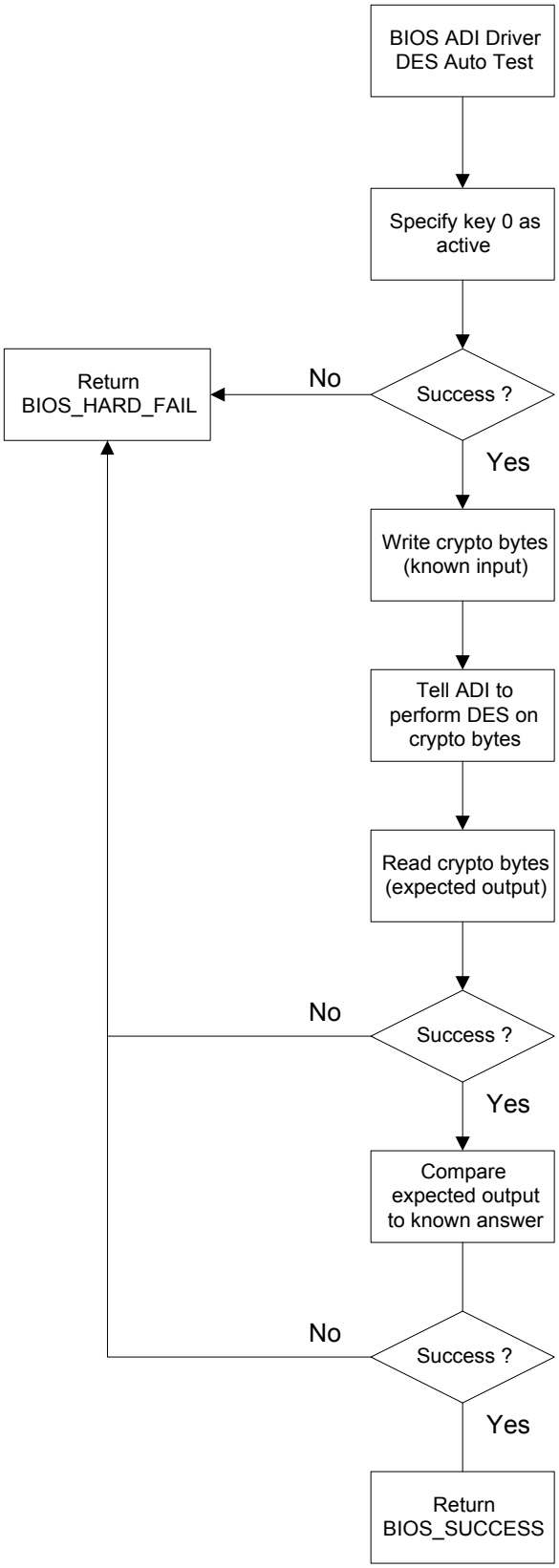
The crypto module performs an automatic Known Answer Test (KAT) before any DES keys are loaded into the ADI DSP. The DES algorithm must pass the test or the keys will not be loaded and cryptographic operation will not be allowed.

Upon power up or a system change, if the new system has private enabled the pre-stored keys will be loaded from EEPROM into the ADI DSP. If the ADI DSP has been loaded with the DES algorithm, the keys will not be transferred until the KAT passes.

The following diagram shows the flow on power up or on a system change:


Power Up
or
System Change
Load Key 0
Success ?
No
Return
BIOS_HARD_FAIL
(don't load keys)
Yes
Execute Known
Answer Test
Success ?
No
Yes
Load keys 1-7
Return
BIOS_SUCCESS

The following diagram shows the flow of the DES known answer test:



If the KAT fails, the radio will indicate this non-fatal error through the display for a short period and continue to operate. No cryptographic operations will be allowed. The radio will act as if no DES keys were loaded into the radio and operate in bypass mode.

9.6 CRITICAL FUNCTION TEST

There are no critical functions that will lead to the disclosure of plaintext information if they fail. The following items are checked at power up and the radio will not function if they fail:

- Radio Personality is present with correct CRC
- Synthesizer is locked
- S/W Feature data is present with correct CRC
- Bypass Test

As far as the DES keys, they must pass the following tests before they can be used:

- DES keys have a CRC that is verified as stored in the Orion EEPROM memory
- Manual entry of the DES keys requires passing a parity test
- DES keys require the algorithm to pass a Known Answer Test (KAT) before they are loaded

If the key can't be used then private operation will not be allowed. The user will get an error message if they try to transmit crypto data or voice.

10. GLOSSARY

TERM	DESCRIPTION
EDACS	Proprietary trunked radio protocol designed by M/A-COM
AEGIS™	Proprietary digital voice algorithm designed by M/A-COM
IMBE	Improved MultiBand Excitation vocoder.
VG	VoiceGuard is a digital voice algorithm that was replaced by AEGIS
Radio Personality	Orion configuration data which controls how the radio operates
DSP	Digital Signal Processor
A/D	Analog to Digital conversion
D/A	Digital to Analog conversion
Hang time	The time after a call has ended until the radio returns to scanning the control channel
WHC	Who Has Called feature which keeps track of the last calls received

This page intentionally left blank

M/A-COM Wireless Systems
221 Jefferson Ridge Parkway
Lynchburg, Virginia 24501
(Outside USA, 434-385-2400) Toll Free 800-528-7711
www.macom-wireless.com

Printed in U.S.A.