SECURITY POLICY
FOR THE EDACS ORION
SYSTEM/SCAN (AEGIS/DES)
MOBILE TWO-WAY FM RADIO

M/A Com
10/21/02
Version 1.5
Table of Contents

Table of Contents ................................................................................................................................. 2
1. Introduction ......................................................................................................................................... 3
2. Scope .................................................................................................................................................. 3
3. Cryptographic Boundary .................................................................................................................... 3
4. Physical Security ............................................................................................................................... 4
5. Module Description ............................................................................................................................ 5
   5.1. ORION Modules .......................................................................................................................... 5
   5.2. Module Components .................................................................................................................... 5
6. Software/Firmware Capabilities ....................................................................................................... 6
   6.1. Radio Control Processor (RCP) ................................................................................................... 6
   6.2. Interrupt Control Processor (ICP) ............................................................................................... 6
   6.3. AEGIS DSP (ADI) ....................................................................................................................... 6
   6.4. Firmware .................................................................................................................................. 7
7. Roles & Services ............................................................................................................................... 7
   7.1. User and Crypto-Officer Interfaces ............................................................................................ 8
   7.2. Crypto-Officer Role ..................................................................................................................... 8
   7.3. User Role .................................................................................................................................. 9
   7.3.1. Transmit / Receive .................................................................................................................. 9
   7.3.2. Zero DES keys ......................................................................................................................... 9
   7.3.3. Display DES key index ........................................................................................................... 9
   7.3.4. Bypass Mode .......................................................................................................................... 9
   7.4. Status Functions ........................................................................................................................ 10
   7.5. Key Management ....................................................................................................................... 11
   7.6. Table of Services ....................................................................................................................... 11
8. Secure Operation ............................................................................................................................ 12
      8.1.1. Clear Mode (Analog) ............................................................................................................. 12
      8.1.2. Digital Mode (AEGIS) ......................................................................................................... 12
      8.1.3. Private Mode (AEGIS DES) ............................................................................................... 13
      8.1.4. Receiving An Encrypted Call ............................................................................................. 13
      8.1.5. Transmitting An Encrypted Call ......................................................................................... 13
   9. Self Tests ....................................................................................................................................... 14
      9.1. Error Messages ......................................................................................................................... 15
      9.2. Resuming Normal Operation .................................................................................................. 18
      9.3. Operator Intervention .............................................................................................................. 18
      9.4. Status ..................................................................................................................................... 18
      9.5. Cryptographic Test .................................................................................................................. 18
      9.6. Critical Function Test ............................................................................................................. 21
10. Glossary ............................................................................................................................................ 21
1. Introduction

The ORION System/Scan (AEGIS) mobile two-way FM radios 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 a LCD. The purpose of this document is to provide the required documentation to the certifying agency for FIPS 140, Level 1 certification. The ORION radio is a multi-chip Stand-alone module.

The ORION radio is synthesized and operates in both trunked (Ericsson EDACS™) and conventional communications systems. The 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 AEGIS digital signaling and DES encryption.

Trunked operation is where a set of radio frequency channels is 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.

A conventional mode of operation is communicating on radio channels allocated for conventional use. Conventional use or operation is where a radio channel (transmit/receive) is allocated for conventional (non-trunked) use and may 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. Think of this mode as “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 the conventional mode, a system is a set of channels. A system may consist of all trunking groups and channels, all conventional channels, or a mixture of both.

2. Scope

This document will define the security policy for the ORION System/Scan mobile radio. This policy will define 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 section are excluded from the security requirements since they do not perform cryptographic functions. They are only used to transmit and receive. The Control Logic Board CMC-682 includes CMOS Microprocessors U701 and U702, which are part of a microcomputer circuit. For a circuit description of the Microcomputer circuit including memory devices and major functions of this circuit, refer to Maintenance Manual LBI-39165. The executable software and storage devices are, as provided before:

- RCP ROM Code (U701) 344A4867G2
- ICP ROM Code (U702) 344A4708G1
- Radio Code Flash Code (U707) 19089-CXC 112 1281/1 Rev. R42A
- ADI ROM Code (U710) 349A9662G2
- ADI RAM DES Code (U710) 349A9999G1

The only circuit not described in LBI-39165 is the AEGIS Digital Signal Processor (ADSP) U710 and it is as follows:
ADSP chip U710 performs speech digitization, Aegis or Voice Guard speech compression and optional decryption for Aegis equipped ORION radios. Chip U710 communicates with the H8/532 microcomputer U701 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.

ADSP U710 contains both Read-Only-Memory (ROM) and Random-Access-Memory (RAM). At power-up, the H8/532 loads the ADSP RAM. This software is stored separately in the Flash E²PROM along with the H8/532 operating software and radio personality. The software installed in Flash E²PROM is specific to the encryption algorithm installed (including un-encrypted Aegis), and must match the options enabled in the S/W 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 keyboard, rotary channel switch and volume control with an on/off 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 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 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 accesses to the ORION radio are protected from water entry by suitable gaskets and seals. However, degradation due to use or disassembly during repairs, may affect the integrity of
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.

### 5.1. ORION Modules

![ORION Block Diagram]

5.2. **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. AEGIS DSP (ADI)**

The ADI S/W resides in the ADI DSP ROM and RCP FLASH memory. The FLASH portion is downloaded at power up to the ADI’s 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 a proprietary algorithm known as AEGIS. Also, the ADI 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 certified 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 & 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. So, anyone can be a User or Crypto-Officer. It is strictly up to the owners of the product to control.
7.1. User and Crypto-Officer Interfaces

User Interface
- LCD, Tones
- Keypad, Switches

PC Programmer

User Role
(Control Input, Status Output)

Crypto-Officer Role
(Data Input, Control Input, Status Output)

Crypto-Officer Role

Radio Processing
(Data Input, Data Output)

Microphone
Speaker
RF

DSP (AEGIS/DES)
MODEM

Battery Power

User and Crypto-Officer Roles

7.2. 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, AEGIS-clear, and AEGIS 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).
7.3. 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

7.3.1. 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 8. Secure Operation.

7.3.2. 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.

7.3.3. 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.

7.3.4. 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 AEGIS 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:

The diagram shown below 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.
7.4. 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.
7.5. 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.

7.6. Table of Services

<table>
<thead>
<tr>
<th>Services</th>
<th>Inputs</th>
<th>Outputs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Encryption</td>
<td>PTT, microphone audio, encryption key</td>
<td>Encrypted speech and messages</td>
</tr>
<tr>
<td>Decryption</td>
<td>Received encrypted message, encryption key</td>
<td>Speaker audio</td>
</tr>
<tr>
<td>Key Entry</td>
<td>Keyloader device, key selection</td>
<td>Encryption keys stored in radio</td>
</tr>
<tr>
<td>Key Zeroization</td>
<td>CLEAR/CLR and OPTION/O buttons</td>
<td>Encryption keys erased in radio</td>
</tr>
<tr>
<td>Audit Key Entry</td>
<td>Key selected during key loading</td>
<td>Encryption key with “odds-one” parity</td>
</tr>
<tr>
<td>Status: Active Role</td>
<td>Operational state of radio, radio personality, encryption keys</td>
<td>Transmit/receive (TX/BSY), private mode (PVT) keylight, communication group and system</td>
</tr>
<tr>
<td>Status: Cryptographic State of Module</td>
<td>Radio personality, encryption keys, power up test</td>
<td>“DSP ERR” if power up test failed, “NO KEY” if encryption key error, otherwise no indication is given if crypto module is fully operational</td>
</tr>
<tr>
<td>Status: Error State</td>
<td>Power up test</td>
<td>See errors above</td>
</tr>
<tr>
<td>Status: Bypass</td>
<td>Radio personality, operational state of radio, radio PVT button</td>
<td>PVT keylight on indicates bypass mode is off, PVT keylight off indicates bypass mode is on</td>
</tr>
<tr>
<td>Cryptographic Bypass</td>
<td>Radio personality, operational state of radio, radio PVT button</td>
<td>Transmit and receive audio and messages without encryption when bypass mode is active</td>
</tr>
</tbody>
</table>
8. Secure Operation

8.1. Clear, Digital, and Private Operation

Each system (trunked or conventional) is programmed for either AEGIS or Voice Guard (VG) communications. VG is an earlier generation algorithm that was replaced by AEGIS and is only mentioned in this document because it appears in the Radio Personality as an option. AEGIS programmed systems have three different voice modes: Clear (analog), Digital (AEGIS, not private), and Private (AEGIS 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:

<table>
<thead>
<tr>
<th>Group/Channel Programming (Transmit)</th>
<th>CLEAR Receive</th>
<th>DIGITAL Receive</th>
<th>PRIVATE Receive</th>
</tr>
</thead>
<tbody>
<tr>
<td>CLEAR</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>DIGITAL</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>PRIVATE</td>
<td>Yes</td>
<td>No</td>
<td>Yes (with proper cryptographic key)</td>
</tr>
</tbody>
</table>

8.1.1. 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.

8.1.2. Digital Mode (AEGIS)

Digital mode allows the radio to transmit and receive digitized voice signals. AEGIS digital signals provide improved weak signal performance and cannot be easily monitored with a standard receiver. Groups and channels programmed for AEGIS 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.

8.1.3. Private Mode (AEGIS DES)

Private (cryptographic) mode allows the radio to transmit AEGIS 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.

8.1.4. 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.

8.1.5. 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
- E²PROM 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

<table>
<thead>
<tr>
<th>Error message</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>HARDWARE</td>
<td>ROM errors</td>
</tr>
<tr>
<td>SOFTWARE</td>
<td>General software failure</td>
</tr>
<tr>
<td>TRACKING</td>
<td>tracking data fatal error</td>
</tr>
<tr>
<td>NO LOCK</td>
<td>Synthesizer not locking</td>
</tr>
<tr>
<td>FREQDATA</td>
<td>frequency data fatal error</td>
</tr>
<tr>
<td>PERSDATA</td>
<td>Radio Personality errors</td>
</tr>
<tr>
<td></td>
<td>Non Fatal Errors</td>
</tr>
<tr>
<td>UNKNOWN</td>
<td></td>
</tr>
<tr>
<td>FEAT ERR</td>
<td>S/W Feature data error</td>
</tr>
<tr>
<td>DSP ERR</td>
<td>DSP error</td>
</tr>
</tbody>
</table>

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

```
DSP ERR
ERR=XXX
```

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.

<table>
<thead>
<tr>
<th>Error Name</th>
<th>Message</th>
<th>Code</th>
<th>Description</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>FATAL_RAM_ERROR</td>
<td>HARDWARE</td>
<td>2</td>
<td>8k RAM test error.</td>
<td>Return radio for service</td>
</tr>
<tr>
<td>FATAL_ROM_CHKSUM</td>
<td>HARDWARE</td>
<td>3</td>
<td>32k ROM CRC error</td>
<td>Return radio for service</td>
</tr>
<tr>
<td>FATAL_FLASH_CHKSUM</td>
<td>HARDWARE</td>
<td>4</td>
<td>Flash CRC error</td>
<td>Return radio for service</td>
</tr>
<tr>
<td>FATAL_ICP_LOAD</td>
<td>HARDWARE</td>
<td>10</td>
<td>ASIC driver failed initialization</td>
<td>Return radio for service</td>
</tr>
<tr>
<td>FATAL_ICP_LOAD</td>
<td>HARDWARE</td>
<td>11</td>
<td>ICP driver failed initialization</td>
<td>Return radio for service</td>
</tr>
<tr>
<td>FATAL_ASP_LOAD</td>
<td>HARDWARE</td>
<td>12</td>
<td>ASP driver failed initialization</td>
<td>Return radio for service</td>
</tr>
<tr>
<td>Error Name</td>
<td>Description</td>
<td>Action</td>
<td></td>
<td></td>
</tr>
<tr>
<td>----------------------</td>
<td>--------------------------------------</td>
<td>---------------------------------------------</td>
<td></td>
<td></td>
</tr>
<tr>
<td>FATAL_EE_LOAD</td>
<td>EEPROM driver failed initialization</td>
<td>Return radio for service</td>
<td></td>
<td></td>
</tr>
<tr>
<td>FATAL_ICP_PORTINIT</td>
<td>ICP digital I/O initialization failed</td>
<td>Return radio for service</td>
<td></td>
<td></td>
</tr>
<tr>
<td>FATAL_INOUT_LOAD</td>
<td>Standard input/output driver failed initialization</td>
<td>Return radio for service</td>
<td></td>
<td></td>
</tr>
<tr>
<td>FATAL_INTN_LOAD</td>
<td>Standard input driver failed initialization</td>
<td>Return radio for service</td>
<td></td>
<td></td>
</tr>
<tr>
<td>FATAL_RADIO_LOAD</td>
<td>RADIO driver failed initialization</td>
<td>Return radio for service</td>
<td></td>
<td></td>
</tr>
<tr>
<td>FATAL_MODEM_LOAD</td>
<td>MODEM driver failed initialization</td>
<td>Return radio for service</td>
<td></td>
<td></td>
</tr>
<tr>
<td>FATAL_EXTIO_LOAD</td>
<td>External I/O driver failed initialization</td>
<td>Return radio for service</td>
<td></td>
<td></td>
</tr>
<tr>
<td>FATAL_SCI_LOAD</td>
<td>Serial communication interface driver failed initialization</td>
<td>Return radio for service</td>
<td></td>
<td></td>
</tr>
<tr>
<td>FATAL_ICP_CHKSUM</td>
<td>ICP prom checksum</td>
<td>Return radio for service</td>
<td></td>
<td></td>
</tr>
<tr>
<td>FATAL_ADI_NOACK</td>
<td>ADI did not respond to command</td>
<td>Return radio for service</td>
<td></td>
<td></td>
</tr>
<tr>
<td>FATAL_ADI_QUNDERFLOW</td>
<td>ADI rx circular queue underflowed</td>
<td>Return radio for service</td>
<td></td>
<td></td>
</tr>
<tr>
<td>FATAL_LCD_NOACK</td>
<td>LCD did not ack message</td>
<td>Return radio for service</td>
<td></td>
<td></td>
</tr>
<tr>
<td>FATAL_LCD_HARD_FAIL</td>
<td>LCD hardware is invalid</td>
<td>Return radio for service</td>
<td></td>
<td></td>
</tr>
<tr>
<td>FATAL_ICP_NOACK</td>
<td>ICP did not ack message</td>
<td>Return radio for service</td>
<td></td>
<td></td>
</tr>
<tr>
<td>FATAL_EXTIO_ICPFAIL</td>
<td>ICP failed in a fork</td>
<td>Return radio for service</td>
<td></td>
<td></td>
</tr>
<tr>
<td>FATAL_RADIO_ASPWRT</td>
<td>Radio driver could not write to ASP</td>
<td>Return radio for service</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Operational software Fatal system errors:**

<table>
<thead>
<tr>
<th>Error Name</th>
<th>Description</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>RADC_PITD_ERROR</td>
<td>Radio Personality tracking data error.</td>
<td>Reprogram the tracking data</td>
</tr>
<tr>
<td>RADC_PIHW_ERROR</td>
<td>Radio Personality hardware data error.</td>
<td>Reprogram the radio personality</td>
</tr>
<tr>
<td>RADC_FREQ_ERROR</td>
<td>Radio Personality frequency data error.</td>
<td>Reprogram the radio personality</td>
</tr>
<tr>
<td>RADC_PITD_MALLOC_ERROR</td>
<td>Radio Personality tracking data malloc error.</td>
<td>Reprogram the tracking data</td>
</tr>
<tr>
<td>RADC_PITD_CKSUM_ERROR</td>
<td>Radio Personality tracking data checksum error.</td>
<td>Reprogram the tracking data</td>
</tr>
<tr>
<td>DACS_NO_LOCK</td>
<td>Synthesizer did not lock or became unlocked.</td>
<td>Check the frequencies in the PC programmer and reprogram the radio personality</td>
</tr>
<tr>
<td>DACS_MODEM_FATAL_ERROR</td>
<td>Unable to correctly configure the modem for EDACS operation.</td>
<td>Reprogram the radio personality</td>
</tr>
</tbody>
</table>
## M/A Com Security Policy

### ORION (AEGIS/DES) Radio

#### 17

<table>
<thead>
<tr>
<th>Error Name</th>
<th>Message</th>
<th>Code</th>
<th>Description</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>CONV_NOLOCK_ERROR</strong></td>
<td>NO LOCK</td>
<td>401</td>
<td>Synthesizer became unlocked.</td>
<td>Check the frequencies in the PC programmer and reprogram the radio personality.</td>
</tr>
<tr>
<td><strong>CONV_PERS_ERROR</strong></td>
<td>PERSDATA</td>
<td>407</td>
<td>Conventional radio personality error.</td>
<td>Reprogram the radio personality</td>
</tr>
<tr>
<td><strong>PI_NOPERS_ERROR</strong></td>
<td>PERSDATA</td>
<td>500</td>
<td>Radio Personality data is not present.</td>
<td>Reprogram the radio personality</td>
</tr>
<tr>
<td><strong>PI_CRC_ERROR</strong></td>
<td>PERSDATA</td>
<td>501</td>
<td>Flash radio personality CRC did not match EEPROM.</td>
<td>Reprogram the radio personality</td>
</tr>
<tr>
<td><strong>PI_DESC_CRC_ERROR</strong></td>
<td>PERSDATA</td>
<td>502</td>
<td>Crucial radio personality data has incorrect CRC.</td>
<td>Reprogram the radio personality</td>
</tr>
<tr>
<td><strong>UI_FATAL_DEVICE_NOTSUPPORTED</strong></td>
<td>PERSDATA</td>
<td>609</td>
<td>I/O device type (from personality) not supported.</td>
<td>Reprogram the radio personality</td>
</tr>
<tr>
<td><strong>AEGIS_KEYLOAD_ERROR</strong></td>
<td>SOFTWARE</td>
<td>804</td>
<td>General keyload error has occurred.</td>
<td>Reprogram the radio personality</td>
</tr>
<tr>
<td><strong>AEGIS_KEYLOAD_NOTABL</strong></td>
<td>SOFTWARE</td>
<td>806</td>
<td>No key table was found in eeprom.</td>
<td>Reprogram the radio personality</td>
</tr>
<tr>
<td><strong>AEGIS_KEYLOAD_BADSIZE</strong></td>
<td>SOFTWARE</td>
<td>807</td>
<td>Key table is wrong size in eeprom.</td>
<td>Reprogram the radio personality</td>
</tr>
<tr>
<td><strong>AEGIS_KEYLOAD_CORRUPT</strong></td>
<td>SOFTWARE</td>
<td>808</td>
<td>Key table has been corrupted.</td>
<td>Reprogram the personality and reload encryption keys.</td>
</tr>
</tbody>
</table>

### Operational software Non-Fatal system errors:

<table>
<thead>
<tr>
<th>Error Name</th>
<th>Message</th>
<th>Code</th>
<th>Description</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>PIFEAT_SNR_ERROR</strong></td>
<td>FEAT ERR</td>
<td>550</td>
<td>S/W Feature Data - Cannot read radio ROM serial number.</td>
<td>Service radio and replace SNR.</td>
</tr>
<tr>
<td><strong>PIFEAT_READ_ERROR</strong></td>
<td>FEAT ERR</td>
<td>551</td>
<td>Radio Personality S/W feature data read failure or data not available.</td>
<td>Service radio and replace SNR.</td>
</tr>
<tr>
<td><strong>PIFEAT_CRC_ERROR</strong></td>
<td>FEAT ERR</td>
<td>552</td>
<td>Radio Personality S/W feature data CRC failure.</td>
<td>Re-program the radio personality</td>
</tr>
<tr>
<td><strong>RI_DSPDOWN_NOATTEMPT</strong></td>
<td>DSP ERR</td>
<td>850</td>
<td>DSP not found. Radio does not support private operation.</td>
<td>Re-program the ADI file.</td>
</tr>
<tr>
<td><strong>AEGIS_ADIDOWN_NOTFOUND</strong></td>
<td>DSP ERR</td>
<td>851</td>
<td>DSP file not found.</td>
<td>Re-program the ADI file.</td>
</tr>
<tr>
<td><strong>AEGIS_ADIDOWN_CRCFAIL</strong></td>
<td>DSP ERR</td>
<td>852</td>
<td>DSP file is corrupted.</td>
<td>Re-program the ADI file.</td>
</tr>
<tr>
<td><strong>AEGIS_ADIDOWN_ENCERR</strong></td>
<td>DSP ERR</td>
<td>853</td>
<td>S/W feature data does not match DSP file.</td>
<td>Re-program the radio personality.</td>
</tr>
<tr>
<td><strong>AEGIS_ADIDOWN_PMFAIL</strong></td>
<td>DSP ERR</td>
<td>854</td>
<td>DSP file is corrupted or hardware failure.</td>
<td>Re-program radio or power cycle the radio.</td>
</tr>
<tr>
<td><strong>AEGIS_ADIDOWN_DMFAIL</strong></td>
<td>DSP ERR</td>
<td>855</td>
<td>DSP file is corrupted or hardware failure.</td>
<td>Re-program radio or power cycle the radio.</td>
</tr>
<tr>
<td><strong>AEGIS_ADIDOWN_BIOSERR</strong></td>
<td>DSP ERR</td>
<td>856</td>
<td>Hardware failure.</td>
<td>Service the radio.</td>
</tr>
<tr>
<td>Error Code</td>
<td>Error Type</td>
<td>Error Code</td>
<td>Error Type</td>
<td></td>
</tr>
<tr>
<td>-----------------------------</td>
<td>-------------</td>
<td>------------</td>
<td>-------------</td>
<td></td>
</tr>
<tr>
<td>AEGIS_KEYLOAD_NOBANKS</td>
<td>DSP ERR</td>
<td>860</td>
<td>Radio Personality did not assign banks for the keys.</td>
<td></td>
</tr>
<tr>
<td>AEGIS_PVT_NONE</td>
<td>FEAT ERR</td>
<td>870</td>
<td>Private is not S/W feature enabled.</td>
<td></td>
</tr>
</tbody>
</table>

### 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:

1. **Power Up or System Change**
   - Load Key 0
   - Success?
     - Yes: Execute Known Answer Test
       - Success?
         - Yes: Load keys 1-7
           - Return BIOS_SUCCESS
         - No: Return BIOS_HARD_FAIL (don't load keys)
     - No: Return BIOS_HARD_FAIL (don't load keys)
The following diagram shows the flow of the DES known answer test:

1. **Specify key 0 as active**
   - **Success?**
     - Yes: **Write crypto bytes (known input)**
     - No: **Return BIOS_HARD_FAIL**
2. **Write crypto bytes (known input)**
   - **Tell ADI to perform DES on crypto bytes**
     - **Read crypto bytes (expected output)**
       - **Success?**
         - Yes: **Compare expected output to known answer**
         - No: **Return BIOS_HARD_FAIL**
   - **No**: **Success?**
     - Yes: **Return BIOS_SUCCESS**
     - No: **Return BIOS_HARD_FAIL**
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

<table>
<thead>
<tr>
<th>Term</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>EDACS</td>
<td>Proprietary trunked radio protocol designed by Ericsson</td>
</tr>
<tr>
<td>AEGIS</td>
<td>Proprietary digital voice algorithm designed by Ericsson</td>
</tr>
<tr>
<td>VG</td>
<td>VoiceGuard is an old digital voice algorithm that was replaced by AEGIS</td>
</tr>
<tr>
<td>Radio Personality</td>
<td>ORION configuration data which controls how the radio operates</td>
</tr>
<tr>
<td>DSP</td>
<td>Digital Signal Processor</td>
</tr>
<tr>
<td>A/D</td>
<td>Analog to Digital conversion</td>
</tr>
<tr>
<td>D/A</td>
<td>Digital to Analog conversion</td>
</tr>
<tr>
<td>Hang time</td>
<td>The time after a call has ended until the radio returns to scanning the control channel</td>
</tr>
<tr>
<td>WHC</td>
<td>Who Has Called feature which keeps track of the last calls received</td>
</tr>
</tbody>
</table>