MOTOROLA

MCS 2000 Mobile Radio
SECURENET Option
Service Instructions

68P81083C25-A, Issued 7/97

Safety Information

Every radio, when transmitting, radiates energy into the atmosphere which may, under certain conditions, cause the generation of a spark.

All users of vehicles fitted with radios should be aware of the following warnings:

Do not operate radio near flammable liquids or in the vicinity of explosive devices.

To ensure personal safety, please observe the following simple rules:

Check the laws and regulations on the use of two-way mobile radios in the areas where you drive. Always obey them. Also, when using your radio while driving, please:

- Give full attention to driving,
- Use hands-free operation, if available and
- Pull off the road and park before making or answering a call if driving conditions so require.

Airbag Warning

VEHICLES EQUIPPED WITH AIR BAGS

An air bag inflates with great force. DO NOT place objects, including communication equipment, in the area over the air bag or in the air bag deployment area. If the communication equipment is improperly installed and the air bag inflates, this could cause serious injury.

Installation of vehicle communication equipment should be performed by a professional installer/technician qualified in the requirements for such installations.

An air bag's size, shape and deployment area can vary by vehicle make, model and front compartment configuration (e.g., bench seat vs. bucket seats). Contact the vehicle manufacturer's corporate headquarters, if necessary, for specific air bag information for the vehicle make, model and front compartment configuration involved in your communication equipment installation.

LP Gas Warning

It is mandatory that radios installed in vehicles fuelled by liquefied petroleum gas conform to the National Fire Protection Association standard NFPA 58, which applies to vehicles with a liquid propane (LP) gas container in the trunk or other sealed off space within the interior of the vehicle. The NFPA58 requires the following:

- Any space containing radio equipment shall be isolated by a seal from the

space in which the LP gas container and its fittings are located.

- Removable (outside) filling connections shall be used.
- The container space shall be vented to the outside.

Anti-Lock Braking System (ABS) and Anti-Skid Braking System Precautions

WARNING

Disruption of the anti-skid/anti-lock braking system by the radio transmitter may result in unexpected vehicle motion.

Motorola recommends the following radio installation precautions and vehicle braking system test procedures to ensure that the radio, when transmitting, does not interfere with operation of the vehicle braking system.

Installation Precautions

1. Always provide as much distance as possible between braking modulator unit and radio, and between braking modulator unit and radio antenna and associated antenna transmission line. Before installing radio, determine location of braking modulator unit in vehicle. Depending on make and model of vehicle, braking modulator unit may be located in trunk, under dashboard, in engine compartment, or in some other cargo area. If you cannot determine location of braking modulator unit, refer to vehicle service manual or contact a dealer for the particular make of vehicle.
2. If braking modulator unit is located on left side of the vehicle, install radio on right side of vehicle, and conversely.
3. Route all radio wiring including antenna transmission line as far away as possible from braking modulator unit and associated braking system wiring.
4. Never activate radio transmitter while vehicle is in motion and vehicle trunk lid is open.

Braking System Tests

The following procedure checks for the most common types of interference that may be caused to vehicle braking system by a radio transmitter.

1. Run vehicle engine at idle speed and set vehicle transmission selector to PARK. Release brake pedal completely and key radio transmitter. Verify that there are no unusual effects (visual or audible) to vehicle lights or other electrical equipment and accessories while microphone is NOT being spoken into.
2. Repeat step 1. except do so while microphone IS being spoken into.
3. Press vehicle brake pedal slightly just enough to light vehicle brake light(s). Then repeat step 1. and step 2.
4. Press the vehicle brake pedal firmly and repeat step 1. and step 2.
5. Ensure that there is a minimum of two vehicle lengths between front of vehicle and any object in vehicle's forward path. Then, set vehicle

transmission selector to DRIVE. Press brake pedal just far enough to stop vehicle motion completely. Key radio transmitter. Verify that vehicle does not start to move while microphone is NOT being spoken into.

6. Repeat step 5. except do so while microphone IS being spoken into.
7. Release brake pedal completely and accelerate vehicle to a speed between 15 and 25 miles/25 and 40 kilometers per hour. Ensure that a minimum of two vehicle lengths is maintained between front of vehicle and any object in vehicle's forward path. Have another person key radio transmitter and verify that vehicle can be braked normally to a moderate stop while microphone is NOT being spoken into.
8. Repeat step 7. except do so while microphone IS being spoken into.
9. Release brake pedal completely and accelerate vehicle to a speed of 20 miles/30 kilometers per hour. Ensure that a minimum of two vehicle lengths is maintained between front of vehicle and any object in vehicle's forward path. Have another person key radio transmitter and verify that vehicle can be braked properly to a sudden (panic) stop while microphone is NOT being spoken into.
10. Repeat step 9. except do so while microphone IS being spoken into.
11. Repeat step 9. and step 10. except use a vehicle speed of 30 miles/50 kilometers per hour.

LIST OF EFFECTIVE PAGES

MCS 2000 Mobile Radio

SECURENET Service Instructions

Motorola Publication Number 68P81083C25-O

Issue Dates of Original and Revised Pages are:

Original: August 1996
Revision A: July 1997

The Number of pages in this publication is 60 consisting of the following:

Page Number	Revision Letter	Page Number	Revision Letter
Front cover	O	15	A
Inside front cover (blank)	O	16 through 41	O
Title	A	42	A
Safety 0 through Safety 2	O	43 and 44	O
A	A	Questionnaire (Front)	O
B	O	Questionnaire (Back)	O
i	A	Inside back cover	O
ii through iv	O	Back cover	O
1 through 14	O		

Note: The letter O in the Revision Letter column of the table above denotes an original page. Original pages ARE NOT identified as such in the page footors except by the absence of a revision letter and date.

IMPORTANT ELECTROMAGNETIC EMISSION INFORMATION

The Federal Communications Commission (FCC), with its action in General Docket 79144, March 13, 1985, has adopted a safety standard for human exposure to radio frequency electromagnetic energy emitted by FCC regulated equipment. Motorola subscribes to this safety standard for the use of its products, and the design of your Motorola radio complies with this standard. Proper use of this radio will result in exposure levels below specified limits.

In keeping with sound installation practice and to maximize radiation efficiency, a one-quarter (1/4) wave length antenna should be installed at the center of the vehicle roof. If it is necessary to mount the antenna on the vehicle's trunk lid, an appropriate 3db gain antenna should be used. This installation procedure will assure that vehicle occupants will be exposed to radio frequency energy levels lower than the limits specified in the standard adopted by the FCC in General Docket 79144.

To assure that radio frequency (RF) energy exposure to bystanders external to a vehicle is lower than that recommended by FCC adopted standard, transmit with any mobile radio only when bystanders are at least two (2) feet away from a properly installed externally mounted antenna for radios with less than 50 watts of output power, or three (3) feet away for radios with 50 watts or greater power.

Control Station Operation

In the event of Control Station operation, to assure operators and bystanders are exposed to radio frequency (RF) energy levels lower than the limits specified in the FCC adopted standard, the antenna should be installed outside of any building, but in no instance shall the antenna be within two feet (less than 50 watts power output) or within three feet (50 watts or higher power output) of station operators or bystanders.

Table of Contents

Table of Contents (Continued)

List of Figures

List of Tables

1 Description

General Description

SECURENET is an optional feature for the Motorola MCS 2000 Mobile FM Radio Transceiver. It is intended for radio users who need completely private and protected communications. SECURENET uses digital encryption/decryption techniques to prevent unintended listeners from hearing confidential voice traffic.

The SECURENET option is physically incorporated into the radio by adding a circuit card subassembly, called the Secure Module, to the Radio Transceiver Board. (Hereafter in this manual, the Secure Module is also referred to as the module; the Radio Transceiver Board is also referred to as the transceiver board).

In addition to the physical addition of the module to the radio, certain modifications are made to the radio's codeplug and the radio's alignment.

The module is mounted inside an enclosure, which consists of a metal fence covered by a metal shield. The enclosure is mounted on the controller section of the transceiver board. The assembled module enclosure is illustrated in Figure 1. The module plugs into a connector located on the transceiver board inside the fence.

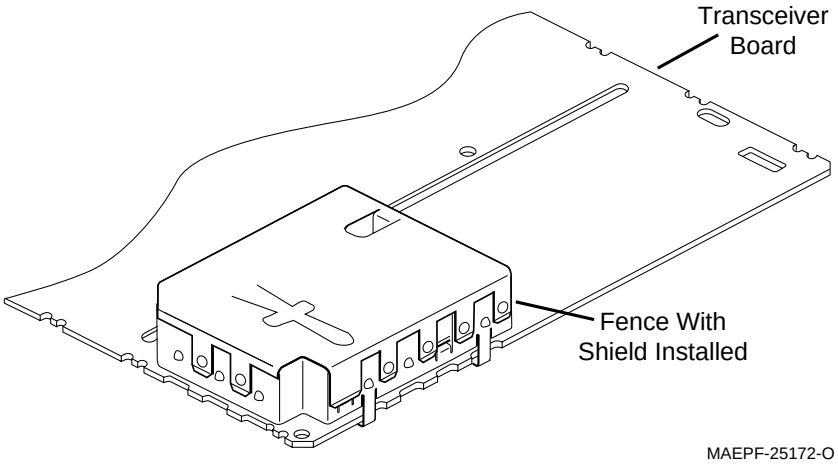


Figure 1 Transceiver Board with Secure Module Enclosure In Place

In transmit, a SECURENET-equipped radio converts the analog voice signal to digital form. The digitized signal is then encrypted using one of four possible non-linear mathematical encryption algorithms. A filtered version of the encrypted digital signal is amplified and radiated by the same circuits and antenna used for clear (non-secure) transmissions.

In receive, a SECURENET-equipped radio decrypts the encrypted digitized voice signal using the same algorithm as in the transmitting radio. It then converts the decrypted digital signal into analog form. The analog voice signal is amplified and output to the loudspeaker or handset using the same circuits used for clear reception.

There are five encryption types: DES, DES-XL, DVP, DVP-XL, and DVI-XL. The five encryption types differ from one another according to the combination of encryption algorithm and encryption synchronization type each uses. There are four different encryption algorithms, which are: DES/DES-XL, DVP, DVP-XL, and DVI-XL. (The DES and DES-XL encryption types use the same encryption algorithm but may use different types of encryption synchronization.)

The encryption algorithms use an operator-entered key-variable (or key), which makes the encryption process unique to that operator and other operators using the same algorithm and key. The key is loaded into the radio, via the radio's microphone connector, using a hand held Key Variable Loader (KVL). There are five different models of KVL. The model numbers for the applicable KVLs are listed in Table 1.

Secure modules for the five encryption types are available in two configurations, one with 3-day key retention (standard) and the other with long-term key retention (optional). This results in there being 10 module configurations. The 10 configurations and their corresponding Motorola kit and option numbers are listed in Table 1.

Table 1 Encryption Type, Key Retention, and KVL vs Motorola Kit and Option Numbers

Encryption Type	Key Retention	Motorola Option Number for Secure Module	Motorola Kit Number for Secure Module	Motorola Model Number for Applicable KVL (See Note at End of Table)
DES	3 Days	B388	HLN6575	T3011_X
DES	Long Term	B388 & G367	HLN6587	T3011_X
DES-XL	3 Days	B795	HLN6576	T3011_X
DES-XL	Long Term	B795 & G367	HLN6585	T3011_X
DVP	3 Days	B794	HLN6577	T3010_X
DVP	Long Term	B794 & G367	HLN6586	T3010_X
DVP-XL	3 Days	B797	HLN6578	T3014_X
DVP-XL	Long Term	B797 & G367	HLN6584	T3014_X
DVI-XL	3 Days	B793	HLN6579	T3012_X or T3013_X
DVI-XL	Long Term	B793 & G367	HLN6583	T3012_X or T3013_X

NOTE: All KVLs connect to the MCS 2000 radio with cable assembly TKN9152.

Reference Publications

Refer to the Motorola publications listed in Table 2 for additional information related to installation, operation, and servicing of Motorola MCS 2000 Mobile FM Radio Transceivers.

Table 2 Reference Publications

Motorola Publication Number	Title
68P81083C20	Motorola MCS 2000 Mobile FM Radio Transceiver Service Instructions Volume 1, Common Information
68P81080C43	Motorola MCS 2000 Mobile FM Radio Transceiver Service Instructions Volume 2a, 800-MHz Frequency Band Specific Information
68P81080C41	Motorola MCS 2000 Mobile FM Radio Transceiver Service Instructions Volume 2b, VHF Frequency Bands Specific Information
68P81080C42	Motorola MCS 2000 Mobile FM Radio Transceiver Service Instructions Volume 2c, UHF Frequency Bands Specific Information
68P81080C44	Motorola MCS 2000 Mobile FM Radio Transceiver Service Instructions Volume 2d, 900-MHz Frequency Band Specific Information
68P81080C46	Motorola MCS 2000 Mobile FM Radio Transceiver Service Instructions Volume 2e, Mid Frequency Band Specific Information
68P81081C15	Motorola MCS 2000 Mobile FM Radio Transceiver Radio Service Software (RSS) Operation Instructions
68P81083C05	Motorola MCS 2000 Mobile FM Radio Transceiver Model I Quick Start Operating Instructions
68P81083C10	Motorola MCS 2000 Mobile FM Radio Transceiver Models II and III Quick Start Operating Instructions
68P81080C35	Motorola MCS 2000 Mobile FM Radio Transceiver Detailed Operating Instructions
68P02058U20	Motorola Mobile FM Radio Transceiver Installation Instructions for Models MC 900, GM 900, GM 1100, GM 1200, GM 2000, MCX 1200, MCS 2000, MCX 2000, and MC 2100
68P81080C47	Motorola MCS 2000 Accessory Catalog
68P02058U21 (Applicable to European Audiences Only)	Motorola Mobile FM Radio Transceiver Service Instructions for Models MC900, GM900, GM1100, GM1200, GM2000, MCX1200, MCS2000, MCX2000 and MC2100

Functional Description

The SECURENET function requires that both the transmitting and receiving radios be equipped with a Secure Module, and that the codeplug software and tuning in both radios be set up for SECURENET operation.

The module is connected to the transmit, receive, and controller circuits on the transceiver board. All connections between the transceiver board and the Secure Module are made via connector P1 on the module, which mates with connector J0401 on the transceiver

board. Table 3 lists and describes all the signals that pass through these connectors.

In transmit mode, the Secure Module receives the microphone audio signal (ASFIC PRE EMP) at pin 7 of P1/ J0401. The module digitizes the signal, encrypts it, and low pass filters it. The module then passes the resultant splatter filtered encrypted signal to the radio's modulator circuit via the AUX TX line, pin 14 of P1/ J0401. The modulated signal is RF amplified and transmitted via the radio's antenna

Table 3 Interface Between Transceiver Board and Secure Module

Signal Name		**Pin Number on Connector**	**Function**
Secure Module Plug P1	**Transceiver Board Connector J0401**		
A+ CONT	A+ CONT	1	Unswitched battery voltage
Vdd	+5V	2	Switched 5 volt supply
2.1 MHz	2.1 MHz	3	2.1/2.4 MHz clock signal
GROUND	GROUND	4	Ground
ASFIC PRE EMP	ASFIC PRE-EMP OUT	7	Transmit clear audio (mic audio)
RX AUDIO	AUX RX IN1	9	Receive clear audio
UNIV IO	UNIV I/O	10	Receive encrypted audio
TAMPER	GROUND	11	Ground
RADIO RESETb	$\overline{\text{RESET}}$	12	Radio reset - Does NOT reset Secure Module or erase key
KVL KFb	KEY/FAIL	13	Keyloading signal
AUX TX	AUX TX1	14	Transmit encrypted audio
KID	RX DATA / KID	15	Keyloading signal
KVL WEb	RTS / DVP WE	16	Keyloading signal
SPI CLK	CLK	17	SPI data clock
SPI MOSI	SPI TX DATA	18	SPI data from host processor
SPI MISO	MISO	19	SPI data to host processor
JABBA INTb	JABBA INT	20	SPI Secure Interrupt Request
JABBA SELb	JABBA SEL	21	SPI Secure Slave Select
CONT 5V	NOT CONNECTED	24	Continuous 5-Volt regulator output
KEYLOADING	ASN_INTb	22	Keyloading Indicator
		5,6,8,23,25	Not used

In receive mode, the Secure Module takes the discriminator signal (UNIV IO) from pin 10 of P1/ J0401. It synchronizes, decrypts, and converts the signal from digitized data back into an analog voice signal. The signal is then passed on to the audio section of the transceiver board via the AUX RX line, pin 9 of P1/ J0401, where it is amplified by the radio's audio amplifier circuits and supplied to the radio's loudspeaker.

The Secure Module communicates with the controller section of the transceiver board via the transceiver board's serial peripheral interface (SPI) bus. The controller's host processor (U0103) is the master on this bus, while the module is one of several slaves on the bus. The SPI CLK line, on pin 17 of P1/J0401, is the data rate clock for communication on the SPI bus. It is present only when the SPI bus is in use.

Since the module is not the only slave on the SPI bus, the JABBA INTb line (pin 20 of P1/J0401) and the JABBA SELb line (pin 21 of P1/J040) indicate usage of the bus by the module. The JABBA INTb line is active low. When this line is active, it indicates that the module is requesting communication with the host processor. The JABBA SELb line is also active low. When this line is active, it indicates that the processor in the radio's controller section is currently communicating with the module. The SPI MOSI (Master Out Slave In) line, pin 18 of P1/J0401, allows transmission of data from the host processor to the module. The SPI MISO (Master In Slave Out) line, pin 19 of P1/J0401, allows transmission of data from the module back to the processor.

The Secure Module can encrypt or decrypt voice data only if it has been loaded with a key. Only one key can be stored in the module at a time. The key is loaded from the KVL into the radio via the microphone connector. It passes from the control head to the transceiver board via pins 10, 11, and 12 of J0650/J0405. From there, it passes into the module via pins 13, 15, and 16 of P1/J0401. The key is stored in volatile electronic memory and, therefore, remains viable only while the memory is supplied with a source of electrical power.

If the radio is disconnected from the external source of electrical power and the secure module is the standard 3 day key retention type, a large capacitor (0.22F) on the module supplies power to the encryption circuitry and retains the key for approximately 3 days.

If the radio is disconnected from the external source of electric power and the module is equipped with the long-term key retention option, a battery on the module provides power to the encryption circuitry and retains the key for an extended period of time. The life of the battery is such that with normal use it should last in excess of 10 years, provided the module does not remain in storage for more than a year between the time the battery is installed on the module and the time the module is installed in a radio. Maximum battery life will be realized as long as storing the module outside of the radio is avoided.

NOTE: Maximum current drain on the key-retention battery occurs when the module is *not* installed in a radio.

The module uses two power supplies. The first supply is a regulated 5 volt supply (Vdd) received from the transceiver board (+5V) via pin 2 of P1/J0401. Vdd turns on and off with the radio's on/off switch. The second power supply (A+ CONT) is the unregulated voltage from the car battery. A+ CONT is received from the transceiver board (A+ CONT) via pin 1 of P1/J0401. A+ CONT provides continuous power to the module for as long as the radio is connected to a source of external power.

2

Service Aids

The service aids required for troubleshooting and repair of a SECURENET-equipped radio are listed and described in Table 4. These service aids are in addition to those listed in Volume 1 of the Service Manual for the MCS 2000 Radio.

NOTE: As of the publication date of this service manual, the current version of the KVL has a DX suffix, however, the MCS 2000 Secure Module is compatible with all versions of these model numbers (i.e., AX, BX, CX, DX).

Table 4 Service Aids for Troubleshooting a SECURENET Equipped Radio

Motorola Model Number	Description	Application
T3010_X	Key Variable Loader	Used to load key into DVP Secure Modules.
T3011_X	Key Variable Loader	Used to load key into DES and DES-XL Secure Modules.
T3012_X	Key Variable Loader	Used to load key into DVI-XL Secure Modules. This is the fully functional Supervisor model.
T3013_X	Key Variable Loader	Used to load key into DVI-XL Secure Modules. This is the Operator model. Keys must be loaded from another T3012 or T3013 KVL. Keys cannot be enterred through the keypad in this model.
T3014_X	Key Variable Loader	Used to load key into DVP-XL Secure Modules.
TKN9152	Cable Assembly	Used to connect any of the four types of Key Variable Loaders to the MCS 2000 Radio.
3080370E05	Cable Assembly	Used to operate a Secure Module outside of its shielded enclosure during troubleshooting.
Not Applicable	3/4-Inch Spring Binder Clip	Used to defeat Tamper Popple during troubleshooting and testing of SECURENET Option.

NOTES

Troubleshooting A SECURENET-Equipped Radio

3

General Information

The information in this chapter applies primarily to troubleshooting the SECURENET option. If both the clear function and the SECURENET option are faulty, refer to the troubleshooting information in Service Manual Volume 1 and Service Manual Volume 2 (Volume 2a, 2b, 2c, or 2d) listed in Table 2 and troubleshoot and repair the clear function. When you are sure the clear function is working correctly, try the SECURENET option again. If it is still not working properly, troubleshoot and repair the SECURENET option using the troubleshooting information in this chapter. Also refer to the troubleshooting flowcharts (Figures 5 through 10) in Chapter 9, which will help identify and eliminate some of the more common problems associated with secure operation.

Troubleshooting the Secure Module can be extremely difficult. Due to the physical location of the module within its enclosure, it is difficult to access and probe signals on the module while it is installed in the radio. Removing the module from the radio for the purpose of troubleshooting is not a simple matter either because the module is equipped with anti-tamper mechanisms that cause the module to erase the key when the radio is disassembled.

Repairing the module can be difficult because replacing components, especially the larger ones, from the module can result in permanent damage to the circuit board. In addition, replacements are not available for any of the encryption related components (i.e., integrated circuits U1, U3, and U4).

Error Conditions

Two failure conditions are associated with the SECURENET option: ERROR 09/10 and KEY FAIL.

An “ERROR 09/10” or “ER 09/10” message on the radio display signifies a communications failure between the controller host processor (U0103) on the transceiver board and the SPI interface on the module’s Encryption Support IC (U1). This means that there is a problem with either one or more of the four SPI lines (SPI CLK, SPI MOSI, SPI MISO, or JABBA SELb) or the reference clock (2.1 MHz/2.4 MHz) or the Encryption Support IC itself. Typically this error occurs when a radio is configured for secure operation, but does not have a Secure Module installed.

A “KEY FAIL” message on the radio display occurs whenever the Secure Module detects the absence of a key, either when the radio is first

turned on or when a secure transmission is attempted. Moreover, if the Periodic Keyfail Alert Tone option is enabled (See Table 5), the radio will beep periodically and display the message “KEY FAIL” whenever the radio is configured for SECURENET transmit operation. All transmit and receive secure operations are inhibited during a key fail condition.

There are three primary causes for a key fail condition: the radio user forces a key erase manually from the secure menu on the control head; an attempt is made to disassemble the radio causing the anti-tamper circuitry on the module to erase the key; or in the case of a 3-day key retention type of module, the radio is disconnected from the external source of electrical power long enough for the key storage capacitor to discharge completely. (Or in the case of a long term key retention type of module, the radio is disconnected from the external source of electrical power and the key retention battery is dead.)

Be aware that the Secure Module will retain key for 3 days only after the capacitor has been fully charged. Typically this means that the radio has been connected to a source of electrical power for at least one day. If the radio is installed in such a way that power is removed from the radio whenever the car is turned off, then it is likely that the key will eventually be lost.

Basic Troubleshooting

Due to the complexities related to troubleshooting and repairing the Secure Module, before disassembling the radio it is advisable to first investigate the possibility that the cause of a problem is something other than a faulty module. To that end, here are a few relatively simple troubleshooting steps that can be tried before opening the radio:

- Turn the radio off then back on again to reset the host processor in the controller section of the transceiver board. Then verify that the problem still exists.
- Try to load a good key into the radio. This does two things: First, it ensures that the problem radio is using the same key as the other radios on the system. Second, the keyloading operation itself helps to verify the integrity of the Secure Module. If the attempt to keyload fails, then investigate the cause of the keyloading problem before addressing the original problem.
- Verify that the codeplug in the problem radio is configured correctly for secure operation (see Chapter 6). In particular, make sure that the XL IC PRESENT parameter is configured correctly. A codeplug that is configured incorrectly can manifest itself in numerous ways. However, it usually manifests itself in one or more inoperable features.
- If the SECURENET function operates but the transmitted voice quality is poor at the receiving radio, or if the range of the radio is abnormally short (i.e., the radio’s transmit coverage is not as large as it should be), retune the radio using first the alignment procedure given in Service Manual Volume 1 and then using the secure alignment procedure listed in Chapter 7. Additionally, check the MCS 2000 Accessories Catalog to make sure that the microphone being used is recommended for use with SECURENET.

Identifying A Faulty Secure Module

If, after performing the basic troubleshooting steps given above, the problem still exists, then it is likely that some hardware on the Secure Module or in the radio is faulty. The next logical step in troubleshooting is to determine whether the module hardware or the radio is the source of the problem. To determine which of the two is the actual source of the fault, replace the problem module with one known to be in good working condition. Instructions for removing the existing module and installing another one are provided in Chapter 4, Sections 4-1 and 4-2, respectively. Be certain to reload the key into the radio after replacing the module.

If replacing the module with one known to be in good operating condition does NOT correct the problem, then the original module was not the source of the problem. Reinstall the original module into the radio, and reload key into the radio.

If replacing the module with one known to be in good working condition DOES fix the problem, then the original module that was replaced is faulty and requires repair or replacement. If practical, return the radio to the owner/user with the working module in place.

NOTES

Secure Module Removal And Installation

4

Caution

The transceiver board and Secure Module employ Complementary Metal Oxide Semiconductor (CMOS) devices, which can be damaged severely and permanently by electro-static discharge (ESD). Handle transceiver board and Secure Module

NOTE: The removal procedure in Section 4-1 and the installation procedure in Section 4-2 can be used during troubleshooting to replace a module suspected of being faulty, either temporarily or permanently, with a module known to be in good operating condition. The installation procedure can also be used to retrofit a new Secure Module onto a transceiver board that was not originally equipped with SECURENET.

Section 4-1 Removal

The procedure for removing the Secure Module from the transceiver board is as follows:

1. *High Power models:* Refer to the disassembly and reassembly chapter in Volume 1 of the MCS 2000 Service Manual listed in Table 2 and remove the bottom cover of the radio. This will expose the Secure Shield and Fence. It is not necessary to remove the transceiver board from the radio chassis.

   Low and Mid Power models: Refer to disassembly and reassembly chapter in Volume 1 of the MCS 2000 Service Manual listed in Table 2 and remove the transceiver board from the radio chassis.
2. Refer to Figure 2 and orient the transceiver board as shown.
3. Remove the shield by inserting a small flat bladed screwdriver into the gap between the shield and the fence on the diagonal section of the shield. Taking care not to damage the shield, gently twist the screwdriver causing the shield to lift away from the fence.

Repeat this procedure on the notched corner of the shield. The shield can then be pulled away from the fence.

4. Refer to Figure 3. Reach inside the fence, grasp the module by its edges, and using a slight rocking motion pull the module up to disengage the plug on the module from the mating connector on the transceiver board.

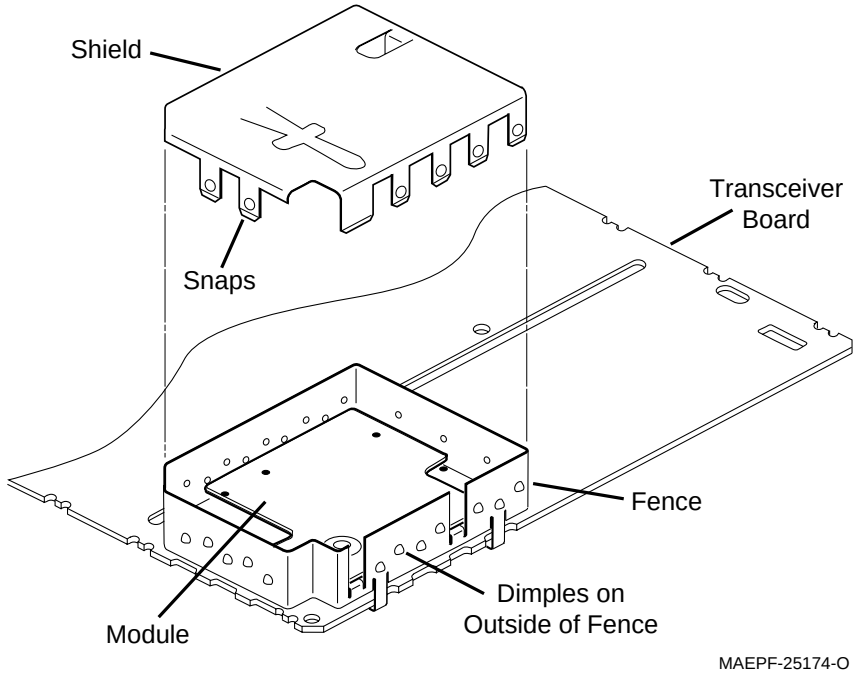


Figure 2 Removal and Installation of Shield

Section 4-2 Installation

The procedure for installing the module on the transceiver board is basically the opposite of the removal procedure.

The module installation procedure is as follows:

1. Refer to Figure 3 and position the Secure Module above the section of the transceiver board surrounded by fence.
2. Align the male connector (P1) on the module with the female connector (J0401) on the transceiver board.
3. Lower the module straight down and plug the male connector on the module carefully and securely into the female connector on the transceiver board. When installed correctly, the module rests on top of the two inside fence tabs shown in Figure 3.

Caution

While handling the shield, be certain that the shape of the anti-tamper spring on the shield is not changed, or that the spring is not otherwise damaged.

Caution

Do not install a shield on a radio if that shield has been installed previously on another radio.

1. Position the shield as shown in Figure 2. Bring the shield down and snap it onto the fence making sure that all of the snaps on the shield are on the outside of the fence. The final assembly should look like the one shown in Figure 1.
2. Refer to the disassembly-and-reassembly chapter in Volume 1 of the MCS 2000 service manual. Install the transceiver board back into the radio and reassemble the radio completely.

   NOTE: The Secure Module will NOT operate properly until the radio is reassembled completely.

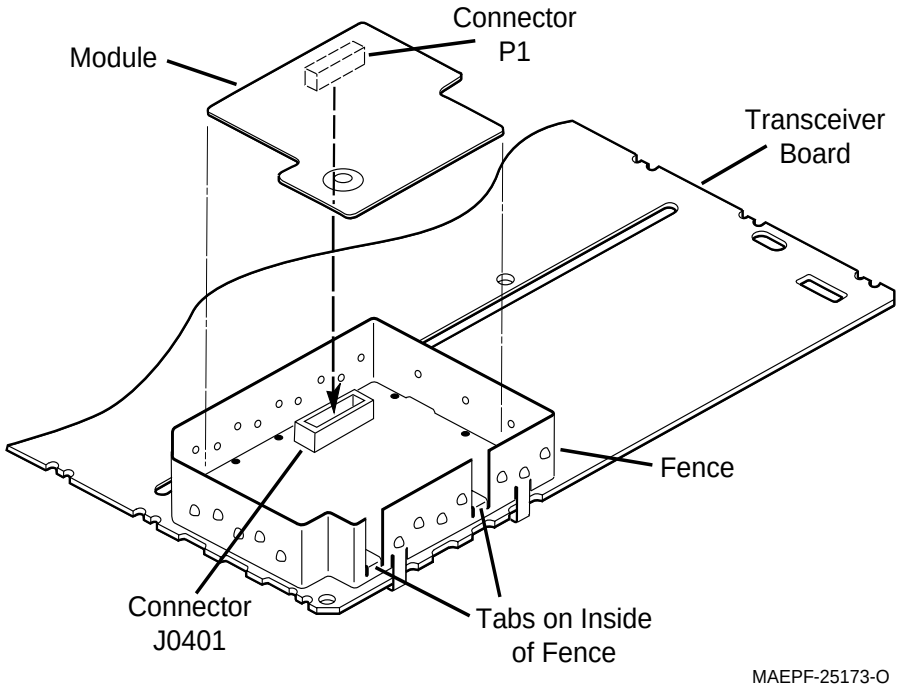


Figure 1 Removal and Installation of Module

NOTES

Troubleshooting And Repairing The Secure Module

5

Caution

The transceiver board and Secure Module employ Complementary Metal Oxide Semiconductor (CMOS) devices, which can be damaged severely and permanently by electro-static discharge (ESD). Handle transceiver board and Secure Module only on an ESD workstation and while you are wearing a grounded ESD wrist strap.

Introduction

You should not attempt to troubleshoot and repair the Secure Module unless it cannot be avoided. If you must troubleshoot and repair the module, the following information may be useful:

- The Secure Module is attached to the transceiver board via connector P1 on the module, which mates with connector J0401 on the transceiver board.
- In some models of the radio (depending on power level and frequency range), the module is physically located on the side of the transceiver board that faces down (i.e., the side facing the metal chassis). In such radios, the module cannot be probed without removing the transceiver board from the radio enclosure.
- In other models of the radio (depending on power level and frequency range), the transceiver board is mounted so that the module is physically located on the side of the transceiver board that faces up (i.e., the side not facing the metal chassis). In such radios, the module is more readily accessible once the enclosure's removable cover and an internal shield, which covers the entire surface of the transceiver board, are removed.

The module can be operated outside its enclosure and separated from the transceiver board by using an extension cable, Motorola stock number 3080370E05. However, after the module is reconnected to the transceiver board using the extension cable, the anti-tamper mechanism on the module must be defeated temporarily with a binder clip, as shown in Figure 4, and the key must be reloaded into the radio.

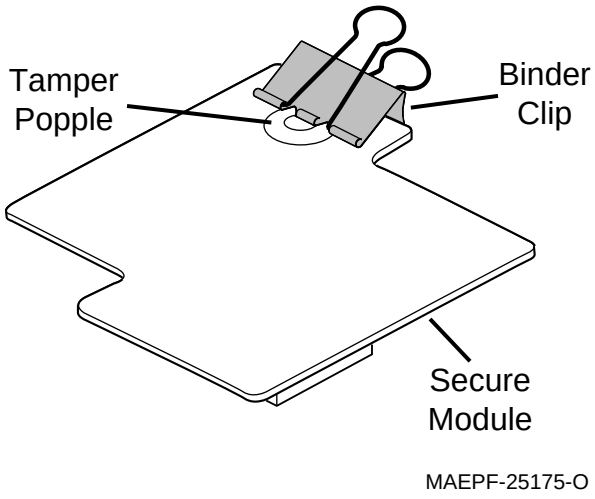


Figure 4 Module with Binder Clip Used to Defeat Anti-Tamper Popple

Troubleshooting

The following is a general procedure for troubleshooting the Secure Module.

1. Turn off radio, and disconnect it from the external source of electrical power.
2. Remove module from transceiver board using procedure in Section 4-1.
3. If the transceiver board had to be removed from the chassis in order to access the Secure Module, mount the transceiver board in a chassis eliminator fixture, as listed in Service Manual Volume 1.
4. Connect module to transceiver board using module extender cable Motorola stock number 3080370E05.
5. Refer to Figure 4 and defeat the anti-tamper circuitry on the module using a binder clip of appropriate size or some similar kind of mechanical device to depress the anti-tamper popple switch.
6. Reattach the radio to the external source of electrical power, turn the radio on, and re-load key.
7. Refer to the following drawings in Chapter 9 for guidance in localizing the fault in the module or radio:
   - Figures 5 through 10; Troubleshooting flowchart diagrams
   - Figure 11; Module component locations and parts list
   - Figure 12; Module schematic diagram

The parts list on Figure 11 lists the reference designators and Motorola part numbers for the components of the Secure Module.

NOTE: Keep in mind that only the common electronic and mechanical

components for the module are readily available through normal Motorola repair parts supply channels. The custom encryption related components (i.e., integrated circuits U1, U3, and U4) are NOT available as repair parts. Consequently, if the fault in the module is caused by one of these three integrated circuits, then the entire module MUST be replaced.

Repair

The module can be repaired to an extent limited primarily by the availability of replacement components. Replacements are not available for any of the three encryption related components (i.e., integrated circuits U1, U3, and U4).

Repairing the module by removing and replacing components, unless carried out with great skill and care and with exactly the right tools, can cause permanent damage to the module's printed circuit board. Field repairs may also decrease the reliability of the module and increase the likelihood of key failures in the future. Excessive heat will warp the printed circuit board. Replacing the anti-tamper switch is not recommended due to critical alignment issues.

NOTES

Programming Radio Codeplug Using RSS

6

Introduction

After the Secure Module is installed in the radio, the radio's codeplug must be modified to activate the SECURENET option. The Radio Service Software (RSS) is used to modify the codeplug. MCS 2000 RSS version 03.00.00 or higher is required, however, whenever possible use the latest version of RSS. The RSS Operation Instructions manual is listed in Table 2.

NOTE: The RSS software has a help screen for every menu and parameter. If there is any confusion as to how to configure a particular parameter, highlight the option and press F1 to access the help screen for that option.

Codeplug Programming Procedure

Set Secure-Equipped Parameter

1. Start RSS program.
2. Press F4 at the MAIN MENU to display the CHANGE/VIEW menu.
3. Press F3 to display the RADIO WIDE CONFIGURATION menu.
4. Press F2 to display the RADIO WIDE OPTIONS menu.
5. Press Tab key to highlight the Secure Equipped field.
6. Press Up or Down arrow key to set the Secure Equipped field to Yes. Leave the RADIO WIDE OPTIONS menu displayed.

Set XL IC Present Parameter

NOTE: The radio codeplug MUST be programmed to indicate whether or not the module is the XL type.

1. Press F6 to display the RADIO WIDE SECURE OPTIONS menu. The XL IC Present field should be highlighted.
2. Refer to Table 1 of this manual to determine whether or not the module used in this radio is the XL type.
3. Press Up or Down arrow key as required to set XL IC Present field to Yes if the module IS the XL type, or to No if the module IS NOT

the XL type.

4. Press F10, F10 to return to the RADIO WIDE CONFIGURATION menu.

Enable Secure Select Button

To allow user control of Secure functionality, a pushbutton on the control head or DTMF microphone must be programmed for selecting Secure operation.

1. Press F3 at the RADIO WIDE CONFIGURATION menu to display the RADIO WIDE FEATURES CONFIGURATION menu.
2. Press F2 to display the CONTROL HEAD menu. The display shows the control head for the radio, including the buttons which are programmable on the DTMF mic, if applicable.

   NOTE: If a secure button (Ø) has already been placed on the control head, make sure that the button being configured for secure matches the location of the existing secure button on the control head.

3. Choose a button to control Secure operation, and-press the Up or Down arrow key as required to select the button option “Sec”.
4. Press F10, F10, F10 to return to the CHANGE/VIEW menu.

Enable Secure/Clear Strapping

For Conventional Personalities

By default, every conventional personality in the radio can be used with Secure by enabling Secure with the Secure Select button (i.e., by default, every conventional personality is set to Secure/Clear Selectable). However, by enabling Secure/Clear Strapping, it is possible to strap a conventional personality to Secure-only, Clear-only, or Secure/Clear-selectable.

Perform the following procedure for each conventional personality to be strapped:

1. Press F6 at the CHANGE/VIEW menu to display the CONVENTIONAL menu.
2. Press F3 to display the CONVENTIONAL PERSONALITY menu.
3. Press F6 to display the CONVENTIONAL SECURE PERSONALITY screen.
4. Press Tab key to highlight the Secure/Clear Strapping field.
5. Press Up or Down arrow key as required to set the Secure/Clear Strapping to Select, Secure, or Clear.
6. Other Secure options are available from this screen. Refer to Table 5 for more information about these options.
7. Press F3 or F4 as required to cycle through all the available personalities. Set the Secure/Clear Strapping as desired for each personality.

8. Press F10, F10, F10 to return to the CHANGE/VIEW menu.

For Trunked Personalities

Perform the following procedure for each trunked personality to be strapped:

1. Press F4 at the CHANGE/VIEW menu to display the TRUNKING menu.
2. Press F4 to display the TRUNKING PERSONALITY menu.
3. Press Tab to highlight the Announcement Group field.
4. If you wish to strap an announcement group, enter the number of the proper announcement group and press Enter. If you do not wish to strap an announcement group, skip to step 6.
5. Press Up or Down arrow key as required to set the Secure/Clear Strapping to Select, Secure or Clear.
6. If you wish to strap a talkgroup, press F7 to select the TRUNKING TALKGROUPS screen. If you do not wish to strap a talkgroup, skip to step 9.
7. For each talkgroup in the personality, press the Tab key and the Up and Down arrow keys as required to configure the strapping of that talkgroup.
8. Press F10 to return to the TRUNKING PERSONALITY menu.
9. If you wish to configure the Revert Announcement Group and Revert Talkgroup strapping, press F8 to select the EMERGENCY DATA CONFIGURATION screen. If you do not wish to configure these options, press F10, F10 to return to the CHANGE/VIEW menu.
10. Press the Tab key as required to highlight the Revert Announcement Group field.
11. Type the number of the proper Revert Announcement Group and press Enter.
12. Press TAB to highlight the Strapping field.
13. Press Up or Down arrow key as required to set the Secure/Clear Strapping to Select, Secure or Clear.
14. Press TAB to highlight the Revert Talkgroup field.
15. Type the number of the proper Revert Talkgroup and press Enter.
16. Press Up or Down arrow key as required to set the Secure/Clear Strapping to Select, Secure or Clear.
17. Press F10, F10, F10 to return to the CHANGE/VIEW menu.

Other Secure Options

There are many other optional Secure parameters in the codeplug that can be configured with the RSS. These options, along with a brief description, are listed in Table 5.

NOTE: Not all of the options will always be available. Some options will only appear after others have been enabled or disabled.

Radio wide secure options are options that are valid for all personalities. These options are found on the RADIO WIDE SECURE OPTIONS menu, and can be reached from the CHANGE/VIEW menu by pressing F3, F2, F6. Per personality secure options are options that can be independently configured for each personality. For conventional personalities these options can be found on the CONVENTIONAL SECURE PERSONALITY screen, and can be reached from the CHANGE/VIEW menu by pressing F6, F3, F6. For trunked personalities these options can be found on the TRUNKING PERSONALITY OPTIONS screen, and can be reached from the CHANGE/VIEW menu by pressing F4, F4, F9.

Table 5 Optional SECURENET Parameters

Parameter	Default	Possible Settings	Radio Wide/Per Channel	Used in Conv or Trunk	Description
Secure equipped	No	Yes or No	Radio wide	Both	Enables Secure operation in a SECURENET equipped radio. The radio will not know it is secure equipped if this parameter is not set.
XL IC Present	No	Yes or No	Radio wide	Both	Informs radio that module is XL type. The Secure Module will not function if this parameter is set incorrectly.
Secure/ Clear Strapping	Select	Select or Clear or Secure	Per channel	Conven-tional	Sets channel to Clear-only, Secure-only or user selectable.
Strapping	Clear	Select or Clear or Secure	Per channel	Trunking	Sets channel to Clear-Only or Secure-Only or user Selectable.
XL Transmit	Enabled	Enabled or Disabled	Per channel	Conven-tional	When enabled, XL synchronization will be used. When disabled, Non-XL synchronization will be used. Messages transmitted with XL synchronization can only be received by radios equipped with the XL IC.
Scan Select	Non-XL&XL	Non-XL or Non-XL&XL	Per channel	Conven-tional	Selects between Non-XL and XL Scan Unsquelch Duration.
Scan Holdoff Strapping	Both	Both or Clear Only or Secure Only	Per channel	Conven-tional	Scan for Clear, Secure, or both on a particular channel.
Rx Modulation	2-Level Rx	Auto Rx or 2-Level Rx	Per channel	Both	Tells radio to look for 2 and 4-level signals or 2-level signals only. Note: When Auto-RX is selected, the radio will *only* receive XL.
Proper Code Detect	Enabled	Enabled or Disabled	Per channel	Both	When enabled, the radio will unmute on secure data only if it was encrypted with the same key used by the receiving radio.
TX Clear Alert Tones	Enabled	Enabled or Disabled	Radio wide	Both	Enables alert tone every time PTT is pressed while in the clear mode.

Table 5 Optional SECURENET Parameters

Parameter	Default	Possible Settings	Radio Wide/Per Channel	Used in Conv or Trunk	Description
Periodic Keyfail Alert Tone	Enabled	Enabled or Disabled	Radio wide	Both	When enabled, a periodic alert tone is generated whenever the radio has lost key and the channel is either strapped secure or the secure select button is depressed.
Non-XL Scan Unsquelch Duration	275 mS	0-6375 mS	Radio wide	Both	When scanning for secure messages, this determines the period of time that the radio will wait on channel for a Non-XL encrypted signal to be detected following a carrier detect.
XL Scan Unsquelch Duration	875 mS	0-6375 mS	Radio wide	Both	When scanning for secure messages, this determines the period of time that the radio will wait on channel for a Non-XL or XL encrypted signal to be detected following a carrier detect.
Echo Mute Time	0 mS	0-1500 mS	Per channel	Conven-tional	Mutes radio after a secure transmission to prevent radio from receiving user's own message through systems with large throughput delays.
Proper Code Enhancer	Enabled	Enabled or Disabled	Radio wide	Both	When enabled, the radio will provide optimal and consistent proper code detect operation. (Not available in all versions of RSS).
Secure Punch Thru	Disabled	Disabled or Always On or 1-254 (Variable Volume Position)	Radio wide	Both	When enabled, this feature should improve secure receive audio intelligibility in high background noise environments (i.e., the radio is at high volume) by boosting the high frequency content of the receive audio. The Secure Punch Thru feature is activated when the radio is receiving in the secure mode and the volume knob is beyond an RSS programmable position.

NOTES

Radio Alignment Procedure

7

General

For optimum secure radio performance, the SECURENET transmit deviation and the receive discriminator level must be set.

Refer to Service Manual Volume 1 for a description of the radio alignment test setup, for an RSS Service Menu overview, and general radio tuning procedures. All normal radio tuning should be performed in the proper sequence before proceeding with SECURENET tuning.

Secure TX Deviation

Transmit deviation balance compensation and transmit deviation limit adjustments should be completed before secure deviation is adjusted..

NOTE: All external signal sources must be removed from the test box prior to performing this alignment procedure.

1. Press F2 at the MAIN menu to display the SERVICE menu.
2. Press F2 to display the TRANSMITTER ALIGNMENT menu.
3. Press F8 to display the SECURE TX DEVIATION softpot. The screen will indicate the test frequency to be used.
4. Press F6 to key radio on the test frequency. The screen will indicate that the radio is transmitting.
5. Measure the deviation on service monitor.

   NOTE: A SECURENET eye pattern usually has a deviation of 4 KHz. The lower than usual deviation setting of 2.91 to 3.06 KHz is required because this alignment procedure uses a 6-KHz sine wave, not SECURENET, to set the deviation.

6. Use the Up and Down arrow keys to obtain a deviation level between 2.91 and 3.06 KHz.
7. Press F6 to dekey radio.
8. Press F8 to program the softpot value into the radio.
9. Press F10, F10 to return to the SERVICE menu.

Secure RX Discriminator Level

1. With Test Box RLN 4460A: With the Meter Selector METER OUT switch set to DISC, connect an AC voltmeter capable of 1-mV resolution on a 2-Volt scale to the AC/DC Meter terminal on the test box.

   With Test Box GTF180B: A wire must be added to pin 25 of the mobile radio test cable radio accessory connector. Connect the positive probe of an AC voltmeter capable of 1-mV resolution on a 2-Volt scale to the free end of this wire and connect the negative probe of the AC voltmeter to ground (pin 4) on the mobile radio test cable radio accessory connector. If addding a wire to the cable is not practical, attach the negative probe of the voltmeter to ground on the radio chassis.

Caution

Do not use the ground terminal on the test box.

2. Press F3 at the SERVICE menu to display the RECEIVER ALIGNMENT menu.
3. Press F8 to display the SECURE RECEIVE DISCRIMINATOR LEVEL softpot. The screen will indicate the receive test frequency to be used.
4. Set RF test generator to the receive test frequency. Set the RF level at the radio antenna port to 1mV (-47dBm) modulated with 3.0 kHz FM deviation of a 1 kHz tone.
5. Use Up and Down arrow keys to set the softpot for a mid-range value of 64.
6. Observe the discriminator level on the AC voltmeter. In most radios it will nominally be 150 mVrms, while in others it will nominally be 450 mVrms.
7. If the discriminator level in the previous step was near the nominal value of 150 mVrms, use the Up and Down arrow keys to obtain a discriminator level between 206 - 218 mVrms (target value of 212 mVrms). However, if the discriminator level in the previous step was near 450 mVrms, use the arrow keys to obtain a discriminator level between 618-654 mVrms (target value of 636 mVrms).
8. Press F8 to program the softpot value into the radio.
9. Press F10, F10, F10 to return to the MAIN menu.

Retrofit Instructions

8

Introduction

This chapter provides instructions for retrofitting a radio to include the SECURENET option.

NOTE: The MCS 2000 Secure Module REQUIRES radio firmware version R3.01 or higher. The Secure Module will NOT operate properly without this software. Consequently, if the radio being retrofitted does not have radio firmware version R3.01 or higher[1], the firmware must be upgraded before retrofitting the radio (or before enabling the secure option).

NOTE: Microphones originally shipped with secure equipped MCS 2000 radios have been optimized to work with SECURENET. Other microphones available for the MCS 2000 may cause slight degradation of audio quality when used with the SECURENET option, and, therefore, are not recommended. Refer to the MCS2000 Accessories Catalog, Motorola Stock Number 68P81080C47, for more information.

1. The radio firmware version can be determined by putting the radio into Test Mode or by reading the codeplug into RSS. To enter Test Mode, press the bottom left key on the Control Head five times within 10 seconds of turning the radio on. The display will show SERVICE followed by a number of the form RX.XX. For the secure option to work this number should be R3.01 or higher. To get out of Test Mode, turn the radio off and on again. If the bottom left key is assigned to something like EMERGENCY, then use RSS to determine the firmware version. This is accomplished by downloading the codeplug into the computer and checking the radio History (F9) for the firmware version.

NOTE: Without modification of the transceiver board, certain early models of the MCS 2000 Radio are not suitable for retrofit to incorporate the SECURENET option. These radios can be identified by the words "Made in the EC" on the label and one of the following model numbers: M01KHM9PW5AN; M01RHM9PW5AN; M01RFM9PW5AN; M01SHM9PW5AN. If you have such a radio, contact Motorola before attempting to retrofit the radio with the SECURENET option.

Table 6 lists the Motorola kit numbers for the SECURENET retrofit kits cross-referenced to encryption type, key retention duration, and applicable KVL model. Each retrofit kit contains the following two items:

1. Secure Module part number HLN65XX (where XX in the part number stand for the two numbers that depend on encryption type and key retention duration).
2. Secure Shield part number 2605894W01.

Table 6 Encryption Algorithm, Key Retention, and KVL vs. Motorola Retrofit Kit Number

Encryption Type	Key Retention	Motorola Retrofit Kit Number for Secure Module	Motorola Model Number for Applicable KVL (See Note at End of Table)
DES	3 Days	HLN1407	T3011_X
DES	Long Term	HLN1416	T3011_X
DES-XL	3 Days	HLN1408	T3011_X
DES-XL	Long Term	HLN1414	T3011_X
DVP	3 Days	HLN1409	T3010_X
DVP	Long Term	HLN1415	T3010_X
DVP-XL	3 Days	HLN1410	T3014_X
DVP-XL	Long Term	HLN1413	T3014_X
DVI-XL	3 Days	HLN1411	T3012_X or T3013_X
DVI-XL	Long Term	HLN1412	T3012_X or T3013_X

NOTE: All KVLs connect to the MCS 2000 radio with cable assembly Motorola Part Number TKN9152.

Retrofit Procedure

To retrofit a radio to incorporate the SECURENET option, perform the following procedure:

1. Refer to the disassembly and reassembly chapter in Volume 1 of the MCS 2000 Service Manual listed in Table 2 and remove the transceiver board from the radio.
2. Refer to Section 4-2 in Chapter 4 of this manual and install the module and shield on the transceiver board.
3. Refer to the disassembly and reassembly chapter in Volume 1 of the MCS 2000 Service Manual, install the transceiver board into the radio, and reassemble the radio.
4. Refer to Chapter 6 in this manual and program the radio codeplug for compatibility with the SECURENET option.
5. Refer to Chapter 7 in this manual and align the radio for the SECURENET option.

NOTE: For SECURENET equipped radios, it is imperative that the radio's power cable is connected directly to the vehicle battery and not to the switched accessory connector.

NOTES

Reference Diagrams

9

This chapter contains the following reference diagrams for the SECURENET option:

- Troubleshooting Flowchart Diagrams
  - Figure 5; Troubleshooting Flowchart Diagram Number 1, Error 09/10
  - Figure 6; Troubleshooting Flowchart Diagram Number 2, No Keyload
  - Figure 7; Troubleshooting Flowchart Diagram Number 3, No Encrypted Mic Audio
  - Figure 8; Troubleshooting Flowchart Diagram Number 4, No Secure Message Reception
  - Figure 9; Troubleshooting Flowchart Diagram Number 5, No Keyload
  - Figure 10; Troubleshooting Flowchart Diagram Number 6, No Transmit Eye Pattern
- Component Locations Diagrams and Parts List
  - Figure 11; SECURENET Module Component Locations and Parts List
- Schematic Diagram

NOTE: Certain components are either included (placed) or not included (not placed) on the Secure Module depending on the module type. Table A, the Parts Placed matrix, is included on Figure 12 to indicate which components are placed or not placed for each SECURENET option type (i.e., kit number).

  - Figure 12; SECURENET Module Schematic Diagram

NOTES

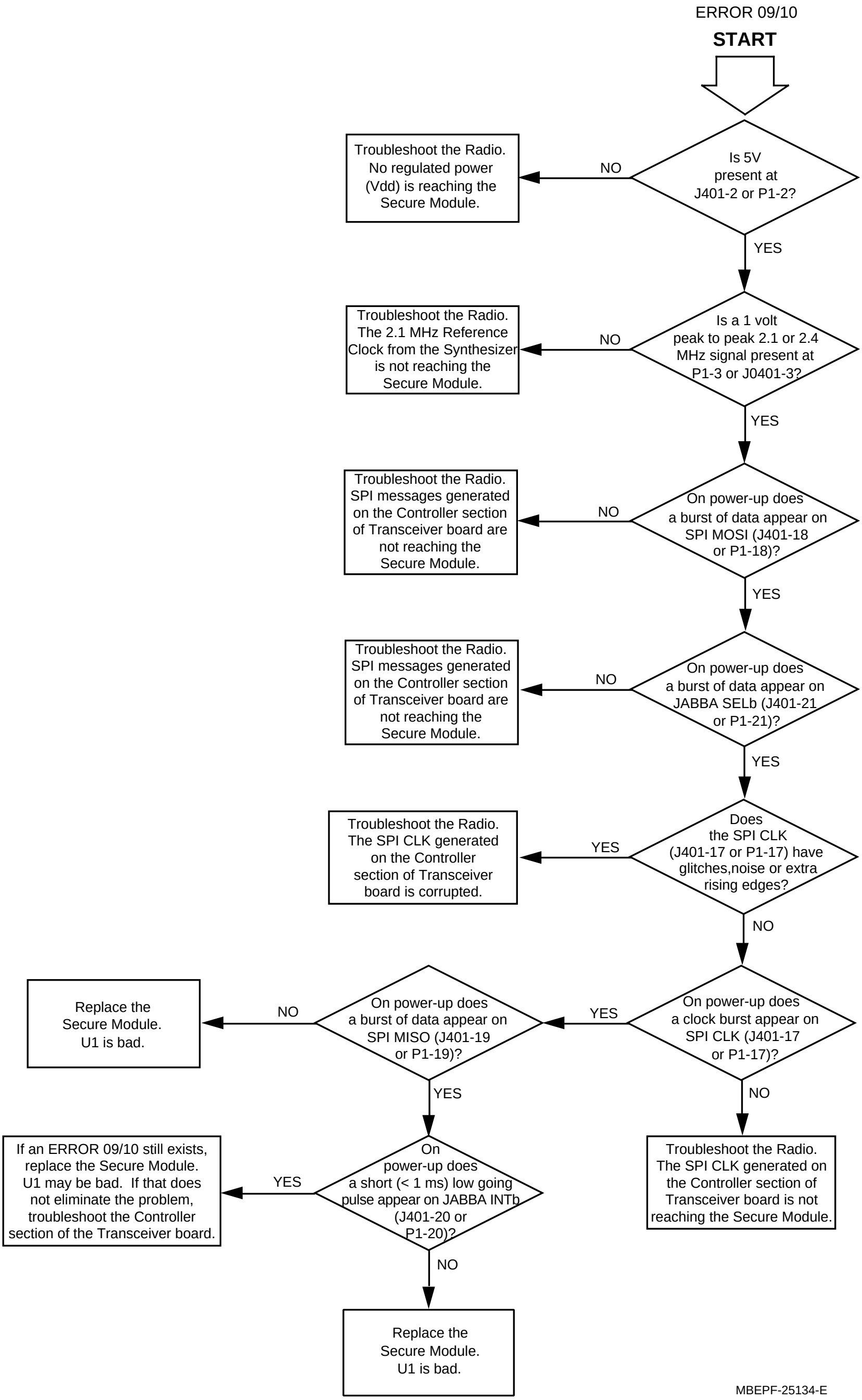
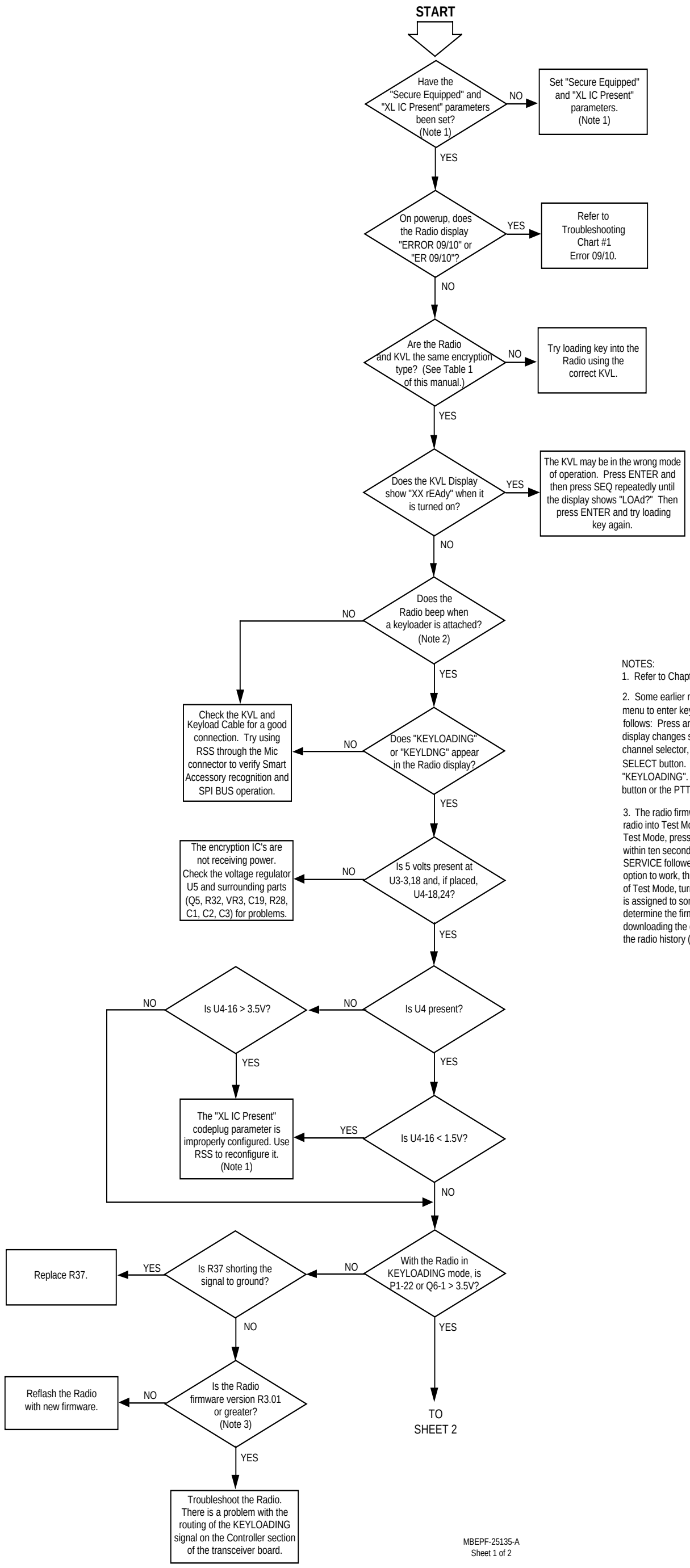


Figure 5 SECURENET Troubleshooting Flowchart No. 1, Error 09/10



NOTES:

1. Refer to Chapter Titled Programming Radio Codeplug using RSS.

2. Some earlier radio models may require use of the keyloading menu to enter keyloading mode. Enter the keyloading mode as follows: Press and hold the SECURENET (Ø) button until the display changes showing the SECURENET menu. Using the channel selector, scroll to the "KEYLOAD" choice, and press the SELECT button. The radio is now in keyload mode and displays "KEYLOADING". Once finished loading key, press the HOME button or the PTT switch to exit the keyload mode.

3. The radio firmware version can be determined by putting the radio into Test Mode or by reading the codeplug into RSS. To enter Test Mode, press the bottom left key on the Control Head five times within ten seconds of turning the radio on. The display will show SERVICE followed by a number of the form RX.XX. For the secure option to work, this number should be R3.01 or higher. To get out of Test Mode, turn the radio off an on again. If the bottom left key is assigned to something like EMERGENCY, then use RSS to determine the firmware version. This is accomplished by downloading the codeplug into the computer and checking the radio history (F9) for the firmware version.

Figure 6 SECURENET Troubleshooting Flowchart No. 2, No Keyload (Sheet 1)

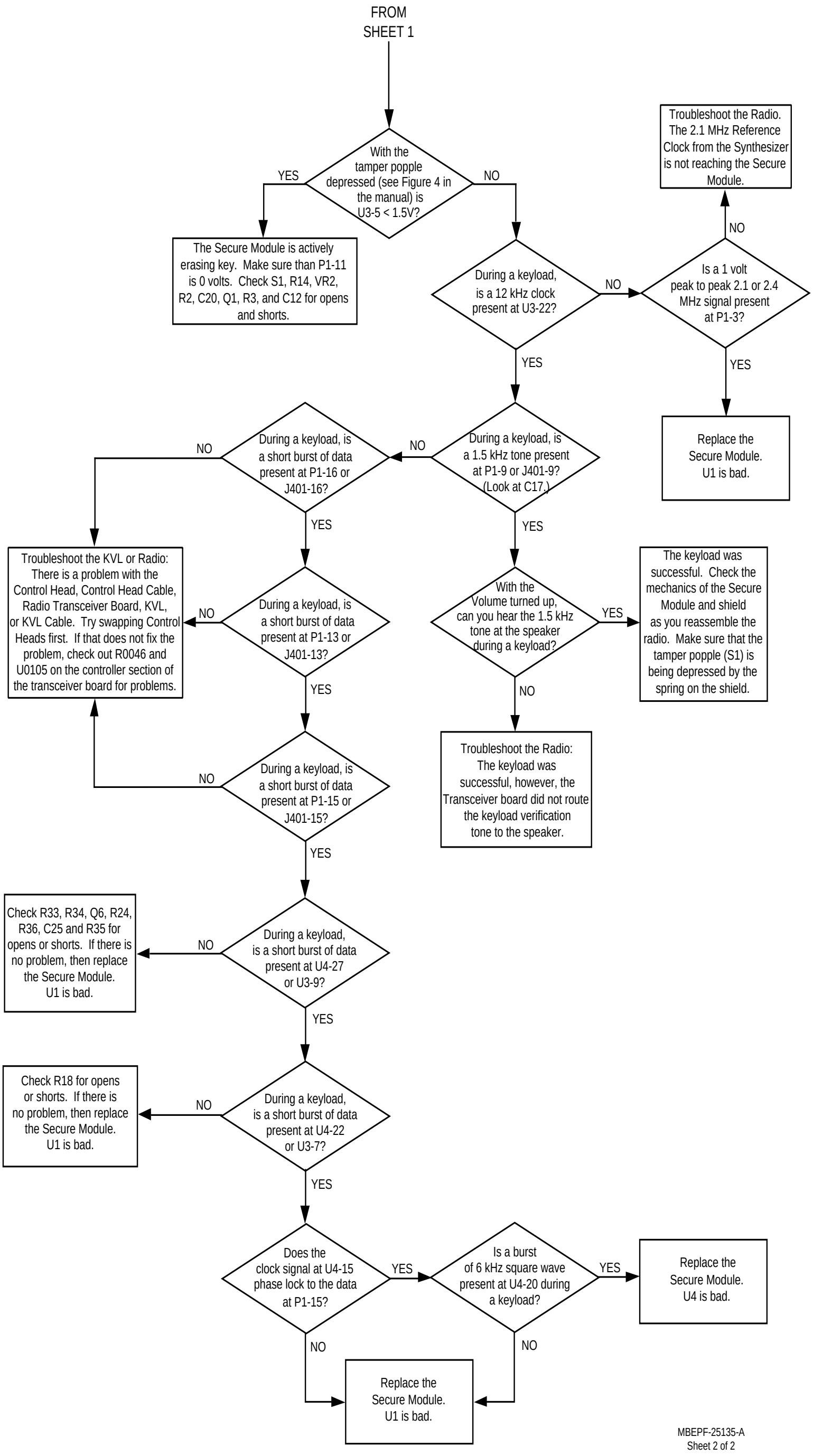


Figure 6 SECURENET Troubleshooting Flowchart No. 2, No Keyload (Sheet 2)

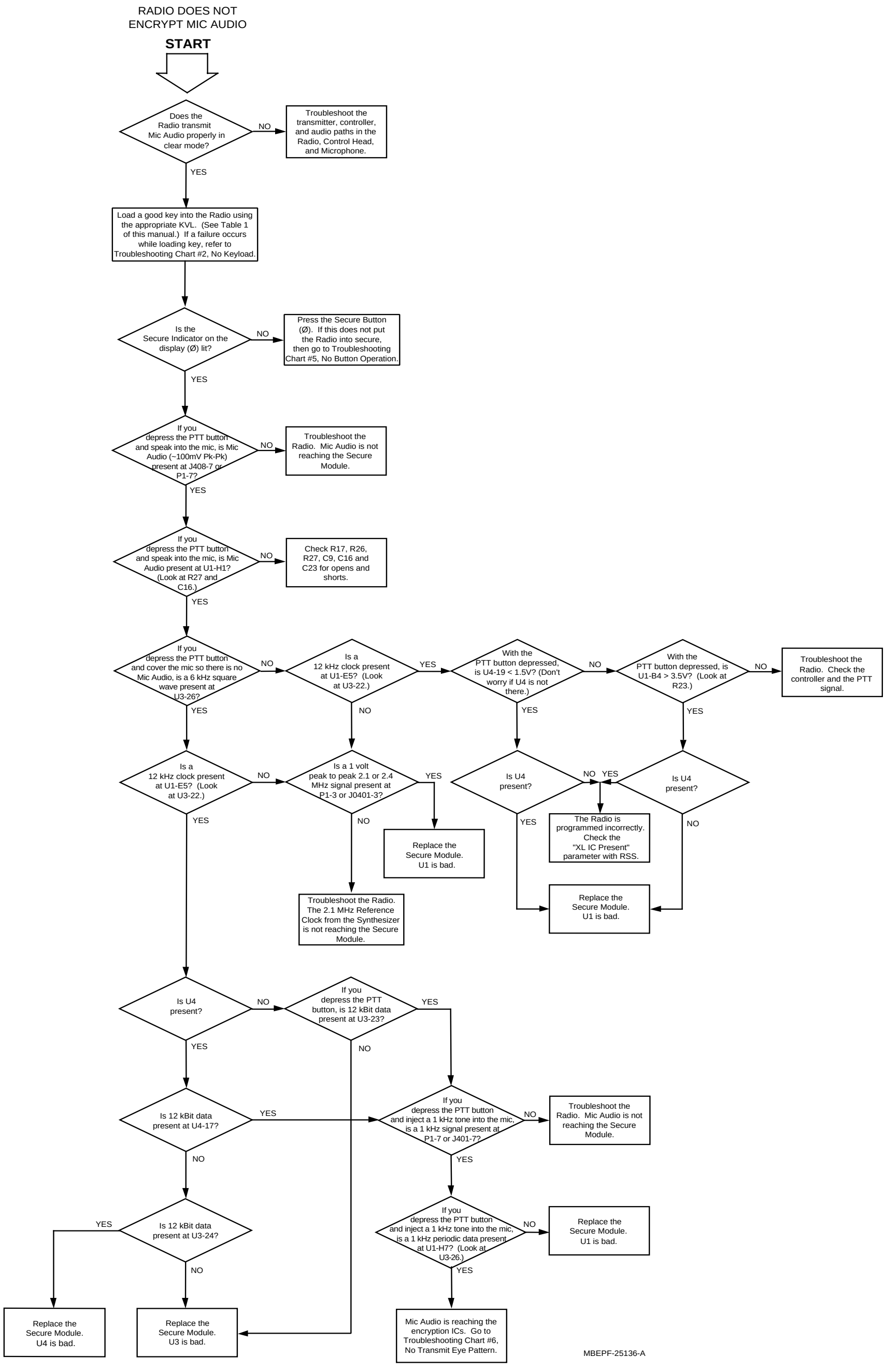


Figure 7 SECURENET Troubleshooting Flowchart No. 3, No Microphone Audio Encryption

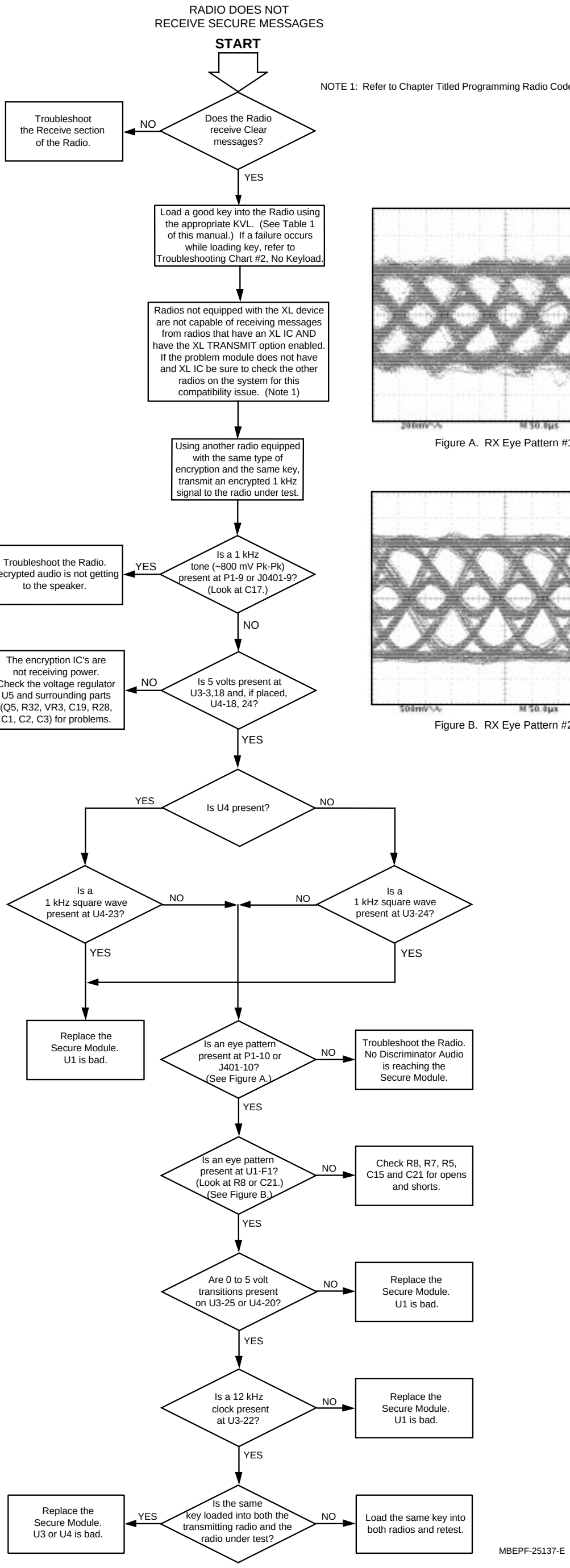


Figure A. RX Eye Pattern #1.

Figure B. RX Eye Pattern #2.

Figure 8 SECURENET Troubleshooting Flowchart No. 4, No Secure Message Reception

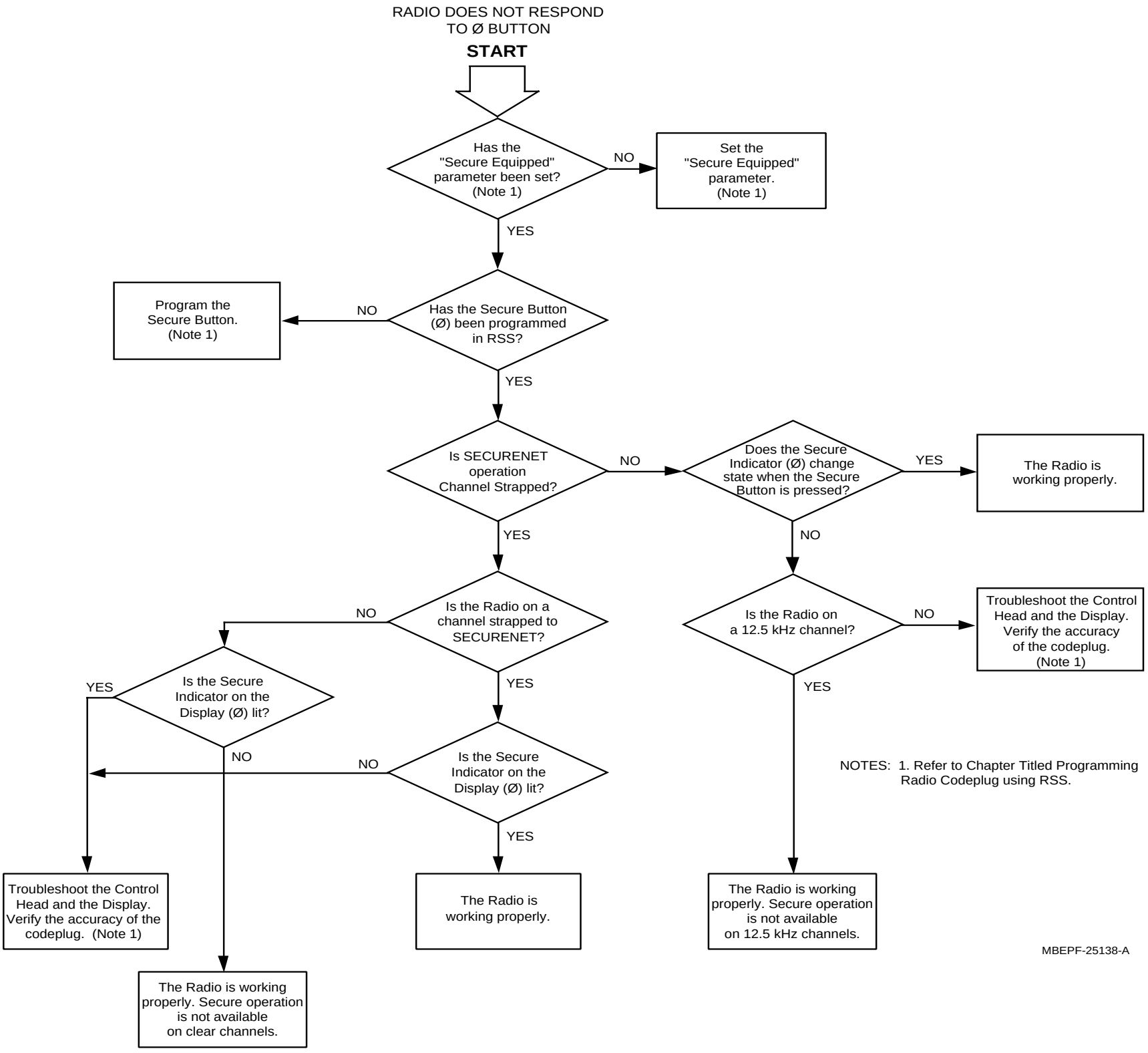


Figure 9 SECURENET Troubleshooting Flowchart No. 5, No Button Operation

Figure A. TX Eye Pattern as seen at C14.

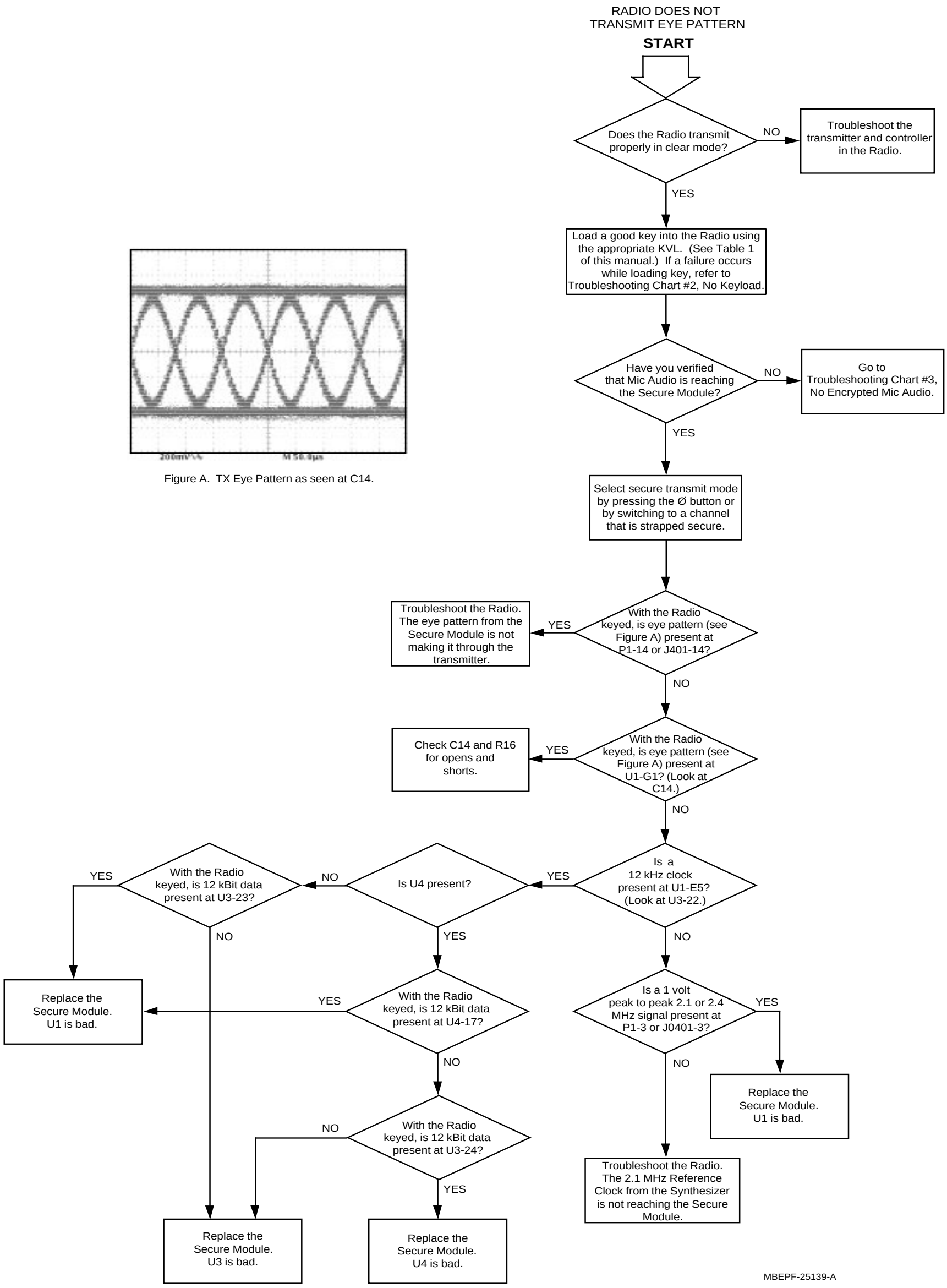
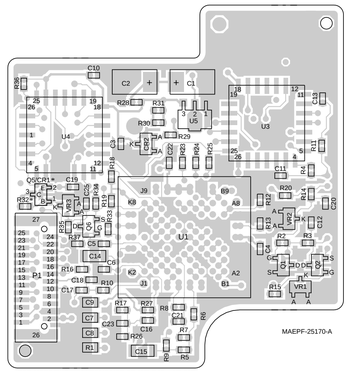
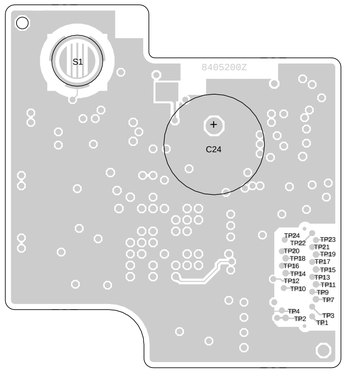


Figure 10 SECURENET Troubleshooting Flowchart No. 6, No Transmit Eye Pattern

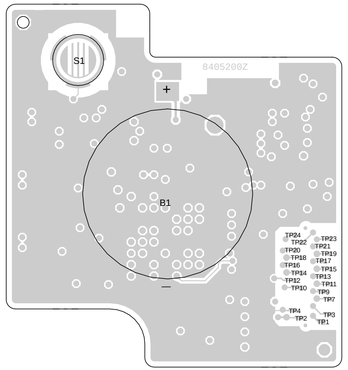
SECURENET Module Component Locations



Connector Side of 3-Day and Long Term Key Retention Type Modules



Capacitor Side of 3-Day Key Retention Type Module



Battery B1 Side of Long Term Key Retention Type Module

SECURENET Module Parts List Kit Numbers: HLN6575B; HLN6576B; HLN6577B; HLN6578B; HLN6579B; HLN6583B; HLN6584B; HLN6585B; HLN6586B; HLN6587B

REFERENCE SYMBOL	MOTOROLA PART NO.	DESCRIPTION
		BATTERIES:
B1		Lithium, coin-cell, 3 Volts
(See Note 1)		and associated insulator/ adhesive pad
		CAPACITORS:
C1	2311049a92	47µF, polarized
C2	2311049a92	47µF, polarized
C3	2113932k15	0.1µF
C4	2113932k15	0.1µF
C5	2113932k15	0.1µF
C6	2113932k15	0.1µF
C7	2113741a59	39nF
C8	2113741a59	39nF
C9	2113741a59	39nF
C10	2113932k15	0.1µF
C11	2113932k15	0.1µF
C12	2113931f25	1nF
C13	2113741f09	220pF
(See Note 2)		
C14	2113743b27	0.68µF
C15	2113743b27	0.68µF
C16	2113939f49	10nF
C17	2113931f49	10nF
C18	2113931f49	10nF
C19	2113932k15	0.1µF
C20	2113932k15	0.1µF
C21	2113740f37	27pF
C22	2113932k15	0.1µF
C23	2113931f49	10nF
C24	2360565a01	0.22F, polarized
(See Note 3)		
C25	2113931F25	1nF
		DIODES:
CR1	4805129m67	Dual
CR2	4880236e05	
		CONNECTORS:
P1	2813916b11	Edge, 25 pins
		TRANSISTORS:
Q1	4805218n11	TMOS FET, N-channel
Q2	4805218n11	TMOS FET, N-channel
Q5	4805128m12	NPN
Q6	4805218n11	TMOS FET, N-channel
		RESISTORS:
R1	0662057g14	110K, 1%
R2	0662057b46	10 Megohms
R3	0662057b05	200K
R4	0662057a97	100K
R5	0662057a49	1K
R6	0662057b22	1 Megohm
R7	0662057b02	150K
R8	0662057b14	470K
R9	0662057b02	150K
R10	0662057a49	1K
R11	0662057a63	3.9K
(See Note 2)		
R12	0662057a97	100K
R13	0662057a97	100K
R14	0662057a49	1K
R15	0662057a49	1K
R16	0662057a49	1K
R17	0662057a49	1K
R18	0662057a80	20K
R19	0662057a80	20K
R20	0662057b47	0
(See Note 2)		
R23	0662057b47	0
(See Note 2)		
R24	0662057b47	0
(See Note 2)		
R25	0662057b47	0
(See Note 2)		
R26	0662057a73	10K
(See Note 2)		
R27	0662057a80	20K
R28	0662057b47	0
R29	0662057a53	1.5K
R30	0662057a41	470
R31	0662057a41	470
R32	0662057a37	10K
R33	0662057a65	4.7K
R34	0662057a65	4.7K
R35	0662057b47	0
R36	0662057b05	200K
R37	0662057a73	10K
		SWITCHES:
S1	3905329w02	Dome type
		INTEGRATED CIRCUITS:
U1	5105835u11	Encryption Support (See Note 4)
U3	5183977m69	Key Generator (DES) (See Note 4)
U3	5105479g33	Key Generator (DVP) (See Note 4)
U3	0105958p92	Key Generator (DVP-XL) (See Note 4)
U3	0105958p91	Key Generator (DVI-XL) (See Note 4)
U4	5105414s21	Range Extension (REX) (See Note 4)
U5	5160880b01	Regulator, 5 Volts
		ZENER DIODES:
VR1	4813830a15	5.6 Volts
VR2	4813830a15	5.6 Volts
VR3	4813830a28	15 Volts
		COMPONENTS WITH NO REFERENCE SYMBOL:
N/A	2605894w01	Secure Shield
N/A	0705892w01	Fence

NOTES:

1. Battery B1 is included (placed) only on the long-term key retention type Secure Module. This battery and its associated insulator/adhesive pad are not field replaceable. Battery B1 is not used in portable applications.

2. Refer to Table A on Figure 12 for placement information related to this component.

3. Capacitor C24 is included (placed) only on the 3-day key retention type Secure Module. This part is not used in portable applications.

4. Integrated circuits U1, U3 and U4 are not available as replacement parts from normal Motorola Supply Channels.

Figure 11 SECURENET Module Component Locations Diagram and Parts List

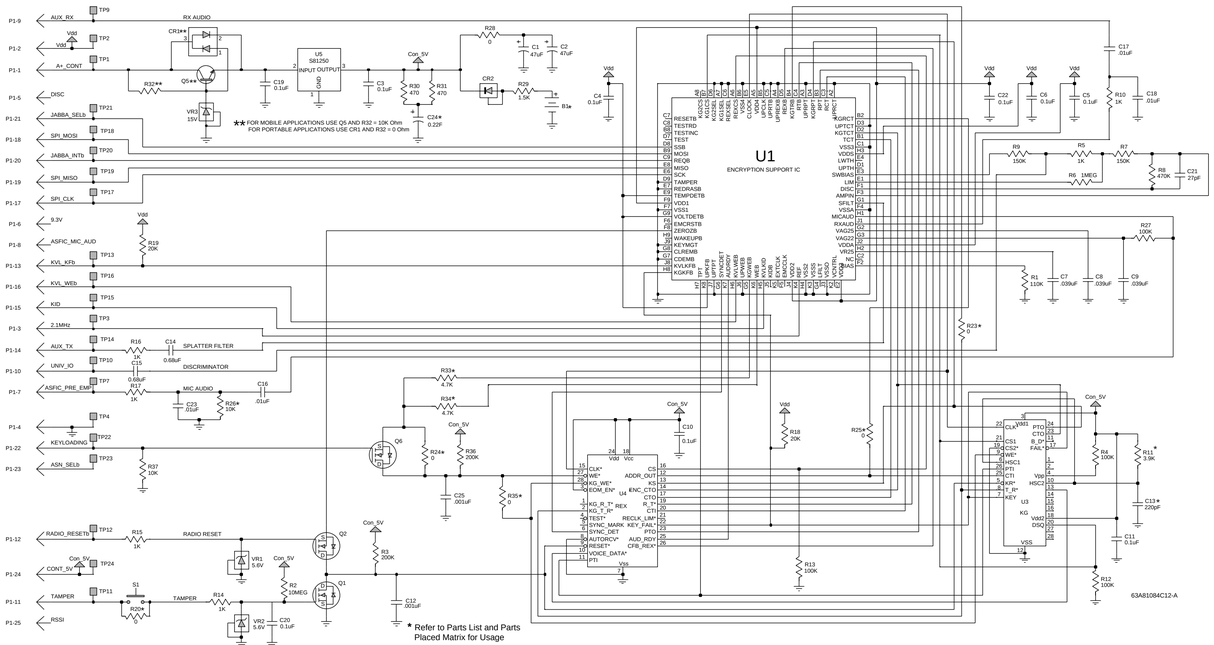


TABLE A PARTS PLACED MATRIX

Kit Number	Encryption	Key Retention Duration	B1	C24	C13	R11	R20, R24, R26, CR1	R23, R25, R33, R35	U4, R34
HLN6575	DES	3-days	Not placed	Placed	Placed	Not placed	Not placed	Placed	Not placed
HLN6576	DES-XL	3-days	Not placed	Placed	Placed	Not placed	Not placed	Not placed	Placed
HLN6577	DVP	3-days	Not placed	Placed	Not placed	Placed	Not placed	Placed	Not placed
HLN6578	DVP-XL	3-days	Not placed	Placed	Not placed	Placed	Not placed	Not placed	Placed
HLN6579	DVI-XL	3-days	Not placed	Placed	Not placed	Placed	Not placed	Not placed	Placed
HLN6587	DES	Long Term	Placed	Not placed	Placed	Not placed	Not placed	Placed	Not placed
HLN6585	DES-XL	Long Term	Placed	Not placed	Placed	Not placed	Not placed	Not placed	Placed
HLN6586	DVP	Long Term	Placed	Not placed	Not placed	Placed	Not placed	Placed	Not placed
HLN6584	DVP-XL	Long Term	Placed	Not placed	Not placed	Placed	Not placed	Not placed	Placed
HLN6583	DVI-XL	Long Term	Placed	Not placed	Not placed	Placed	Not placed	Not placed	Placed

Figure 12 SECURENET Module Schematic Diagram

NOTES

Cut along dotted line

SERVICE MANUAL QUESTIONNAIRE

We believe that reports from users provide valuable information for producing quality manuals. By taking a few moments to answer the following questions as they relate to this specific manual, you can take an active role in the continuing effort to ensure that our manuals contain the most accurate and complete information of benefit to you. Thank you for your cooperation.

In reference to Manual Number: 68P81083C25-O

MCS 2000™ Mobile Radio

1. Please check all the appropriate boxes:

	Complete	Incomplete	Correct	Incorrect	Clear	Confusing	Size Adequate	Size Too Small	Not Covered in This Manual
Disassembly Procedures									
Alignment Procedures									
Exploded Views									
Schematic Diagrams									
Circuit Board Details									
Electrical Parts Lists									
Exploded View Parts List									

2. How would you rate the overall organization of this manual?

☐ excellent ☐ very good ☐ good ☐ fair ☐ poor

3. Did this Service manual provide you with the information necessary to service and maintain the specific equipment?

☐ very much so ☐ generally yes ☐ to some extent ☐ no

4. How do you rate this particular Service Manual?

☐ excellent ☐ very good ☐ good ☐ fair ☐ poor

5. We would appreciate any corrections or recommendations for improving this manual. Please include the specific page number(s) of the diagram or procedure in question.

   a. Disassembly Procedures:(Page No. _____)

   b. Alignment Procedures:(Page No. _____)

   c. Exploded Views:(Page No. _____)

NO POSTAGE
NECESSARY
IF MAILED
IN THE
UNITED STATES

BUSINESS REPLY MAIL

FIRST CLASS MAIL PERMIT NO 9040 FT. LAUDERDALE, FL

POSTAGE WILL BE PAID BY ADDRESSEE

MOTOROLA

Attention: Media and Communication
8000 W. Sunrise Boulevard
Ft. Lauderdale, FL 33322

FOLD FOLD

(Continued)

Please specify the page number along with any corrections or recommendations for improvement.

d. Schematic Diagrams: (Page No. _____)
e. Component Location Details: (Page No. _____)
f. Electrical Parts List: (Page No. _____)
g. Exploded View Parts List: (Page No. _____)

6. General comments/suggestions:

Name:.....
Company:.....

☐Customer ☐COSC ☐MSS ☐FTR ☐Other

Address:.....
City/State/Zip:.....
Phone Number (Please include Area Code):.....

PLEASE USE TAPE TO SEAL

POSTAL REGULATIONS PROHIBIT USE OF STAPLES

REPLACEMENT PARTS ORDERING

ORDERING INFORMATION

When ordering replacement parts or equipment information, the complete identification number should be included. This applies to all components, kits, and chassis. If the component part number is not known, the order should include the number of the chassis or kit of which it is a part, and sufficient description of the desired component to identify it.

Crystal and channel element orders should specify the crystal or channel element type number, crystal and carrier frequency, and the model number in which the part is used.

Orders for active filters, Vibrasender and Vibrasponder resonant reeds should specify type number and frequency, should identify the owner/operator of the communications system in which these items are to be used, and should include any serial numbers stamped on the components being replaced.

MAIL ORDERS

Send written orders to the following addresses:

Replacement Parts/
Test Equipment/Manuals
Crystal Service Items:

Motorola Inc.
Americas Parts Division
Attention: Order Processing
1313 E. Algonquin Road
Schaumburg, IL 60196

Federal Government Orders:

Motorola Inc.
Americas Parts Division
Attention: Order Processing
7230 Parkway Drive
Landover, MD 21076

International Orders:

Motorola Inc.
Americas Parts Division
Attention: International Order Processing
1313 E. Algonquin Road
Schaumburg, IL 60196

TELEPHONE ORDERS

Americas Parts Division:

Call: 1-800-422-4210
1-800-826-1913 (For Federal Government Orders)
1-847-538-8023 (International Orders)

Field Assist Service Training
(FAST VHS Video Tapes):
Call: 847-576-8012

TELEX/FAX ORDERS

Americas Parts Division:

FAX: 847-538-8198 (Domestic)
847-576-3023 (International)

Parts ID: 847-538-8194

Telex: 280127 (Domestic)
403305 (International)

Federal Government Orders:

FAX: 410-712-4991

PARTS CUSTOMER SERVICE

Americas Parts Division:

Call: 1-800-422-4210

Parts Identification:

Call: 847-538-0021

PRODUCT CUSTOMER SERVICE

Customer Response Center
(Sales and Service Assistance):

Call: 1-800-247-2346
FAX: 1-800-232-9272