ISA
Information Security Associates, LLC.

Information Security Associates, LLC

ECR-3 Receiver

OPERATOR'S MANUAL

Rev: January 8, 2008

ENTIRE CONTENTS COPYRIGHT © 2007 INFORMATION SECURITY

Table of Contents

SECTION 1

Features and Panel Layouts

The ECR-3 is a fully synthesized spectrum analyzer with large easy to read displays and easy to use controls. The ECR-3 is a measurement instrument capable of monitoring radio frequency (RF) signals in the range of 50 kHz to 1 GHz to measure frequency, signal level, modulation and other signal characteristics. The ECR-3 is designed for minimal set-up and adjustment.

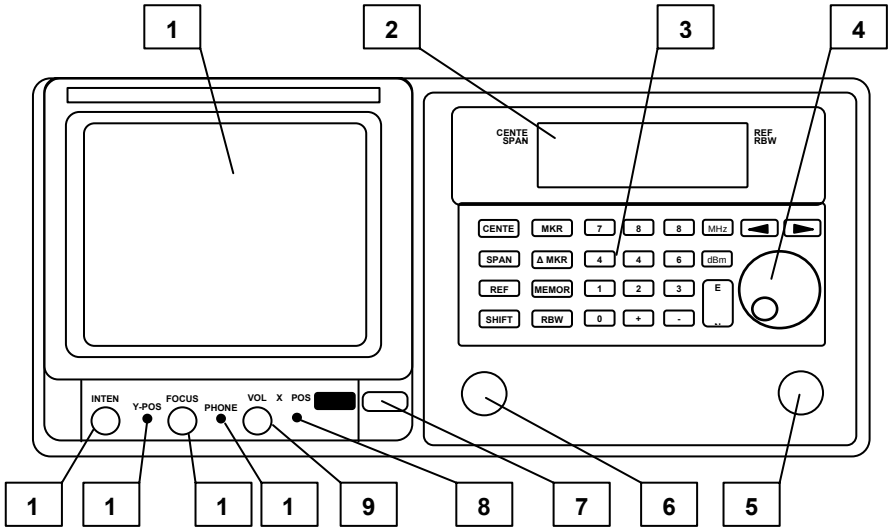

Figure 1 - ECR-3 Front Panel

Item	Description
1	CRT Display, 8 x 10 graticule, 5 inch
2	Liquid Crystal Display (LCD), 4 line x 20 character
3	Keypad, field selection and data entry Spinner
5	RF Input, Coaxial, Type N Female
6	Tracking Generator Output, Not used.
7	Switch, Power ON / OFF
8	Adjustment, CRT Trace Rotation, potentiometer
9	Volume Control (optional demod receiver)
10	Phone Jack, head set output
11	CRT Focus Control Knob
12	Adjustment, CRT Y-axis position, potentiometer
13	CRT Intensity Control Knob

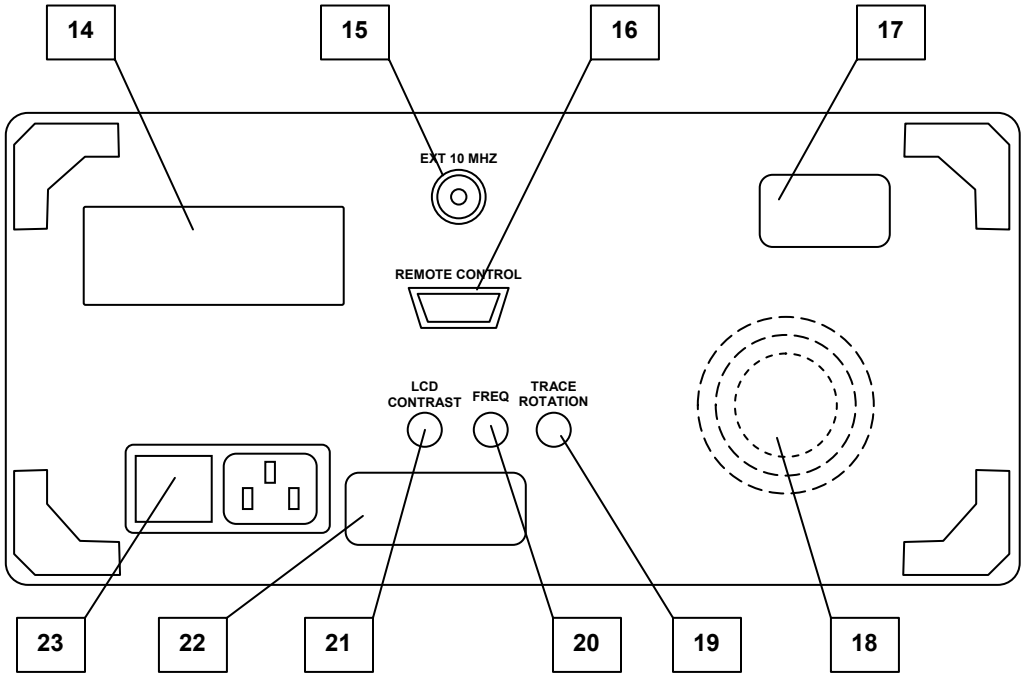

Figure 2 - ECR-3 Rear Panel

Item	Description
14	Panel Label, Usage Warning
15	External calibration signal
16	Connector, DB9, Female, RS-232
17	Serial Number
18	Cooling Fan Vent
19	Adjustment, CRT Trace Rotation
20	Adjustment, Internal Frequency Reference
21	Adjustment, LCD Contrast
22	Panel Label, Input Voltage
23	AC Input, Connector, Voltage Select and Fuse

SECTION 2

Usage Precautions and Recommendations

The following precautions are recommended to insure your safety and to provide protection of the ECR-3.

CAUTION

- Do not place any heavy object on the instrument.
- Avoid severe impacts or rough handling that could damage the ECR-3.
- Use electrostatic discharge precautions while handling and making connections to the ECR-3.
- Do not place wires into the connectors of the ECR-3; use only mating connectors and adapters.
- Do not block or obstruct cooling fan vent openings on side panels or on the rear panel of unit.
- Do not disassemble the instrument; refer the instrument to a factory approved service facility only.

AC POWER INPUT WARNING

AC input should be within the range of selected line voltage +/- 10%.

- Fuses: 90 V – 132 VAC input: T 1.0A / 250V
- Fuses: 198 – 250 VAC input : TO.5A / 250V
- Insure the correct fuse is installed prior to applying voltage for the first time.

AC Line Voltage Setting

On first use and after traveling internationally, be sure to check the AC line voltage settings for compatibility with local power sources. Failure to change line voltage settings to match local AC power will damage the ECR-3 and void the warranty.

If the line voltage does not match input voltage, change as follows:

- Remove AC Power Cord.
- Open cover of AC socket with flat blade screwdriver.
- Remove Selector Cam Drum and rotate to the correct voltage selection.
- Replace Cam Drum.

Grounding

WARNING: To avoid electrical shock, the power cord protective grounding conductor must be connected to earth ground.

Fuse Replacement

WARNING: For continued fire protection, replace the fuse with the specified type and rating only. If the fuse is blown, there is something wrong with the instrument. Determine the cause of the fault before replacing the fuse.

- Disconnect power cord before replacing fuse.

Cleaning

- Disconnect AC Power Cord from the instrument before cleaning.
- Use a soft cloth dampened in a solution of mild detergent and water. Do not spray any liquid into the unit.
- Do not use chemicals or cleaners containing benzene, toluene, xylene, acetone or other harsh chemicals. This may damage the finish.

SECTION 3

Controls

The ECR-3 is a digitally synthesized spectrum analyzer capable of monitoring and displaying RF signal characteristics over a frequency bandwidth of 1 GHz. The RF input is used to connect to the external antenna. The characteristic frequency and level of the signals received are detected and displayed on the CRT.

The ECR-3 contains a demodulator receiver for listening to AM and FM signals.

1. CRT Display

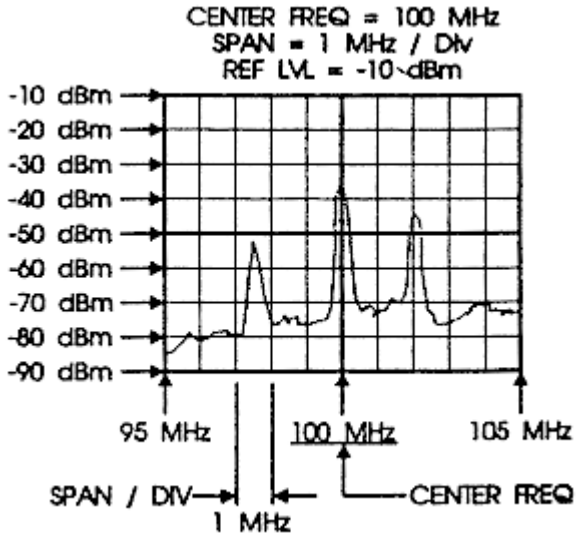

Figure 3 - Spectrum Display

Figure 3 shows a typical spectrum display. This example shows how signals might appear with the following settings: 100 MHz center frequency, a 1 MHz / division span and a reference level of-10 dBm. The 8 by 10 division display indicates RF signal strength on the vertical or y-axis, and frequency on the horizontal or x-axis. The reference level is the top line on the screen, and each vertical division down represents 10 dB. The center frequency is located at the center grid position of the display, and each division across the display represents I MHz. Signals can be evaluated for the presence of room audio and signal strength measurements can be made to track down, localize, and find suspicious signals.

2. Key Pad Controls

The settings for the ECR-3 are selected by keypad entry and appear in the LCD display. They can be changed by numeric entry on the keypad, by rotating the spinner knob, and by the cursor arrows on the keypad.

The blue Shift key on the touchpad is used to access the alternate functions identified by the blue text above the respective keys on the touchpad. For instance, pressing **SHIFT** followed by **DEMOD** accesses the demodulation function which is controlled by the spinner knob and cursor keys.

The following table contains a list of the various selections that can be controlled within the ECR-3, the selection for the field and the means to change or enter data into the field.

Table 1 - Data field selection and entry.

Field	**Selection Key**	**Data Entry**
Center Frequency	**CENTER**	0-9, ".", to directly enter a value. ◄ ► Or **SPINNER** to scroll; **ENTER** or **MHZ** to complete.
Frequency Span	**SPAN**	**SPINNER** to scroll
Resolution Bandwidth	**RBW**	◄ ► Or **SPINNER** to scroll;
Demodulation	**SHIFT, DEMOD**	**SPINNER** to select Demod type
Memory Storage/Recall	**MEMORY**	**SPINNER** selects recall or save; ► to edit Recall/Save number; **SPINNER** scrolls to select number; **ENTER** to complete.
Marker to Peak	**SHIFT,PK>MKR**	Automatic. No data to enter
Set Up	**SHIFT,SET UP**	**SPINNER** to select set up item; To change value or turn function on/off.

Trace	**SHIFT, TRACE**	**SPINNER** to select trace item; ◄ ► To edit selected marker;
Markers	**MKR**	**SPINNER** to select Mkr 1or Mkr 2; ► To edit selected marker; **ENTER** or **MHz** to complete.
Reference Level	**REF LVL**	**SPINNER** to scroll

Center Frequency

Center frequency is a term that refers to the frequency the ECR is turned to. It is the frequency that appears in the Frequency readout on the LCD. The term is derived from that fact that the center of the CRT display corresponds to the tuned frequency. The frequency may be changed by entering the digits, including the decimal point, on the key pad and pressing **ENTER** or **MHz**.

It can also be changed by turning the **SPINNER**. The ◄ ► keys control the size of the tuning steps or how fast the analyzer can be tuned with the spinner knob.

Setting the Center Frequency may change the Span field if the span must be lowered to include the desired frequency. For example, if the Span is set to 100 MHz/div and the Center Frequency is changed to 50 MHz, the span will change from 100 MHz/div to 10 MHz/div.

Span

Span is the width in MHz of the portion of the RF spectrum shown on the CRT. On this analyzer, span is referenced to MHz per division. A span of 2 MHz per division will show a total of 20 MHz across the CRT. This span value may be changed by the **SPINNER** to roll through the list of valid spans.

The range of valid entries is 2 kHz /division through 100 MHz/division plus zero span (0 Hz / div.), which is used for demodulation. Setting the Span may change the Center Frequency field if the frequency must be increased to include the desired Span. For example, if the Center Frequency is 25 MHz and the Span is changed from 5 MHz/div to 10 MHz/div, the Center Frequency will change to 50 MHz.

REF LVL (Reference Level)

Reference Level refers to the value the top of screen in dBm. It is used to visually calculate the apparent strength of a signal shown on the CRT. This reference level value may be changed by the rotating the **SPINNER** to scroll through the list of valid reference levels.

The range of valid entries is +20 dBm to -30 dBm in 10 dB steps. The reference level might be changed to show weak signals better or to show the top of a very strong signal.

RBW (Resolution Bandwidth)

This field sets the Resolution Bandwidth of the unit for Zero Span (0 Hz / div) mode. Resolution bandwidth can only be changed while the span is set to Zero Span. When the span changes to any selection other than Zero-Span, the RBW shown will be the preset value for the given Span. This RBW value may be changed by the rotating the SPINNER to scroll through the list of valid RBWs.

Markers

The ECR-3 has 2 markers. To access the marker screen, press the **MKR** key. Two marker frequencies will be displayed. Accessing the marker frequency fields is performed through the left column of numbers. Move the cursor to the left most position, then use the **SPINNER** to switch between marker 1 and marker 2. Pressing **ENTER** will also switch between the 2 marker fields. The frequency value may be changed by entering the digits, decimal point, followed by the **ENTER** key, or the ◄ ► keys can select a digit within a marker to increment or decrement by using the **SPINNER.** The valid range of entries is 0.000 MHz to 1150.000 MHz.

A marker will appear on the CRT when the marker frequency selected falls within the range of the Center Frequency and Span. For example, if the center frequency selected is 100. MHz and the span is 1 MHz per division, a marker will appear on the screen if the marker frequency is anywhere between 95 MHz and 105 MHz, the 10 MHz span of the screen. If the marker frequency is outside the range of frequencies for a given Center Frequency and Span, a message will indicate its status. If the marker frequency is too high to be displayed on the CRT, instead of the marker level, "Off (high)" will be displayed. If the marker frequency is too low, then "Off (low)" will be displayed.

If the Markers are disabled, then "OFF" is displayed. To disable the markers, simply press the Marker key while in the markers sub-screen.

When the marker is displayed on the CRT, the signal level at the location of the marker will be displayed to the right of the marker frequency. This level will continuously update while in the marker screen.

If the markers are enabled, their position on the CRT will be updated on each Center Frequency change and each Span change. If a Center Frequency or Span is selected such that the marker moves off the CRT screen, they will be off until the parameter is changed to allow the marker to re-appear.

The resolution of the marker on the screen is based on the span selected. There are 50 positions between major divisions on the CRT that a marker can be moved to. In the 100 MHz/div Span, for example, every 2 MHz will move the marker 1 position. On the outside edges of the trace, however, the maximum and minimum marker positions are considered out of range.

PK->MKR (Peak Marker)

This is a peak search function which can be used to automatically tune the receiver to the next signal.

Using marker 1, the ECR-3 begins at the current marker 1 frequency and scans for a peak. When a peak is found in the trace, the marker frequency is updated to show the frequency of the signal and the level of the peak is also displayed. If no peak is found (that is greater in frequency than the current marker position), the marker stops at the end of the trace. Another press of the **PK->MKR** key will start a new search from the frequency point at the left-most edge of the span. If the marker is not active, it will be activated and a new search will begin from the frequency point at the left-most edge of the span. If the marker is active but the bottom half of the LCD display does not show the marker, the peak function will still complete and the marker on the CRT can be viewed.

Trace

The **TRACE** key provides access to the Peak Hold, Average, and Freeze features of the ECR-3. These items are shown on the bottom half of the LCD display. By scrolling, all three items can be accessed.

The Max. Hold Function, when enabled, will maintain a trace showing the maximum signal received for each point in the trace. It can be reset by disabling the function followed by re-enabling. Enabling Markers may be used with the peak hold function when not in zero span.

The Freeze Function, when enabled, will freeze the CRT trace with no subsequent updates to the screen. Updates will resume on the first key press after enabling the Freeze function.

Memory Operations: Save / Recall

The save and recall functions are accessed by pressing the MEMORY key. The bottom half of the screen shows one line for saving and one line for recalling up to 10 setups.

The "Recall" field provides the user with the ability to recall up to 10 different configurations of the ECR-3 including main screen fields, and markers. To recall a new set of parameters, press the ► key to move the cursor to the load number field. Then use the **SPINNER** to change the number from I to 10. While the cursor is on that field, pressing the ► key will load the current state of the ECR-3 with the loaded parameters. The "Save" field provides the user with the ability to save up to 10 configurations of the ECR-3 including the main screen fields, markers, tracking generator fields, and the power meter fields. To save the current state of the unit, press the ► key to move the cursor to the save number field. Then use the SPINNER to change the number from 1 to 10. While the cursor is on that field, pressing the **ENTER** key will save the current state of the ECR-3 into that storage location.

Setup Screen

The setup screen provides access to various parameters. The setup screen functions are accessed by pressing the **SHIFT, RBW** key. The trace will stop updating while in the setup screen. The parameters are accessible using the **SPINNER.** The following identifies the various parameters:

DEMOD (Demodulation)

The ECR-3 is configured to perform FM and AM demodulation. To access this feature, press the **SHIFT, DEMOD** key. The bottom half of the LCD display will show the current demodulation selection that can be changed with the **SPINNER,** rotating counter-clockwise through OFF, AM, Wide, Medium, Narrow. Zero span is activated when DEMOD is activated. The demodulation audio will be routed to the speaker or the front panel audio jack. There are default RBWs associated with the various demodulation modes. For FM-Wide, FM-Medium, and FM-Narrow, the default RBW is 220 kHz. For AM demodulation, the default RBW is 30 kHz. For FM demodulation modes, the RBW may be changed between 220 kHz and 4 MHz. For AM demodulation modes, the RBW may be changed between 3 kHz, 30 kHz, 220 kHz, and 4 MHz. The default RBW is restored each time **SHIFT, DEMOD** is pressed. Therefore, the DEMOD value(AM, WIDE-FM, MEDIUM-FM, NARROW-FM) should be selected first, then the RBW value.

3. System Adjustments

AC Input Selector and Fuse. See Figure 2, Rear Panel, Item 23 and section 2, page 3 for details of setting the proper voltage and fuse.

Intensity. See Figure 1, Front Panel, Item 13. This is a knob adjustment which sets the trace brightness for the signal and marker display on the CRT.

Focus. See Figure 1, Front Panel, Item 11. This is a knob adjustment that sets the focus of the trace and marker displayed on the CRT.

Volume. See Figure 1, Front Panel, Item 9. This is a knob adjustment for the optional receiver volume when the receiver is activated.

Y-Position. See Figure 1, Front Panel, Item 12. This is a flat blade screwdriver adjustment for setting the horizontal position of the displayed trace and marker. Activate the marker function at the current center frequency (see section 3, page 8). Adjust the **Y-Position** so that the bottom of the marker just touches the bottom line of the CRT graticule.

X-Position. See Figure 1, Front Panel, Item 8. This is a flat blade screwdriver adjustment for setting the horizontal position of the displayed trace and marker. Activate the marker function at the current center frequency (see section 3, page 8). Adjust the **X-Position** so that the marker is positioned on top of the center vertical graticule. Adjust trace rotation, if necessary. The Trace Rotation Adjustment may need to be performed at the same time.

Note: X-Position, Y-Position, Trace Rotation may be affect by the orientation of the unit relative to the earth's or other local magnetic field sources. The display will shift in apparent position, but the marker accuracy will not be affected. Simply readjust the X-position, Y-position and Trace rotation when the instrument's position is changed, if it is desired to maintain the display in the precise orientation.

LCD Contrast. See Figure 2, Rear Panel, Item 21. This is a flat blade screwdriver adjustment for setting the contrast of the 4-Line LCD display. Adjust for best contrast at the viewing angle you prefer.

Frequency. See Figure 2, Rear Panel, Item 20. This is a flat blade screwdriver adjustment for setting the reference oscillator frequency for the entire system.

Trace Rotation. See Figure 2, Rear Panel, Item 19. Activate the marker function at the current center frequency (see section 3, page 8). Adjust the **X-Position** so that the marker is positioned on top of the center vertical graticule. Adjust **Trace Rotation**, so that the vertical marker is parallel with the center vertical graticule line.

SECTION 4

Specifications

Frequency

• Frequency range	10 MHz through 1 GHz, usable 30 kHz to 1 GHz
• Frequency resolution	1 kHz
• Span Range	2 kHz to 100 MHz/div in 1-2-5 sequence plus Zero span
• Resolution Bandwidth	3 kHz, 30 kHz, 220 kHz, 4 MHz

Amplitude

• Input level (maximum) for 1 minute	+20 dBm (max. atten.), protected to +30 dBm
• Display level flatness	+/-1.5 dB @ 10 MHz / div dBm to +20 dBm
• Ref. Level range	-30 dBm to +20dBm

Other

• Power	100-130 VAC, 210 to 240 VAC (selectable), Less than 100 VA
• RF input	Type BNC, Female
• External Frequency Reference In	BNC Female
• RS-232 input/output	Computer Interface, DB-9

Functions

- Marker, Marker Delta, Marker to Peak, Marker to Center Frequency
- Trace Average, Trace Max Hold, Trace Freeze
- Internal Reference Signal, Self-test
- System Setup and Recall

SECTION 5

Becoming Familiar With The ECR-3

1. Basic Usage

This section will give you a chance to learn the basic operation of the ECR-3. You will be able to tune in a signal, listen to it and continue tuning to the next signal.

Connect the AC power cord between the receptacle on the rear panel of the ECR-3 to a 120V AC outlet. The ECR-3 is set at the factory for 120 V AC for operation. If only 220V power is available refer to Section 4.1 for instructions on power supply settings.

Connect the right angle whip antenna to the RF input connector on the lower right hand side of the front panel, or for clearer reception, use the remote antenna mount provided with the ECR-3. Attach the hand-held whip antenna to the remote mount's BNC connector. Set the mount on a horizontal surface 8-10 feet away from the ECR-3.

It takes approximately 10-20 seconds for the ECR-3 to become operational. After a short self test the receiver will reset to 1000 MHz, the factory default power on setting. These settings include frequency, resolution bandwidth (RES BW), span, and sensitivity level.

To become familiar with the operation of the ECR-3, run through the following exercise. Sample signals in the FM band will be examined and receiver settings will be explained.

1. Set the Span to 3 MHz/div. Press **SPAN** and use the spinner knob to set the dial to 3. View the Span setting on the 2nd line of the LCD display.

2. Set the center frequency to 100.00 MHz by depressing 1, then 0, then I on the numerical touchpad, then press the **CENTER** touchpad. This puts 101 MHz at the center of the display. If the LED on the TUNE touchpad is not illuminated, press **CENTER** again.

3. Several signals should appear on the CRT. The CRT is displaying a 30 MHz slice of the RF spectrum, from 85 MHz (100 MHz minus half of the span) to 115 MHz (100 MHz plus half the span. If it is hard to identify the signals, remove the antenna and note the changes that occur on the display. Reconnect the antenna and you will see signals rise out of the baseline. FM stations will appear spike-like and rise up at least two horizontal lines.

4. Turn the **SPINNER** knob until the peak of one of the signals is in the center of the screen, lined up with the dashed vertical line. Turning the knob clockwise raises the frequency, counterclockwise lowers the frequency. You will see the signals move across the display.

5. When a signal has been centered, demodulate it to listen to its content. Press **SHIFT**, then **DEMOD**. The LCD display now says DEMOD TYPE: OFF. Turn the **SPINNER** knob counterclockwise and the radio receiver will demodulate to Wide, Medium and Narrow band FM and finally to AM. Usually the audio is best in NARROW FM. You may have to turn the **SPINNER** knob to slightly tune the station for better audio. Remember to turn up the volume with the VOL. (volume) control.

6. To return to sweeping, depress the **SPAN** button and turn the **SPINNER** knob until the span reads 200 kHz/div.

7. Depress the **CENTER** button and the receiver will reset for further tuning.

8. Tune to other signals in the FM band and demodulate them.

2. Other Tuning Techniques

The steps set forth above are used to listen to and identify wide-band signals that are spaced fairly far apart. Let's look at crowded narrow band signals and find out how to resolve them.

1. Tune the ECR-3 to 454 MHz. This can be done by turning the **SPINNER** knob or by entering the frequency directly via the touch pad. To enter it directly, press 4, 5, 4 and press **ENTER** on the upper touchpad. 454 MHz is the beginning of a crowded 2-way radio band.

2. Depress the SPAN button and turn the SPINNER knob until the span reads 100 kHz/div to lower the span to 1 MHz. Now more individual signal detail can be seen on the display.

3. Use the demodulation technique to listen to sounds of these signals.

*Note: The receiver tuning rate is changeable. To change it, press the **MHz** key. Note the frequency readout in the LCD display Use the ◄ ► keys to change which numeric position is highlighted. The receiver will tune more slowly as the smaller number is selected. Larger tuning steps are chosen by larger numbers.*

SECTION 6

Performing a Sweep

The physical area of the sweep must be defined and the location of the operator should be in the approximate middle of the area. The thickness and the materials of the walls will determine the ease with which signals will pass through them. Therefore, some thought should be given to the maximum size of an area which will be covered with one sweep.

As a general rule, the maximum area that can safely be covered in one sweep is a radius of about 100 feet. This is a rather large area, and if a suspicious signal is encountered, it means that you have a very large area to search for the transmitter. Locating a transmitter will be covered later. The sensitivity of the ECR is great enough to pick up even very weak transmitters within an area this size. Generally, in multi-storied commercial buildings, low power signals do not propagate from floor to floor because of steel and concrete used in building construction. A sweep will have to be made on each floor that has an area to be checked.

Utilize the VHF test transmitter supplied with the ECR-3 to "calibrate" the area. First, determine the frequency of the test transmitter. The approximate frequency of operation (in MHz) is marked on the serial number plate on the rear panel of the transmitter.

Tune the ECR-3 tuning knob until the frequency display indicates that frequency or enter the frequency on the numeric touchpad and press TUNE. Set the Span to 2 MHz/div. Turn the transmitter on and a strong signal should appear. Turn the tuning knob to put the signal in the center of the display.

The test transmitter is not frequency stable. It will drift in frequency quite a bit if it is moved around. It may be easier to leave the transmitter in the room you want to do the RF sweep in and carry the receiver to the edges of the area under investigation. As long as the signal is visible on the screen, the area can be successfully covered. If the signal cannot be detected at the edge of the area, more than one sweep will have to be made.

A sound source such as the SS-3, four of which are supplied with the ECR, can be utilized to provide an easily recognizable sound to aid in identifying demodulated signals.

There are advantages and disadvantages in using sound sources:

Advantages:

It is far easier to identify every signal you detect if you know what sound you are listening for.

A sound source will activate a voice activated transmitter.

Disadvantages:

An unusual sound may alert an eavesdropper that a countermeasures sweep is being performed. In that case, he may switch off his transmitter, if he has that capability, but a remote controlled transmitter is extremely rare. In any case, if the eavesdropper is monitoring or has a voice activated recorder attached to his receiver, it will be known that a sweep was made.

Alternative sound sources:

There are several sound sources which may not be as alerting as an SS-3, but bear in mind that the SS-3 was designed for optimum effectiveness and the following items are not as efficient.

A metronome purchased in a music store puts out a recognizable ticking sound. However, the sound level of the ticks may not be great enough to activate a voice activated transmitter within the area.

An FM radio tuned to a classical music station may also be used in each area, but care should be taken that the operator also is listening to the station so that he may identify the sound. A tape recording of an easily recognizable musical piece such as Ravel's Bolero is probably the best non-alerting sound. In any event, if the sweep is being done during non-business hours, there is very little likelihood that the eavesdropper is monitoring the signal and therefore the threat of him turning off the transmitter is essentially nonexistent.

If a transmitter is in the area and its receiver is connected to a VOX (sound activated transmitter) and the receiver is on, regardless of the sound source used during the sweep, there is a strong likelihood that the sweep will be detected. It is virtually impossible to make a sweep without creating sounds of some sort and any activity at an unusual hour or creating unusual sounds will be detected by the eavesdropper may be enough to tip off the operation.

Performing a Sweep

To perform an RF sweep, it is best to start at 1000 MHz and tune down. Set the receiver as follows:

1. Turn on the ECR-3 by depressing the POWER button.

2. Press l,0,0,0, on the keypad and then push **ENTER,** setting the receiver to 1000 MHz.

3. Depress the **SPAN** button. Turn the **SPINNER** knob clockwise until the span reads 200 kHz./div.

4. Depress the **REF LVL** and turn the **SPINNER** knob until the **Ref Lvl** on the LCD display reads -- 30 dBm (fully counterclockwise).

5. Depress the **CENTER** button, the center should read 1000. Use the ► key to place the cursor on the third zero (1000.00).

6. Rotate the **SPINNER** knob counterclockwise. This tunes the receiver down in frequency.

7. When you come to a signal that you want to listen to, Press **SHIFT, DEMOD**. The screen now says DEMOD TYPE: OFF. Turn the **SPINNER** knob counterclockwise and the radio receiver will demodulate to wide, medium and narrow FM and finally to AM. Usually the audio is best in NARROW FM. You may have to press the **CENTER** button and use the spinner knob to slightly tune the signal for better audio.

To return to sweeping, depress the SPAN button and turn the **SPINNER** knob until the span reads 200 kHz/div.

Depress the **CENTER** button and the receiver will reset itself for further tuning.

SECTION 7

THE RF SPECTRUM

This section describes the radio spectrum covered by the ECR-3. Generally, an RF sweep is made from the top end of the spectrum down, so the description begins with the first groups of signals the ECR-3 tunes through.

The first group of signals encountered is at about 930 MHz. These are paging and data transmitters. Between 928 and 900 is a band for low powered consumer products. This includes video transmitters and 900 MHz cordless phones.

The cellular telephone band is from 894-869 MHz for the base to mobile transmissions and 854 MHz to 824 MHz for the mobile to base transmissions.

There are two-way communications between 869 and 854.

The UHF television band extends from 806 MHz down to 470 MHz. Set the SPAN to 10 MHz to tune through this relatively vacant area. You will encounter several television stations. A television signal consists of two parts. The audio signal is an FM signal and can be demodulated the same as any other FM signal. The video or picture portion of the signal will be 4.5 MHz lower in frequency than the audio for that channel. The video is an AM signal which may be identified by a steady buzz. The TV channels are normally spaced 6 MHz apart and adjacent channels are not assigned in the same area to eliminate interference between stations.

A UHF mobile band extends from 470 MHz down to 450 MHz and is fairly crowded with signals in urban areas, especially around 454 MHz. A lightly populated Amateur Radio Band is located between 450 and 420 MHz. Between 420 and 400 MHz you may find a radar signals from an airport or a search radar. Radar signals may be identified by their characteristic buzz. If a rotating antenna is involved at the radar station, the buzz will last for a second or two and be repeated every 15 to 30 seconds as the antenna makes a complete revolution. Set the Span to 1 MHz/div to look at this band.

Between 440 and 220 MHz there are very few signals since these frequencies are reserved for military use. From 225 to 220 MHz there is a seldom used band. From 216 to 174 MHz you will

find television Channels 13 through 7. From 174 MHz to 148 MHz will be public service signals such as police and fire, taxi cabs, mobile radio-telephones, and weather broadcasts. The weather broadcasts are at about 162 MHz. The aviation band is 136 to 108 MHz and is AM whereas the signals previously heard were almost all FM with the exception of the television video. Between 148 and 144 MHz is the two meter ham band which is mostly a mobile repeater type operation.

The FM commercial broadcast band extends from 108 to 88 MHz. Be very careful when tuning this band since easily obtainable transmitters such as those sold by mail order and by Radio Shack are found in or adjacent to this band.

Television channels 6 through 2 appear from 88 to 54 MHz. What at one time was Channel 1 is now an amateur radio ham band from 54 to 50 MHz. Low power walkie-talkies appear between 49 and 50 MHz. Also in this range are various wireless microphone and cordless telephones.

Two-way mobile, public service, etc.., are between 49 and 30 MHz. A ham band is at 30 through 28 MHz and the citizens band is at 27 MHz.

Above 30 MHz you will normally receive only FM signals with the exception of television picture signals and aircraft between 115 and 130 MHz. Below 30 MHz you will normally only find AM signals.

Between 1.5 and 27 MHz you will find mostly ship to shore, ham bands, and the foreign long distance broadcast band. This is sometimes referred to as the short wave band. The amount and strength of the short wave signals depend upon the time of day, sunspot cycles, etc. and will vary considerably. After dark there will be very few foreign signals present. This is especially important to remember when using the chart plotter and comparing charts taken at different times of the day.

The AM broadcast band extends from 1.5 to .5 MHz or as it is sometimes referred to, 1500 kHz to 500 kHz (Kilohertz). Below 500 Hz you will seldom encounter a signal but there may be signals such as marine broadcast, airport weather stations, navigation signals, etc.

Power line carrier current transmitters will be found below 500 kHz.

SECTION 8

POWER LINE DETECTION SYSTEM

The Power Line Detection System has been designed to check for listening devices operating at very low radio frequencies on the AC power lines. These eavesdropping devices are commonly called Carrier Current Transmitters and are similar in operation to wireless intercoms. They use the AC power lines as a common antenna. Carrier current transmitters usually operate at frequencies below 500 kHz.

In most cases, the RF signal from a carrier current transmitter will not pass through a transformer, so the receiver and listening post or recorder must be on the same side of the transformer. It is possible, however, to bypass the transformer with a capacitor, but this installation is dangerous and is probably not found in the civilian environment.

To make a carrier current sweep:

Receiver Set up

Tune the receiver to 0.5 MHz using the tuning knob or by pressing 0.5 on the numerical touchpad, followed by pressing the **ENTER** button. Set the span to 1 MHz by pressing **SPAN** and turning the **SPINNER** until the screen reads span: 100 KHz/div.

Connect the Power line Adapter to an AC outlet and to the ECR-3 RF input. Several strong signals will appear on the display.

Use the tuning knob to move the cursor to the highest frequency signal on the display. When you come to a signal that you want to listen to, Press **SHIFT, DEMOD**. The LCD display now shows DEMOD TYPE: OFF. Turn the **SPINNER** knob counterclockwise and the radio receiver will demodulate to WIDE, MEDIUM and Narrow FM and finally to AM. Usually the audio is best in NARROW FM. You may have to press the **CENTER** button and slightly tune the station for better audio using the **SPINNER** knob.

Check each signal in this manner.

If you select a signal higher than the center of the display, the display will change and put the selected signal in the center when you switch back to the display from the listen mode. Just remember this signal selection process and put the cursor on the next lower signal and you will end up at the original screen setting. Be sure to check all of the signals.

SECTION 9

DETECTION OF SURREPTITIOUS TELEVISION TRANSMITTERS

Tune in a broadcast TV video signal. Refer to Section 7 for hints on where to find such signals. A television signal consists of the video portion and the audio portion. When listening to the TV video signal, a buzzing sound will be heard when AM demodulation is used.

A broadcast television signal consists of three separate signals: a video signal, an audio signal, and a signal called a color burst. The video signal can be identified as the broad signal as shown on the left in Figure 9.1. The audio signal on the far right and is much narrower, compared to the video. The color burst is a little to the left of the audio.

The audio and video signals are separated by 4.5 MHz in North America. The audio is always the higher frequency.

All broadcast television will have an audio signal. Any television signal containing an identifiable audio component can be assumed to be a legitimate signal. Any television signal where the audio is not identifiable should be suspect. It may be a legitimate signal from a station that is not transmitting a show or it may be a covert video transmitter. The following section tells how to identify a video signal.

Set the Span to 1 MHz/div. Tune the signal so that it is very slightly to the left or right of the center.

Now change to Zero Span. Press the **SPAN** and use the **SPINNER** knob to set the span.

The CRT will show the video signal wave form. Watch the display. Look at the area between the spikes. This is the white level, the amount of white in the TV picture. Changes in the appearance of this signal content when there is no motion in the area of the sweep indicate that the signal is coming from elsewhere and that you are seeing the scene changing on a TV broadcast. If there is no motion in the area, the white level should not change.

To dramatically affect the white level, turn the lights off in each area. If the signal is broadcasting a view of something in the area under investigation, the signal will change very noticeably. If there is no change in the display, the signal is not transmitting a view of the area.

SECTION 10

TELEPHONE TESTING APPLICATIONS

The ECR-3 can be used for several applications in detecting eavesdropping attacks on telephone instruments and systems. These include detection of both telephone and room audio transmitters that use the phone line for their transmission medium very much like a carrier current transmitter uses the AC power lines as its antenna.

The ECR-3 can detect RF energy from a radiating free space transmitter when its signal couples to the telephone line. The activation of a series type telephone transmitter can be seen on the ECR-3's CRT when the phone goes off hook.

1. Carrier Current Telephone Transmitter Detection

Carrier Current telephone transmitters can be used in standard single line phone installations or be installed in electronic telephone instruments used in PBX environments.

It is likely that this type of transmitters will require an external power source and not be powered by the central office or PBX. Keep in mind that they could be installed elsewhere on the wiring, rather than just in the telephone instrument. Transmitters of this type are going to be low frequency transmitters since the length of the antenna (the phone line) is ideal for low frequency transmission and not particularly good at higher frequencies. For our purposes, transmitters of this type can be assumed to be operating at frequencies below 1 Megahertz.

ECR-3 Set-up:

To detect this type of transmitter, the ECR-3 has to be connected to the telephone line.

ISA ETA series telephone analyzers are equipped with a BNC type coaxial connector. This connector is connected to whichever wires are selected by the ETA's line selection switches. The ETA therefore can be used as the interface between the ECR-3 and the telephone line.

1. Connect the coax cable used with the AC Power line Adapter between the ECR-3's RF input and the ETA's BNC connector. Set the ETA's line selection switches to 4 and 5.

2. Set the screen to read 1 MHz full scale. Depress 1.0 0 on the key and press **ENTER**. The center should read 1 MHz. This is the same set up as for the AC carrier current tests.

3. Check each signal that appears on the display for room audio.

2. Detecting Radiating Transmitters at the Telephone:

A radiating transmitter on a phone line will be either a series type transmitter that is powered by the telephone line or a parallel type transmitter that has its own power source. Both types generally do not transmit when the phone is not in use.

Neither is usually designed to use the phone line as an antenna; they have their own antennas designed for efficiency at their operating frequencies.

Under certain conditions the signal radiated by this kind of transmitter can couple with the phone line and propagate for some distance. These signals can be detected by the ECR-3 when connected to the phone line as described in the previous section. However, the operator can assume that these transmitters will be operating at frequencies in excess of 30 Megahertz.

Series or parallel telephone transmitters are designed so that they do not operate when the telephone is not in use. They only turn on and transmit when the phone is off hook. It is possible to detect this type of transmitter by seeing its signal appear on the ECR's CRT when a phone is taken off hook. These types of transmitters often radiate harmonics when they transmit, to, making them easier to identify.

<u>ECR-3 Set-up:</u>

1. Set the ECR-3 to display the full spectrum on the screen. Do this by pressing the 5,0,0 buttons and then **ENTER**. The center frequency is now set to 500 MHz. Set the span to 100 MHz/div by pressing **SPAN** and turning the **SPINNER** knob fully clockwise until the span reads 100 MHz/Div. This sets the span to 1000 MHz, and the center frequency to 500 MHz. You are now looking at the full RF spectrum from 10 kHz to 1000 MHz.

2. Connect the whip antenna to the RF input and extend it.

3. Bring the antenna to within a couple of feet of the telephone instrument. Watch the CRT display carefully while taking the phone off-hook. The fundamental signal and harmonics from any near-by telephone transmitter will appear on the CRT. Since you are close to the telephone, the signal from a transmitter in the phone or on the line will be stronger than other signals.

This test should be done at each phone in a residence, even if they are connected to the same line, and at each phone in an office.

SECTION 11

IDENTIFYING AND LOCATING HIDDEN TRANSMITTERS

1. How To Identify an Eavesdropping Transmitter

An eavesdropping transmitter may be identified by its demodulated audio which is generally unlike audio heard on other transmissions. If there is no sound in the area, the demodulated audio sounds hollow with virtually no other noise in the signal. If a sound source is being used, the sound source will be heard, though perhaps somewhat unclearly if the source is not close to the transmitter's microphone. Experimenting with the test transmitter supplied with the ECR-3 will familiarize you with the distinctive sounds.

Another clue in identifying a transmitter is to make a note of the frequency and look for multiples of it. These signals are called *harmonics*. Almost all eavesdropping devices create harmonics which occur at whole number multiples of the fundamental or operating frequency. For example, a transmitter operating at 110 MHz will produce harmonics at 220 MHz, 330 MHz, 440 MHz and so on. If a transmitter is at 150 MHz, harmonics can be found at 300, 450, 600 and 750 MHz.

Even if there is no recognizable audio on the signal, it still needs to be identified. In order for and area to be deem free of transmitters, the rule is that every signal must be identified as a legitimate transmission, a spurious emission from some electronic equipment, or as not emanating from the area under investigation.

To tell if the signal is coming from an area outside of the area being swept, simply move the receiver sixty to eighty feet. If the signal strength does not change significantly or increases, it is emanating from outside of the area. If the strength lessens dramatically, it is coming from the area being swept and is likely to be an emanation from a piece of electronic equipment.

To tell if it is emanating from electronic equipment, turn off equipment in the area one piece at a time. When the right piece has been turned off, the signal will cease. Typical sources of this type of signal are computers, printers, fax machines and the like. FM radios often have a signal radiating from them. This is a local oscillator, used in tuning a station, and is 10.7 MHz above the frequency the radio is tuned to.

The other way to track down a signal, legitimate or a bug, is by the signal strength method described below.

2. Locating A Hidden Transmitter

The easiest way to locate an eavesdropping transmitter is to approximate its location by turning off the sound sources one at a time while listening to the signal until the sound source that is closest to the device is heard to go off. Then locate the microphone by talking or making other sounds in the area. The closer you get, the clearer the audio will become.

If you are not using sound sources, have an assistant move throughout the coverage area making a sound, such as describing where he is. When you hear the voice clearly, make a note of the area. Relocate the ECR-3 to that area.

Use the hand-held antenna with the plastic handle. Connect it to the receiver by using the 10 foot coax cable. Do not extend the antenna. Use it in its collapsed state.

Move around the room with the shortened antenna, watching the display on the ECR. As you get closer to the transmitter, the signal will grow larger on the ECR's display. If the signal increases to the point that it is close to the top of the CRT display, decrease the ECR's sensitivity by depressing the **REF LVL**. Use the **SPINNER** knob to change the reading of the Ref Lvl on the top right of the LCD until the signal is now near the bottom of the CRT display. As you get even closer to the transmitter, you may have to put more attenuation into the system. Once you have decreased the sensitivity and made the signal strong on the display, the antenna is within inches of the transmitter.

Another method is to locate the transmitter by tapping. This technique presumes that you have a good idea of the area that the transmitter is in. Tap very gently on objects in the area. Tap so lightly that you can barely hear the sound. A pencil eraser is a good tool to use. With the ECR tuned to the transmitter and in audio mode, listen for the tapping. It will be very apparent when you get within a couple of inches of the transmitter's microphone. This method works particularly well when trying to locate a carrier current transmitter.

SECTION 12

ACCESSORIES

ACCESSORY	QUANTITY	PART NUMBER
N to BNC adapter	1	5871 installed on receiver
Headset	1	41015
Accessory case	1	41021
Hand held antenna	1	41027
Whip antenna	1	41036
BNC to BNC cable, 3 feet	1	41040
Carrier current adapter	1	41042
Carrier current test transmitter	1	41044
UHF test transmitter	1	41045
AC power cable,	1	41151
AC 2 to 3 wire adapter	1	41054
Training tape	1	41076
SS-3 sound sources	4	41180
Operator's manual	1	41199
Short form instructions	1	41200

Options

Padded soft carrying case	1	42015
Hard shipping/carrying case	1	42016

WARRANTY

Information Security Associates, LLC, warrants to the original user that its products are free from defect in workmanship and material for a period of one year from the date of purchase. Information Security Associates, LLC, under this warranty, is limited to correcting or replacing without charge, at its factory, any part or parts thereof which shall be returned to its factory, transportation prepaid, and upon examination by Information Security Associates, LLC, shall be found to have been originally defective.

INFORMATION SECURITY ASSOCIATES, LLC, SHALL NOT BE LIABLE FOR LOSS OR DAMAGE CAUSED EITHER DIRECTLY OR IN-DIRECTLY BY USE OF ITS PRODUCTS. THIS WARRANTY SUPERSEDES AND IS IN LIEU OF ALL OTHERS EXPRESSED OR IMPLIED. NO OTHER LIABILITIES MAY BE ASSUMED UNLESS AUTHORIZED IN WRITING BY INFORMATION SECURITY ASSOCIATES, LLC.

For service technical questions and problems contact:

Information Security Associates, LLC.
6 Spruce Brook Road
Seymour, CT 06483
USA
Tel: 203 736-9587
Fax: 203 736 9639
www.isa-technology.com
isa-hre@comcast.net