

REI's Technical Corner

By Tom Jones, REI General Manager

OSCOR and Detecting Sophisticated Transmitters

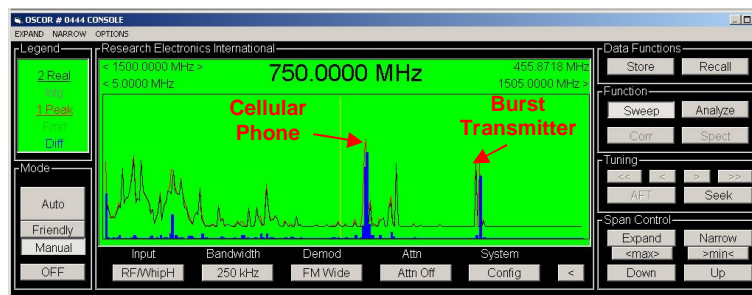
The OSCOR is extremely reliable at automatically detecting and logging signals that have a constant carrier frequency in the automatic mode; this function is one of the prime goals of the OSCOR system. However, there is an increasing number of sophisticated transmitters that the OSCOR will not automatically log in memory. To be more specific, AM, FM, and Sub-carrier modulated signals are easily logged automatically, but a Burst Transmitter, a Frequency Hopper, and many Spread Spectrum signals will not be logged in the OSCOR automatic mode because there is no stable carrier frequency for the OSCOR firmware to lock onto. Therefore, an additional procedure is necessary for increasing the probability of detection for these types of threats. This procedure does not require any new OSCOR hardware, firmware, or OPC software upgrades; it only requires understanding of the current OSCOR functionality and the procedure for reliably detecting these types of threats. This procedure relies heavily on the OSCOR display modes.

OSCOR Peak Display Memory

Many spectrum analyzers have a peak trace mode or a memory function to store a frequency spectrum trace. The OSCOR Peak Display Mode goes beyond this normal Spectrum Display Function to provide increased functionality. The OSCOR Peak Display Mode is, in reality, a memory buffer that is continuously updated in memory. In other words, no matter what the user is doing with the OSCOR or whether or not the OSCOR is in manual or automatic mode, the OSCOR Peak Display memory buffer is constantly being updated. Therefore, if any energy is captured from a short transmission such as a Burst or Frequency Hopper, the evidence of this event is stored in memory in the Peak Display Memory buffer even if the Peak Display is not turned on. Furthermore, the OSCOR can display the difference between the Peak display and the Real-time display. By displaying the Peak minus Real-time display, all of the continuous wave signals will be subtracted from the display, and the remaining graph will simply display all the evidence from intermittent transmitters that have radiated but have ceased to transmit. Here is the basic procedure to put the OSCOR into the Peak-Real-time Display mode.

1. Put the OSCOR in the SWEEP mode. (This is the normal default mode with the OSCOR is first turned on.)
2. Press the MENU button just below the display. (It should be labeled CONFIG on the OSCOR display.)
3. Continuously Press the F1 button until it is labeled "PRIMARY/PEAK"
4. Continuously Press the F2 button until it is labeled "DOT IMAG/REALTIME".
5. Continuously Press the F3 button until it is labeled "DIFFERENCE/ONLY"

This operation can also be performed using the OPC software, and in fact the OPC software provides a better graphic for this type of analysis. Below is an example of the Peak and Real-time sweep display using the OPC software



In this figure, the Red graphic shows the Peak Display, the Black color shows the Real-time display, and the Blue image shows the difference between the Peak and Real-time display. In this particular, image there is a Cellular phone transmission at around 840MHz and a Burst transmitter at around 1.2 GHz. The small Blue sections at the lower edge of the display represent variations in the modulation of signals. Furthermore, this particular display is showing the frequency band from 5MHz to 1505MHz, and the frequency spectrum may become much busier in a larger city, in this case, you can simply zoom into each

portion of the spectrum and analyze the areas as needed. It should also be noted that the OSCOR Peak Display mode stores frequency information at 50kHz resolution throughout the frequency band. Therefore, when the display is zoomed in to view a signal, the Peak display graph will appear to have coarse steps, but the main evidence of transmission will certainly be maintained.

Method of Detection

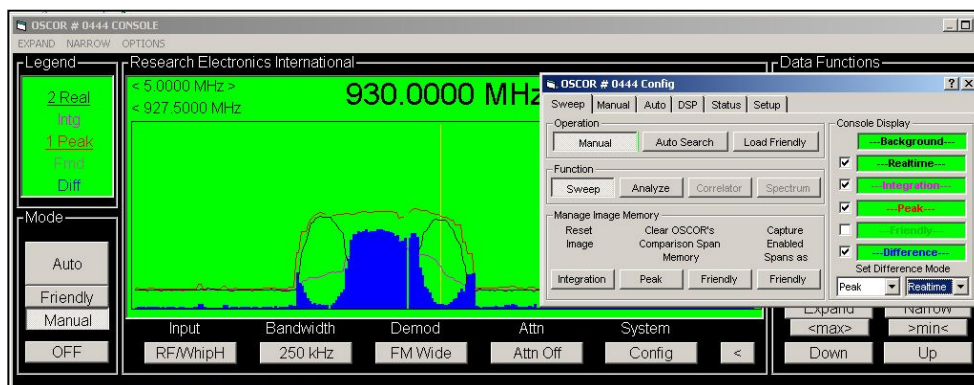
The basic new method of detection is the following.

1. Load Friendly signals at some distance away from the target environment (at least ½ mile).
2. When you enter the target room, first Clear the Peak Display Memory using the following procedure:
 - a. Place the OSCOR in the Sweep mode.
 - b. Press the MENU button.
 - c. Press the F4 button labeled “Manage Images”
 - d. Press the F2 button to clear the Peak Display Memory.
3. Perform the normal Automatic analysis using the Automatic mode and then evaluating all of the newly detected signals manually. (Note: During this time, the peak memory display buffer is continuously being updated both during the normal automatic and manual functions. If you have additional time, the OSCOR should be placed in the Sweep mode with the Whip Hi Antenna selected. Simply letting the unit sit in this mode for several minutes (up to 1 hour) will further improve the probability of detection for any potential sophisticated transmitter.
4. Place the OSCOR (or OPC software) in the Peak minus Real-time display mode so that any evidence of sporadic transmissions will be displayed. Note: you will see evidence of cell phones, pagers, two-way radios, or any other signal that is not currently transmitting.

To better understand this method of detection, several graphics are provided using the OPC software detecting some different types of threats.

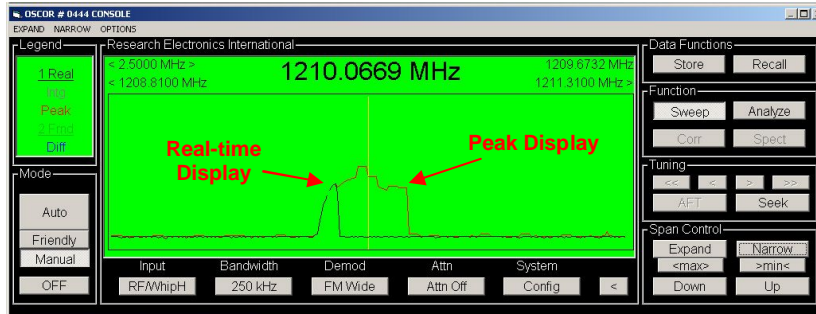
Pager Example

This Pager example is provided mainly to explain the concept of the Peak Display mode. In the graphic, the Red line indicates the Peak Display data, while the Black line indicates the real-time receiver data. The Blue area indicates the difference between the two. This is a simple paging transmission band with 3 primary channels. The channel in the middle is not currently transmitting while the two outside channels were transmitting at the time the OPC screen shot was taken.



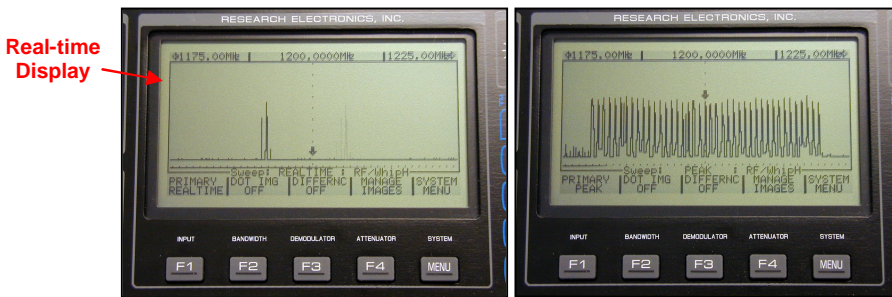
Burst Transmitter Example

In the example below, again the Red indicates the Peak Display and the Black indicates the Real-time display while the difference display (previously shown in blue) is turned off. This graphic is provided simply to indicate that at any given sweep (meaning the receiver sweep across the frequency spectrum), the OSCOR may only capture a portion of the transmission as indicated below. However, on multiple sweeps (passes through the spectrum) the entire envelope of the transmission may be filled in as indicated by the Peak Display.

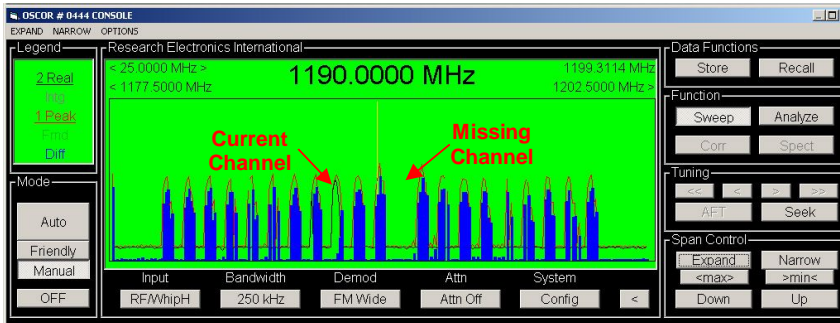


Frequency Hopper Example

This example provides an interesting view of the capture of a frequency-hopping signal. Examples of both the OSCOR display and the OPC display are provided. Note: for the OSCOR display, the graphic on the left shows the Frequency hopper in the normal Real-time display, but the figure on the right shows the Peak Display mode in which all channels of the hopper are visible. The important thing to understand is that to have a good probability of detection, using the previously described method, the OSCOR only needs to intercept some energy from any one of the channels to indicate a potential threat.



This is another view of a hopper using the OPC software. In this view, one channel has yet to be detected by the OSCOR, and one channel is currently being intercepted by the OSCOR.



Using these detection methods, the probability of reliably detecting some very sophisticated threats is greatly enhanced. For more detailed explanations about using the OSCOR to detect these and other sophisticated threats, contact REI at sales@reiusa.net to inquire about additional OSCOR training.