RESEARCH ELECTRONICS INTERNATIONAL

NEWSLETTER
Q1 2005

INSIDE THIS ISSUE:

UPCOMING TRAINING

February 28 - March 4
Technical Surveillance Countermeasures (TSCM 201)

March 15 - 17
Technical Security Equipment (TSE 101)

April 4 - April 8
Equipment Certification Course (ECC 240)

April 12 - 14
OSCOR 5.0 User's Conference

May 17- 19
Technical Security Equipment (TSE 101)

May 23 - 27
Technical Surveillance Countermeasures (TSCM 201)

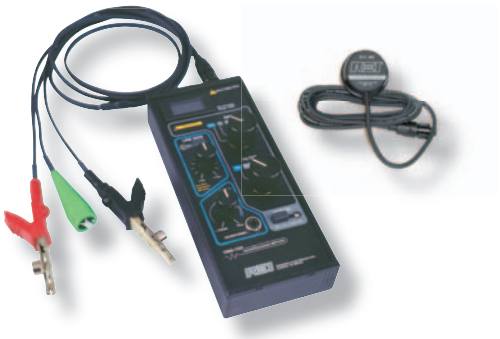
June 7 - 9
Technical Security Equipment (TSE 101)

June 13 - 17
Technical Surveillance Countermeasures (TSCM 201)

Questions, comments, suggestions, or to add someone to the REI Quarterly Newsletter mailing list, please e-mail: newsletter@reiusa.net

The Role of an Audio Amplifier In a TSCM Investigation

During the course of a normal sweep, it is important to be able to identify if miscellaneous cables could be a potential surveillance threat. A good quality Audio Amplifier is a useful tool that can help make this determination.



However, it is important to realize that an inexpensive Radio Shack style audio amplifier may not serve this purpose well. There are some important features that should be considered for a good TSCM amplifier:

1. **Very High Dynamic Range** – A good amplifier should be capable of re-producing audio sound from signals that range from extremely low levels (like a few micro-volts peak to peak) to a few volts. One example of this need is the ability to detect potential audio vulnerabilities of analog audio leakage in some digital phone systems.

2. **AC Power Voltage Protection** – A good amplifier must be protected against accidental voltage overload to protect both the equipment and the user.

3. **Voltage Measurement** – It is important to quickly test the suspect wiring for voltage levels that may indicate DC powered electronics or AC power.

4. **Line Bias –** An electret microphone may be connected to miscellaneous wiring, but only be power (biased) when the eavesdropping occurs. Therefore, it is important to be able to power a line and listen for activated microphones.

5. **Voice Band Filtering** – A good audio amp should have voice band filtering to remove high frequency noise and power line (60 Hz or 50 Hz) noise.

6. **Audio Leakage Probe** – Using a good contact microphone with a quality audio amplifier provides the ability to analyze an environment for structure born audio. You should be able to answer the question: is audio traveling through the duct work, walls, doors, windows, plumbing, etc…

7. **Simple and easy to use** – An amplifier is only as good as the user at the controls; if the amplifier is complicated or requires the user to adjust several settings and/or inputs, effectiveness and usefulness is compromised. Good automatic gain control can make the amplifier easy to use, however you will also want to be able to manually adjust the gain throughout the amplifier's complete range.

In summary, an audio amplifier provides an important comprehensive tool to evaluate the potential sources for audio leakage in an environment. For this reason, REI developed the CMA-100 (CounterMeasures Amplifier) which contains all of the above features. For more information visit our website or e-mail sales at sales@reiusa.net.

455 SECURITY PLACE • ALGOOD TN 38506 USA • TEL +1 931.537.6032 • 800.824.3190 (US ONLY) • FAX +1 931.537.6089 • WWW.REIUSA.NET

RESEARCH ELECTRONICS INTERNATIONAL

NEWSLETTER
Q1 2005

NLJD Detection Through Different Materials

When using the ORION, or any other Non-Linear Junction Detector (NLJD), it is important for the user to understand detection range capabilities and limitations associated with searching in a specific environment. REI has developed our own proprietary mathematical models as well as performed real-world testing to analyze NLJD detection through various materials such as Gypsum board (sheet rock), wood panel, brick, concrete blocks, solid concrete wall, plaster wall, etc.... While we are satisfied with our testing and analysis, the main realization is that it is very difficult to predict what the specific detection range will be, more importantly the user needs to understand how different materials can affect the detection range.

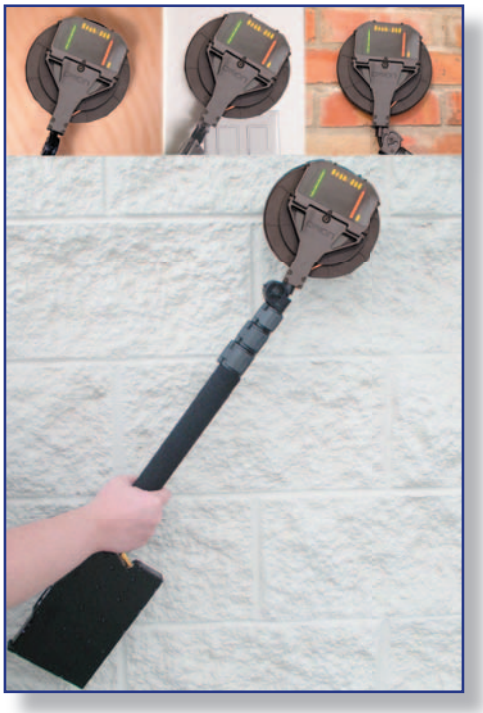
The are three basic issues associated with detection through materials: (1) How well does the threat respond to an NLJD? (This cannot be predicted for an unknown bugging device, and is independent of the material). (2) What is the thickness of the material being scanned? (3) What is the RF loss associated with the type of material?

It is also important to consider that walls may have combinations of materials that affect performance. Sheet rock walls may have metal or wood studs and may contain insulation; furthermore the insulation may contain a foil backing which also affects NLJD response.

In addition to combinations of materials, the materials themselves can vary greatly; for example, all concrete walls are not the same to an NLJD. A concrete wall will have different RF loss depending on how long has the concrete been curing, how much salt is in the concrete mixture, and the amount of steel re-enforcements (re-bar) in the concrete. An exterior brick wall will change depending on how wet the brick is (when did it last rain and what is the humidity level?).

A good rule of thumb is: the greater the thickness, the greater the density, and the presence of RF inhibiting materials will negatively impact the detection range of a NLJD. The user should adjust equipment settings, speed, and thoroughness of the sweep. However, all of these factors can also negatively impact the effectiveness of an eavesdropping device.

Nonetheless, the best method of predicting NLJD detection range for a specific material is not a scientific one. This method simply requires the sweeper to take a test target and place it on the opposite side of a wall or material of interest and test the detection range through the material. The test tag that is supplied with the ORION provides a very strong response, and should easily be seen through common USA 4 or 6 inch sheet rock walls. Further, it is recommended that because the supplied test tag provides a strong response and is easily detected, you should also use another test device such as a clock radio, tape recorder, or telephone etc... The detection range of different electronic devices will vary greatly.



Taking these issues into consideration and experimenting with your ORION, you will gain a much better understanding of affects due to different materials, and equipment limitations. You will also gain a much better "feel" for setting the power level or the DSP gain for searching through various materials while maintaining adequate detection reliability. For more information regarding the ORION power levels and DSP processing gain, please consult the ORION manual or the REI web site.

455 SECURITY PLACE • ALGOOD TN 38506 USA • TEL +1 931.537.6032 • 800.824.3190 (US ONLY) • FAX +1 931.537.6089 • WWW.REIUSA.NET

RESEARCH ELECTRONICS INTERNATIONAL

NEWSLETTER
Q1 2005

OSCOR 5.0 and OPC User's Conference

REI is pleased to announce an OSCOR Version 5.0 User's Conference April 12-14 in Plano Texas, hosted by Perot Services.

The conference will cover new methodology and procedures associated with using the 5.0 OSCOR and OPC Software, including trace analysis and RF mapping for quick detection of threats (specifically sophisticated devices such as burst/packet transmitters, frequency hopping, and spread spectrum devices). There will also be hands-on exercises to give attendees the opportunity to practice the new 5.0 procedures to detect sophisticated transmitters.

REI requests that attendees bring their 5.0 OSCOR with them to use during the conference. If you need to get your equipment upgraded, please contact REI to make arrangements to get this done before the conference. This conference will cost US$495 per attendee and will include lunches each day. REI can provide you with a recommended hotel where conference attendees will receive a discounted rate.

If you are interested in attending this Conference, please contact Nicole Rodgers at +1 931-537-6032 or nicole@reiusa.net to reserve your seat.

TSCM Tips

Locating a Threatening Transmitter using the OSCOR...

Once you have determined that there is a threatening transmitter in the sweep environment, the next step is to locate the origin of the transmitter. If the signal is analog, you can use the OSCOR's patented Threat Locating System to triangulate and locate the transmitter. However, if the signal is digital, you will need to use the OSCOR Locator Probe tuned to the frequency band of the threatening signal; optionally you could use the CPM-700, which is a broadband receiver and responds to total energy regardless of frequency (within the frequency range of the probe). To locate the RF signal, divide the sweep area into four quadrants, and check the RF signal noise floor (signal strength) in each quadrant. The quadrant that contains the transmitter should give you a stronger response, and you can narrow your search to that quadrant, thoroughly "painting" all surfaces with the probe to identify the strongest signal (also consider using the CPM-700 which is especially good for frequency-hopping transmitters because it detects all hops within its frequency range). Make sure that you don't overlook the other quadrants just because one quadrant indicated a stronger response. And, as always, make sure you perform a complete TSCM sweep including NLJD tests and a thorough physical search to locate any non-transmitting or passive threats.

Equipment Tip:

The OSCOR battery needs to be charged on a regular basis to maintain battery life. To ensure battery life is maximized, at least once a month you should plug your OSCOR in to an AC power source and the turn the unit on to sense the battery voltage level and initiate the charge mode.

For more information on performing TSCM sweeps, consider REI's Center for Technical Security training courses. Course descriptions and training dates can be found on REI's website (www.reiusa.net/training) or e-mail sales@reiusa.net.

If you have TSCM sweep tips that you would like to share, please send them to support@reiusa.net

455 SECURITY PLACE • ALGOOD TN 38506 USA • TEL +1 931.537.6032 • 800.824.3190 (US ONLY) • FAX +1 931.537.6089 • WWW.REIUSA.NET