

**U.S. ARMY OPERATIONAL TEST COMMAND  
INTELLIGENCE ELECTRONIC WARFARE  
TEST DIRECTORATE**

**INSTRUMENTATION CATALOG**

**FORT HUACHUCA, AZ 85613-7000  
Updated October 2, 2003**

(This page intentionally left blank.)

# Contents

<b>1</b>	<b>Introduction</b>	<b>1</b>
<b>2</b>	<b>Electromagnetic Vulnerability Test Systems</b>	<b>3</b>
<b>2.1</b>	<b>Electronic Warfare Monitoring Facility (EWMF)</b>	<b>5</b>
<b>2.2</b>	<b>Vulnerability Mobile Transmitter A (VMT-A)</b>	<b>15</b>
<b>2.3</b>	<b>Vulnerability Mobile Transmitter B (VMT-B)</b>	<b>25</b>
<b>2.4</b>	<b>Vulnerability Mobile Transmitter C (VMT-C)</b>	<b>37</b>
<b>2.5</b>	<b>Signal Monitoring, Verification, and Field Intensity Measurement (FIM) Equipment</b>	
<b>3</b>	<b>Automated Intelligence/Electronic Warfare Test System (AI/EWTS)</b>	<b>53</b>
<b>3.1</b>	<b>Operational Test Control Center (OTCC) and Communication Network</b>	<b>55</b>
<b>3.2</b>	<b>Mobile Communications Simulator Threat Facility (MCSTF)</b>	<b>59</b>
<b>4</b>	<b>Mobile Threat Emitter</b>	<b>67</b>
<b>5</b>	<b>Communications-Electronics (CE) Shop</b>	<b>71</b>
<b>6</b>	<b>GPS and Video Instrumentation</b>	<b>73</b>
<b>7</b>	<b>Information Assurance Test Tool (IATT)</b>	<b>81</b>



(This page intentionally left blank.)



## **CHAPTER 1 INTRODUCTION**

---

### **1. MISSION**

The mission of the United States Army Operational Test Command (USAOTC) Intelligence Electronic Warfare Test Directorate (IEWTD) is to conduct operational testing of new materiel, doctrine, organization, and training systems. The mission includes the following:

Planning, conducting, and reporting on operational tests and other user tests of intelligence, surveillance, reconnaissance, and electronic warfare systems.

Conducting electronic support measures/electronic countermeasures (ESM/ECM) operational vulnerability assessment tests.

### **2. PURPOSE**

This catalog is intended to provide the test planner an overview of the capabilities and limitations of the IEWTD test support instrumentation systems. These systems are extremely versatile and highly mobile. They provide a variety of mechanisms to measure, analyze, document, invoke, or stress a system under test (SUT).

### **3. SCOPE**

This instrumentation catalog covers the major IEWTD threat and vulnerability assessment systems and devices. It also addresses the development concept for future instrumentation systems.

### **4. APPLICATION**

The primary use of the IEWTD threat and vulnerability assessment instrumentation is to support operational, concept evaluation, and customer tests.

(This page intentionally left blank.)

## CHAPTER 2 ELECTROMAGNETIC VULNERABILITY TEST SYSTEMS

---

### 1. INTRODUCTION

- 1.1 IEWTD's electromagnetic vulnerability (EMV) test systems include ESM/ECM test facilities, Signal Monitoring, Verification, and Field Intensity Measurement (FIM) equipment (hereafter referred to as Signal Monitoring equipment). These facilities primarily perform vulnerability assessments of tactical intelligence electronic warfare (IEW) systems against current and projected threats in support of operational tests and concept evaluations. Secondary functions include, but are not limited to, maintaining ground truth and replicating threat signals in support of testing. To minimize cost and to maximize flexibility, these facilities have been assembled using commercial off-the-shelf (COTS) equipment. In special cases (for example, intercept, direction find (DF), and jam frequency-hoppers), unique systems have been developed, to IEWTD specifications, to meet projected threats. In each of these unique systems, the equipment is rack-mounted and hard-wired to achieve electrical and testing requirements. All assets may be employed separately or in combination to provide additional capabilities and are normally configured in semi-trailer vans. The Signal Monitoring equipment is usually installed in 4x4 vans.
- 1.2 The ESM van is called the Electronic Warfare Monitoring Facility (EWMF). It is configured in a 40-foot expandable semi-trailer with full climate control and an on-board generator. It operates over the frequency range of 100 kHz to 40 GHz, with collection, LOB, recording, and analysis equipment and subsystems.
- 1.3 The ECM vans are all very similar in capability and operation and are contained within 40-foot semi-trailer vans. Their major differences are in frequency range. The Vulnerability Mobile Transmitter A (VMT-A) covers the VHF/UHF frequency band (20 to 1,000 MHz). The VMT-B covers the microwave frequency range from 1 to 40 GHz. The VMT-C covers the HF frequency band (2 to 30 MHz). Each of these facilities also has a near-real-time integrated ESM capability with display, analysis, and recording systems to verify and document operational parameters as they occur.
- 1.4 The Signal Monitoring equipment is primarily used for signal-strength measurements. The systems consist of measurement, and analysis instruments. Two 4x4 vans with on-board generators and antenna masts are available to support this equipment. Most of the equipment may be automated via IEEE-488 interfaces. Measurements may be recorded on disk or downloaded to a printer/plotter. The nominal measurement frequency range is 10 kHz to 40 GHz.

(This page intentionally left blank.)

## SECTION 2.1 ELECTRONIC WARFARE MONITORING FACILITY (EWMF)

---

### 1. SYSTEM DESCRIPTION

- 1.1 The EWMF represents IEWTD's ESM capability (ESM includes signal intercept, signal identification, and location of signal sources by electronic means). The primary mission of the EWMF is the collection of ESM data during vulnerability testing of IEW systems. The EWMF provides signals intelligence (SIGINT) against communications and non-communications signals. A secondary mission of the EWMF is to act as part of an ECM system, providing *look through while jam* data as well as a source of electronic deception data. An additional secondary mission includes monitoring signal environments; controlling emitter arrays; and verifying emitters, system signatures, or signal characterization.
- 1.2 The EWMF consists of surveillance receivers, spectrum analyzers, recorders, antenna systems, instrumentation control computers, signal analysis equipment, LOB equipment, and printers or plotters. This equipment is installed in a 40-foot, air-ride suspension, expandable semi-trailer with HF, VHF, UHF, and SHF antenna systems. The EWMF also contains a small maintenance area, a data reduction and analysis area, and a diesel generator to accommodate remote and extended missions.



**Figure 2.1-1. EWMF.**



**Figure 2.1-2. EWMF Front Maintenance and Storage Area.**



**Figure 2.1-3. EWMF WJ LOB System and Instrumentation Control.**



**Figure 2.1-4. EWMF Andrew LOB System, Intercept and Analysis Equipment.**



**Figure 2.1-5. EWMF Rear Storage and Office Area.**

## 2. SYSTEM OPERATIONAL CAPABILITIES

- 2.1 The EWMF has an intercept range of 100 kHz to 40 GHz and can demodulate AM, FM, upper sideband, lower sideband, pulse, and phase modulated signals. One specialized item is the high-speed line of bearing (LOB) system, which can provide LOB on signals with a dwell time as short as 10 microseconds ( $\mu$ s) over a range of 2 to 1,200 MHz. This is a time-difference-of-arrival system with  $2^\circ$  root mean square (rms) accuracy. A second LOB system, consisting of omni-directional and rotating LOB antennas, covers the 0.5 to 40 GHz range with up to a  $2^\circ$  rms accuracy (typical  $2^\circ$  to  $6^\circ$  rms) (see figures 3.1-2 and 3.1-3).
- 2.2 The EWMF also contains a full array of support equipment. All instrumentation (excluding the LOB systems) can be controlled with a Pentium computer through either RS-232C or IEEE-488 buses. Signals and data can be recorded on floppy disk, CDROM, or removable hard drive, or can be transferred to hard copy with a printer or plotter. A GPS receiver supplies the EWMF location and accurate timing for test event scheduling and marking. Antennas from HF long wires to 40-GHz dishes are available.

## 3. TECHNICAL SPECIFICATIONS

### 3.1 Monitoring Equipment

#### 3.1.1 Antenna Systems.

##### Barker & Williamson AC-1.8-30

This is a broadband, long-wire, end-fed (via a 50 ohm matching balun), sloping "V" antenna covering the frequency range from 1.8 to 30 MHz. Maximum SWR is 2.0:1. Center support is via a ground mounted, lightweight, sectional mast.

##### SB-V35B

This is a 32-foot, vertical-whip antenna with a frequency range of 2 to 30 MHz. It may be mounted at one of four locations on the perimeter of the van roof.

##### American Electronic Laboratories APN-1509

A 20 to 1,000 MHz log periodic antenna. Gain ranges from 2.4 dBLi at the lower frequencies to 6.0 dBLi at the high end. Nominal beamwidth is  $60^\circ$  in the E plane and  $110^\circ$  degrees in the H plane. Impedance is 50 ohm and SWR is a nominal 2.0:1. It mounts on a rotatable ( $360^\circ$ ), 40-foot pneumatic mast with a mechanical polarization rotator. Polarizations are vertical, horizontal, and  $45^\circ$ .

WJ-8976-4A LOB System Antennas:

AU-3: HF subsystem: 2-30 MHz, vertical polarization, 360° coverage, triple-baseline interferometer, 15-foot monopoles, 14-foot baseline. It must be ground mounted in a clear area within 100 feet of the EWMF.

AU-4: VHF/UHF subsystem: 20-1,200 MHz, three stacked sets of three vertical dipoles, 360° coverage. It mounts to the 40-foot mast. This antenna and the APN-1509 LPA cannot be used at the same time.

Andrew SciComm SCR-2940DF Integrated Radar Monitoring System Antenna Subsystems:

AOA-2640: Omnidirectional, 0.5-40 GHz, slant-polarized, 360° in azimuth, 12°-25° beamwidth in elevation, typical gain -7 to +4 dBi.

ADF-2640: Spinning LOB: 0.5-40 GHz, slant-polarized, 360° in azimuth, 15° beamwidth in elevation, bearing accuracy 6°-2° rms, pointing accuracy ±0.2°, resolution 0.1°, min gain 4-21 dBi, spin rate 0-200 rpm, sector 1°-60°/sec.

### 3.1.2 Receiver Systems.

M/A COM Microwave Wide Bandwidth Receiver System: .5-40 GHz; 100-Hz tuning resolution; 250 kHz to 1 GHz bandwidths(10); AM and FM demodulation modes, 17 dB maximum noise figure.

WJ-8611 Intercept Receiver (2): 2-1,000 MHz; 10 Hz tuning resolution; 200 Hz to 200 kHz bandwidths(17); CW, AM, FM, USB, LSB, and ISB demodulation modes; 12 dB maximum noise figure; -114 dBm CW sensitivity for 16 dB S+N/N; RS-232 and IEEE-488 interfaces.

AOR AR8600 Communications Receivers(8): 530 kHz to 2,040 MHz, 50-Hz tuning resolution; 3, 9, 12, and 150 kHz; CW, AM, FM, USB, and LSB demodulation modes, AM sensitivity for 10 dB S+N/N; RD-232 interface.

### 3.1.3 LOB Systems.

Watkins-Johnson 8976-4 DF System: 20-1,200 MHz; resolution 1 kHz; IF bw 10, 50, 100 kHz, 1-4 MHz; detection modes: AM, FM, CW, SSB, PM; dynamic range 66 dB; response time LOB in 65 milliseconds (ms); minimum signal duration 10 μs with 10 dB signal-to-noise (S/N); LOB resolution 0.01° Az; LOB accuracy 2° rms; IEEE-488.

Andrew SciComm SCR-2940DF Integrated Radar Monitoring System: 0.5-40 GHz, 160 MHz IF with 50 MHz bw, 1 GHz IF with 500 MHz bw, resolution 100 Hz, sensitivity -77 to -86 dBm, RMS monopulse frequency accuracy  $\pm 1.8$  MHz, RMS monopulse amplitude accuracy  $\pm 3.6$  dB, displays--frequency analysis, PRI, pulse width, DF, emitter report, situation map, frequency activity.

### 3.2 Analysis Equipment

HP 89440 Vector Signal Analyzer: DC-1,800 MHz; frequency resolution .001 Hz; advanced time-selective spectrum analysis, digital-modulation analysis, precision AM, FM, and phase demodulation; -30-+25 dBm input range; 50 ohm input impedance.

HP 71910A Surveillance Receiver (Spectrum Analyzer): 100 Hz to 40 GHz, frequency resolution 1 Hz, IF bw 10 Hz to 100 MHz in 10% increments, IF step gain 70 dB, resolution bw 10 Hz to 3 MHz, noise figure @ 12 GHz 32 dB, LO phase noise @ 6 GHz-108 dBc/Hz.

HP 5371A Frequency and Time Interval Analyzer: DC-500 MHz, 10 MHz rate, time-interval range -4.0 to +4.0 seconds, 150 ps rms time-interval resolution, logical triggering, 2 millivolt (mV) trigger level resolution, 2-channel (ch), IEEE-488.

Tektronix 784D Digitizing Oscilloscope: 1 GHz analog bw, 4-channel, 50 kilobyte (kb) memory/ch, max digitizing rate 4 GS/s, color display, input impedance 50 or 1 Meg ohm, fully programmable via RS-232 or IEEE-488 buses.

Tektronix RTD 710 Programmable Waveform Digitizer: Resolution 10 bit,  $\pm 0.4\%$  gain accuracy, 200 MS/s, 100 MHz bw, 8 megaword memory, 1-64 records, adjustable pre- and post-triggering, IEEE-488.

### 3.3 Support Equipment

Instrumentation Controller: Rack-mounted PC, 933 MHz Pentium 3®, 256 MB RAM, 15 GB hard drive, 4x2x24 CD-RW, 32x CDRom, 3½" floppy drive, AGP 32 MB video (1600x1200), 1 AGP, 2 ISA, and 4 PCI slots, 8-port serial extender, 56K modem, GPIB interface (2), onboard sound. With rack mount 17" .25 dot pitch-color monitor and HP 890C color printer.

Trimble AccutimeII 6-Channel GPS Receiver: Trimble Standard Interface Protocol (TSIP) RS-422 data output, 8-32 vdc operating voltage. A software interface application running on the Instrumentation Controller insures that the controller's real-time clock is set to within 20 ms of UTC; displays current latitude, longitude, altitude (LLA), local, and UTC date/time; and provides LLA, UTM, and MGRS coordinates via an internal DDE server to any DDE-capable client application.

Systems Research Labs 1400 Series Lab Modules: Audio amplifier, video gate, sample and hold, pulse stretcher, noise ridding trigger, comparator/trigger, signal slicer.

Test Signal Generator: Gigatronics Model 7100 RF Synthesizer: .01 - 26.5 GHz. 1 Hz resolution, AM (0 - > 90%), FM (< 3 kHz > 20 MHz peak deviation), and pulse (DC - 10 MHz PRF, >50 ns PW) modulation. Internal AM and FM modulation source: sine, square, or triangle, 1 Hz-100 kHz, 1-Hz resolution. Internal pulse modulation source: 5 Hz-1 MHz PRF, 50 ns-2s PW. RF output level: -130 - > +10 dBm. IEEE-488 interface. Provides test signals for EWMF intercept and analysis systems and equipment.

### 3.4 Communications

Motorola MCX1000 Mobile DVP Radio: Digital voice privacy nonlinear digital scrambling, VHF 146-162 MHz, channel spacing 30 kHz, output 30 W.

## 4. SYSTEM LIMITATIONS

The EWMF cannot provide an emitter location fix. It can, however, determine the LOB to the emitter. Therefore, if the EWMF can produce an accurate LOB on an emitter, it indicates emitter vulnerability to DF.

## 5. PLANNING CONSIDERATIONS

- 5.1 A 10- to 15-ton commercial or military tractor is required to pull the EWMF over improved roads only. It has a ground clearance of 14 inches, a 96-inch width, 40-foot length, and is 13 feet 6 inches high. A 14-foot minimum overpass clearance should be observed. Maximum weight is 84,000 pounds. It has tie-down rings and can be transported by aircraft. Approximately 4 hours are required for setup and checkout. Equipment with internal reference oscillators can require up to 24 hours warm-up to meet manufacturer's specifications. However, adequate accuracy levels are usually reached after approximately 1 hour of warm-up time. The internal heating and cooling system it to be operated comfortably in both cold and hot climates. Primary power is 120/208 VAC, 3-phase, 4-wire, 60-Hz at 100 amps per phase. It has an external power cable with *pig tails* to connect to fused power drops. The on-board 45-kW diesel generator requires approximately 25 gallons of fuel for 12 hours of operation and has a tank capacity of 100 U.S. gallons.
- 5.2 For vulnerability testing, operation of the EWMF requires at least two operators for every 8-hour shift. The number of operators is mission-dependent, but two, as a minimum, are required. Unless the EWMF is deployed in a secure area, guards must be employed on-site whenever operators are not present. When LOB data are to be collected, the site must be free of objects, such as trees, utility poles, phone and electrical lines, fences, cars, and buildings, for at least 50 feet (500 feet for low radio frequencies).
- 5.3 The Motorola communications equipment requires frequency authorization at locations other than Fort Huachuca.

## SECTION 2.2 VULNERABILITY MOBILE TRANSMITTER A (VMT-A)

---

### 1. SYSTEM DESCRIPTION

The VMT-A represents IEWTD's ECM capability in the 20 to 1,000 MHz frequency range. It is a highly versatile jammer van with a limited monitoring and analysis capacity. Its primary mission is to replicate current and projected threat ECM in support of vulnerability assessments of IEW systems. Secondary missions include threat and friendly signal simulation in support of operational tests. The high degree of flexibility in the VMT-A is a result of it having been assembled primarily from commercial off-the-shelf (COTS) equipment. It is transportable and is housed in a 40-foot semi-trailer with full-climatic control, on-board generator, and a 31-foot rotating pneumatic mast. The VMT-A also contains a maintenance area, documentation storage area, and a safe, allowing it to support 24-hour per day and classified missions.



**Figure 2.2-1. VMT-A.**



Figure 2.2-2. VMT-A High Power Linear Amplifiers.



**Figure 2.2-3. VMT-A RF Generation and Monitoring.**



**Figure 2.2-4. VMT-A LPI ECM Receiver and Modulation Sources.**



**Figure 2.2-5. VMT-A Maintenance and Storage.**

## 2. SYSTEM OPERATIONAL CAPABILITIES

- 2.1 As a threat jammer, the VMT-A has several possible ECM modes: continuous, swept, barrage, signal-initiated, repeat, phase-coherent repeat, playback, and combination. The target transmission may be degraded or overpowered by noise, tones, or complex modulations. A victim receiver may be captured or spoofed by amplifying and relaying its intended signal or recording and re-transmitting a previous one. The relayed and retransmitted signals may be altered to achieve a desired effect.
- 2.3 The VMT-A may also be used to replicate threat communication or non-communication emitters within its frequency range and power limitations. Three high-power amplifiers cover the frequency range from 20 to 1,000 MHz. RF output power ranges from 2 kilowatts for the 20 to 100 MHz amplifier to 1 kilowatt for the 100 to 500 MHz and 500 to 1,000 MHz amplifiers (see figure 3.2-3). The antenna is a log periodic with a frequency range of 20-1000 MHz, a nominal beamwidth of 60°, and from 3 to 7 dBi gain. The antenna is installed on a 28-foot pneumatic mast with an azimuth rotator and manual-polarization rotator. The combination of modulation and signal sources provides the capability to produce virtually any signal characteristic.
- 2.3 The monitoring and analysis capabilities are used primarily to document emitter parameters and to verify proper operations. The signal and data recording equipment may be used for signal documentation and analysis, for storage of the analysis or raw data, or for recording a target emission, then becoming a source for retransmission. Any data, analysis, or documentation may be stored on computer disk (hard disk, floppy disk, or CDROM) or converted to hard copy. Hard copy media include printer listings and chart recordings.
- 2.4 All instrumentation can be controlled with a Pentium PC through IEEE-488 or RS-232 interfaces (see figure 3.2-4). Instrumentation support equipment includes signal conditioning modules (amplifiers, video gate, comparator/trigger, pulse stretcher, signal clipper), attenuators, filters, and power meters. A GPS receiver provides location and accurate timing.
- 2.5 An item unique to the VMT-A is the Compressive Receiver System (see figure 3.2-5). With a sweep speed of 202.5 kHz per microsecond and a frequency range of 20 to 500 MHz, this receiver is designed to intercept and jam frequency agile signals.

### 3. TECHNICAL SPECIFICATIONS

#### 3.1 Transmit

<u>Frequency (MHz)</u>	<u>Amplifier</u>	<u>Rated Power</u>	<u>Antenna Gain</u>	<u>Effective Radiated Power (ERP)</u>
20 - 100	PST BHED2718	2000 W	3 dBi	1.8 kW
100 - 500	MPD EWAL 1050	1000 W	6 dBi	3.1 kW
500 - 1000	PST BHED5819	1000 W	6 dBi	1.7 kW

#### Antenna System:

AEL Model APN-1509 Log Periodic: 20-1,200 MHz, 60° beam width, 1,000 W CW power handling capability. The system mounts to a 36-foot pneumatic mast with its azimuth remotely controlled from within the facility. Antenna polarization is done manually. The extended height of the antenna is approximately 39 feet above ground level.

#### Transmit and Jamming Modes:

AM, FM, pulse, hop, phase, spot noise, barrage noise, and combinations.

#### Sources:

Rohde & Schwarz SMIQ06B Vector Signal Generator: 300kHz – 6.4GHz, 0.1 Hz resolution, <3.3 ms, digital sweep. Vector (I&Q), AM, Broadband AM, Pulse, FM, Phase, ASK, FSK, 2FSK, GMSK, QAM (16-256), BPSK, QPSK, QPSK (IS-95), OQPSK, pi/4DQPSK, 8PSK, and 8PSK EDGE modulations. Predefined modulations APCO, C4FM, APCO CQPSK, CDPD, CT2, DECT, GSM, IRIDIUM, NADC, ODC, PHS, TETRA, TFTS, PWT, ICO BPSK, ICO GMSK, ICO QPSK, GSM EDGE, CDMA IS-95, and W-CDMA. Digital Standards IS-95, W-CDMA (2GPP), and more. Internal data and arbitrary waveform generators.

HP 8780A Vector Signal Generator: 10 MHz - 3 GHz, 1-Hz resolution, switching speed <220 ms, vector (I&Q), scalar FM (150 Hz - 50 MHz peak deviation), binary phase shift keying (BPSK), quaternary phase shift keying (QPSK), 8 PSK, 16 and 64 QAM modulation modes, external analog and digital modulation sources required, IEEE-488 interface.

HP 8663A Synthesized Signal Generator (2): 0.1-2,560 MHz; resolution <0.5 Hz; AM, FM, BPSK, phase, and pulse modulations; internal and external modulation sources; IEEE-488 interface.

HP 8770A Arbitrary Waveform Synthesizer: DC - 50 MHz; 125-MHz internal or 10 to 130-MHz external sample clock, divisible by 1, 2, 4, 8, 16, 32, 64, 128, or 256; sample size = sample clock period; 131072 12-bit word memory, output -110 to +10 dBm in 10 dB steps, IEEE-488 interface.

HP 3325B Synthesizer/Function Generator: 1  $\mu$ Hz - 21 MHz front, 21 to 60 MHz rear output; sine, square, triangle, negative and positive ramps; 20 ns rise time on square waves; arbitrary function generator via HPIB providing user-defined wave-shapes; resolution  $\leq$  1 millihertz (mHz); IEEE-488 interface.

HP 8130A Pulse Generator: 300 MHz, 2-channel; period 3.33 ns to 99.9 ms, width 1.5 ns to 99.9 ms, delay 0 ns – 99.9 ms, transition time 100  $\mu$ s to 1 ns, output amplitude 100 mVp-p – 5 Vp-p into 50 ohm, IEEE-488 interface.

HP 8018A Serial Data Generator: 2048 programmable bits, > 1 Mbit pseudo random sequences, 2-channel, 6 ns pulses with repetition rates from 0 to 50 Mbits, output up to 15 V, IEEE-488 interface.

NOISE/COM NC 7110 Noise Generator: 100 Hz - 1,500 MHz white gaussian noise, output +10 dBm (max)  $\pm$  2.5 dB, attenuation 0 - 127 dB, resolution 1 dB, IEEE-488 interface.

Elgenco 610A Noise Generator: Symmetrical gaussian distribution, 5 Hz – 5 MHz, output uniform to  $\pm$  0.5 dB from 10 Hz - 500 kHz  $\pm$  2 dB to 5 MHz, output level 0-1 V rms.

### 3.2 Monitoring and Analysis

HP 8566B Spectrum Analyzer: 100 Hz - 22 GHz, resolution bw (-3 dB) 10 Hz - 3 MHz (1,3,10 sequence), video bw 1 Hz - 3 MHz (1,3,10 sequence), amplitude range -114 to +30 dBm. IEEE-488 interface.

Sanders Compressive Receiver System II: 20-500 MHz, sweep rate 202.5 kHz/us, resolution 25 kHz, accuracy 3.125 kHz, sensitivity -100 dBm, dynamic range 60 dB. In the ESM mode, the system intercepts frequency agile signals and sorts them by amplitude, dwell time, and hop rate. It can save all signal intercepts that meet the sorting parameters to a hard disk file for later analysis. In the ECM mode, the system's fast-switching frequency synthesizer follows the victim transmissions and provides the drive signal for the facility's high-power amplifiers. It can follow and jam these signals at up to 492 hops per second over a typical 60-MHz range. This system is controlled by a dedicated Pentium computer via a Hewlett Packard GPIO parallel interface.

ICOM IC-R8500 Receiver (unblocked): 0.1- 1999.99999 MHz. AM, FM, CW, and SSB(USB/LSB) demodulation modes. IF bandwidths 500 Hz, 2.2, 5.5, 12 and 150 kHz. 0.25-3.2 uv sensitivity. 50 dB image rejection. RS-232 interface.

Tektronix TDS 5104 Digital Phosphor Oscilloscope: 1 GHz bw, 5GS/s sample rate (1 ch), 4-ch, color, floppy and CDROM drives, Calculated Rise Time 5 mV/div (typical) 300 ps, input sensitivity 1 mv – 10 v/div, 8 bit resolution, timebase 200 ps – 40s/div, LAN, serial, parallel, USB, PS2, and IEEE-488 interfaces.

### 3.3 Support Equipment

Instrumentation Controller: Rack-mounted PC, 933 MHz Pentium 3®, 256 MB RAM, 15 GB hard drive, 4x2x24 CD-RW, 24x CDROM, 3½” floppy drive, AGP 32 MB video (1600x1200), 1 AGP, 2 ISA, and 4 PCI slots, 56K modem, IEEE-488.2 interface, National Instruments PCI-67114 channel analog output device, onboard sound, rack mount 17”.25 dot pitch color monitor, and HP 870Cxi color printer

ASTRO-MED MT9500 Chart Recorder: Direct-writing thermal array 200 dots/inch, 8 channels, frequency response DC - 3 kHz ≤ 1 dB, resolution 12 bits, 16 kb/ch memory, chart speeds 1-100 mm/sec, /min, or /hr, IEEE-488 interface.

Trimble AccutimeII 6 channel GPS Receiver: TSIP RS-422 data output, 8-32 vdc operating voltage. A software interface application running on the Instrumentation Controller insures that the controller’s real-time clock is set to within 20 ms of UTC; displays current latitude, longitude, altitude (LLA), local, and UTC date/time; and provides LLA, UTM, and MGRS coordinates via an internal DDE server to any DDE-capable client application.

Bird 4387-832 Wattmeter: Power range 100 mW - 10 kW; .45-2,300 MHz; IEEE-488 interface.

Systems Research Labs 1400 Series Lab Modules: Summing amplifier, programmable operational amplifier, video amplifier, video gate, comparator/trigger, signal clipper.

### 3.4 Communications

Motorola MCX1000 Mobile DVP Radio: Digital Voice Privacy nonlinear digital scrambling, VHF 146-162 MHz, channel spacing 30 kHz, output 30 watts.

#### **4. SYSTEM LIMITATIONS**

At present, due to antenna power handling capability, the system is limited to 1,000 Watts.

The upper end of the Compressive Receiver System II is 500 MHz, which provides a maximum bandwidth of 480 MHz.

#### **5. PLANNING CONSIDERATIONS**

- 5.1 A 10- to 15-ton commercial or military tractor is required to pull the VMT-A over improved roads only. It has a ground clearance of 13 inches, is 96 inches wide, 40 feet long, and 12 feet 10 inches high. A minimum overpass clearance of 13.5 feet should be observed. It has tie-down rings and can be transported by aircraft. Approximately 2 hours are required for setup and checkout. Equipment with internal reference oscillators can require up to 24 hours warm-up to meet manufacturer's specifications. However, adequate accuracy levels are usually reached after approximately 1 hour of warm-up time. The internal heating and cooling system can be operated comfortably in both cold and hot climates. The primary power requirement is for 120/208 VAC, 3-phase, 4-wire, 60 Hz at 100 amps per phase. It has an external power cable for connection to commercial service. The on-board 60-kW diesel generator requires approximately 25 gallons of fuel for 8 hours of operation and has a tank capacity of 100 U.S. gallons.
- 5.2 For vulnerability testing, operation of the VMT-A requires at least two operators per 8 hour shift. Unless the VMT-A is deployed in a secure area, guards should be employed on-site whenever operators are not present. Due to the high levels of RF energy emitted by the system, visiting the VMT-A during its operation is discouraged.
- 5.3 A complete list of signal frequencies, modulation types, and power levels will be required for frequency authorization well in advance of the test start date. The Motorola communications equipment will require frequency authorization at locations other than Fort Huachuca.

**SECTION 2.3**  
**VULNERABILITY MOBILE TRANSMITTER B (VMT-B)**

---

**1. SYSTEM DESCRIPTION**

The VMT-B represents the IEWTD's ECM capability for the 1 to 40 GHz frequency range. It also possesses a limited monitoring and analysis capacity. Its primary mission is to replicate current and projected threat ECM in support of vulnerability assessments of IEW systems. Secondary missions include threat and friendly signal simulation in support of operational tests. The facility is transportable and is housed in a 40-foot semi-trailer with full-climatic control and a programmable antenna pedestal. The facility contains maintenance and documentation areas and a diesel generator to support remote and around-the-clock missions.



**Figure 2.3-1. VMT-B.**



**Figure 2.3-2. VMT-B: 1 to 8 GHz Power Amplifiers and Generator Control Panel.**



**Figure 2.3-3. VMT-B Rear Racks.**  
(8–40 GHz Amplifiers, RF and Pulse Signal Generation, and Analysis Equipment)



**Figure 2.3-4. VMT-B Front Racks.**  
(Video Tracking, Analysis, Control, and Recording Equipment)



**Figure 2.3-5. VMT-B Front Area.**  
(Maintenance, Storage, and Documentation Area)

## 2. SYSTEM OPERATIONAL CAPABILITIES

- 2.1 The VMT-B can provide a wide variety of communication and non-communication signals to replicate battlefield electromagnetic threats. There are several possible ECM modes: continuous, swept, barrage, signal-initiated, repeat, phase coherent repeat, playback, and combination. Target transmissions may be degraded or overpowered by noise, tones, or complex modulations. A victim receiver may be captured or spoofed by amplifying and relaying its intended signal or recording and re-transmitting a previous one. Relayed and retransmitted signals may be altered to achieve a desired effect.
- 2.2 The VMT-B can be used to replicate any number of friendly or threat communication or non-communication emitters within its frequency range, power, and antenna beamwidth limitations. The VMT-B contains six traveling wave tube amplifiers (TWTAs); their frequency ranges and powers are listed in the specifications. The VMT-B also contains a selection of eight parabolic dish antennas with overlapping frequency ranges. Typical gain is 35 dBi. The antenna pedestal stows within the van and is raised to operate at rooftop level on an elevator platform. An IEWTD-designed mounting adapter allows installation of any three antennas, providing a capability to transmit three signals from separate amplifiers simultaneously. The modulation and signal sources provide a capability to produce virtually any signal characteristic.
- 2.3 To complement this versatile emitter, the VMT-B also contains monitoring and analysis equipment. This equipment may be used to capture and characterize a target emission or to develop a VMT-B signal. The signal and data recording equipment may be used for signal documentation and analysis, for storage of the analysis or raw data, or to record a target emission, becoming a source for retransmission. Storage media for data, analysis, and documentation include computer hard disk, floppy disk, CDROM, CD-RW, or hard copy. Hard copy media includes plotter outputs, printer listings, and chart recordings.
- 2.4 All instrumentation can be controlled with a Pentium computer through IEEE-488 or RS-232 buses. Instrumentation support equipment includes signal conditioning modules (amplifiers, video gate, comparator/trigger, pulse stretcher, signal clipper), attenuators, filters, and power meters. A GPS receiver provides self-location and accurate timing.

2.5 An item unique to the VMT-B is the scan/pulse generator. This system can generate four individually programmable pulse patterns and two individually programmable scan patterns. This allows the VMT-B to replicate threat or friendly radar, including their rotating or rastering antennas, with a stationary one. Once programmed, an operator can choose the radar of interest from a computer menu, and the generator will take over. Specifying the pulse width and pulse-to-pulse interval for each interval in the pulse train programs the pulse trains. This interval may be a single, repetitive interval or it may be a sequence of as many as a thousand consecutive intervals, with any individual interval or group of intervals in the sequence repeated as often as 255 times. The antenna scan patterns are generated as piece-wise digital approximations of analog functions. The lobe shapes and amplitudes for a full-antenna scan are programmable in azimuth and elevation. Given a target position, the scan generator calculates the instantaneous angular position relative to the boresight of the transmitting antenna and transmits the appropriate instantaneous amplitude.

### 3. TECHNICAL SPECIFICATIONS

#### 3.1 Transmit: Amplifiers

Frequency (GHz)	Manufacturer	Model	Rated Power (Watts)	Min ERP (kW)
1 - 2	VARIAN	VZL6943G61542	200	22
2 - 4	KELTEC	SR633-200	200	76
4 - 8.2	LOGIMETRICS	A600/C	200	269
8.0 - 12.4	dB Control	dB-4200-0812R1	200	78
12.4 - 18	Applied Sys Eng	200Ku	200	1000
18 - 26.5	dB Control	dB-4101	40	117
26.5 - 40	LOGIMETRICS	A425/Ka	40	55

#### Antenna System:

Tecom Model 204486 Antenna System: Consists of 8 parabolic dish antennas.

Size (inches)	Frequency (GHz)	Gain (dBi)	3dB Beamwidth (degrees)
72	1 - 8.2	21 - 36	12 - 3
48	8.2 - 12.4	36 - 39	2
48	12.4 - 18	39 - 41	1.5
24	18 - 26.5	37 - 38	2
18	26.5 - 40	38 - 41	2 - 1.5
12	18 - 26.5	31 - 34	4 - 3
12	26.5 - 40	34 - 37	3 - 8

Tecom 203076 HD Dual Axis (EL/AZ) Pedestal and a model 203350-2 programmable controller. Specifications: Load capacity 250 pounds (lbs), torque 300-ft lbs, velocity 0-10°/sec, azimuth +/- 400°, elevation -5° to +185°. Integrated video-based, auto-track system consisting of Hamamatsu C3162 X-Y Tracker, Robot Senturion camera controller, Cohu 8210 CCD Camera with 50 to 700mm lens in pressurized enclosure.

Transmit and Jamming Modes:

AM, FM, pulse, hop, swept noise, barrage, signal initiated, repeat, phase coherent repeat, playback, and combination.

Signal Sources:

Anritsu 68367C Synthesized High Performance Signal Generator (2): 0.01 – 40 GHz; resolution 1 kHz; accuracy  $<5 \times 10^{-10}$ /day; harmonics  $<-30$  dBc (10-50 MHz),  $<-40$  dBc (50 MHz - 40 GHz); leveled output level -120 to +3 dBm; output resolution 0.01 dB; modulations CW, AM, FM, pulse, noise; step and analog sweeps; IEEE-488 interface.

Rohde & Schwarz SMIQ06B Vector Signal Generator: 300kHz – 6.4GHz, 0.1 Hz resolution,  $<3.3$  ms, digital sweep. Vector (I&Q), AM, Broadband AM, Pulse, FM, Phase, ASK, FSK, 2FSK, GMSK, QAM (16-256), BPSK, QPSK, QPSK (IS-95), OQPSK, pi/4DQPSK, 8PSK, and 8PSK EDGE modulations. Predefined modulations APCO, C4FM, APCO CQPSK, CDPD, CT2, DECT, GSM, IRIDIUM, NADC, ODC, PHS, TETRA, TFTS, PWT, ICO BPSK, ICO GMSK, ICO QPSK, GSM EDGE, CDMA IS-95, and W-CDMA. Digital Standards IS-95, W-CDMA (2GPP), and more. Internal data and arbitrary waveform generators.

Wiltron 68369B Synthesized Signal Generator: 0.01 - 40 GHz; resolution 0.1 Hz; accuracy  $<5 \times 10^{-10}$ /day; harmonics  $<-30$  dBc (10-50 MHz),  $<-40$  dBc (50 MHz - 40 GHz); output level -110 to +20 dBm; output resolution 0.01 dB; modulations CW, AM, FM, pulse, noise; step and analog sweeps; IEEE-488 interface.

HP 8780A Vector Signal Generator: 10 MHz - 3 GHz, 1-Hz resolution, switching speed  $<220$  ms, vector (I&Q), scalar FM (150 - 50 MHz pp deviation), BPSK, QPSK, 8 PSK, 16 and 64 QAM modulation modes, external analog and digital modulation sources required, IEEE-488 interface.

Fluke 6062A Synthesized RF Signal Generator: 100 kHz – 2,100 MHz; resolution 20 Hz; accuracy  $<\pm 0.5$  ppm/month aging rate; harmonics  $<-30$  dBc ( $<1$  MHz),  $<-25$  dBc ( $\geq 1$  MHz); output level -137 to +13 dBm; output resolution 0.1 dB; modulations CW, AM, FM, pulse, phase; IEEE-488 interface.

HP 3325A Synthesizer/Function Generator: 1  $\mu$ Hz - 21 MHz; sine, square, triangle, negative and positive ramps; 20 ns rise time on square waves; arbitrary function generator via GPIB providing user-defined waveshapes; resolution  $\leq$  1 millihertz (mHz); IEEE-488 interface.

HP 8130A Pulse Generator: 300 MHz, 2-channel; period 3.33 ns to 99.9 ms, width 1.5 ns to 99.9 ms, delay 0 ns – 99.9 ms, transition time 100  $\mu$ s to 1 ns, output amplitude 100 mVp-p – 5 Vp-p into 50ohm, IEEE-488 interface.

HP 8018A Serial Data Generator: 2048 programmable bits, >1 Mbit pseudo random sequences, 2-channel, 6 ns pulses with repetition rates from 0 to 50 Mbit/s, output up to 15 V, IEEE-488 interface.

ANTEKNA L1420-12 Scan/Pulse Generator: PRI 1 to 6553.5 us, pulse width (PW) 0.1 to 409.5 us, resolution 0.1 us. complex pulse: stagger up to 1,000 levels, jitter: linear, gaussian, pseudo-random, wobble: sine, linear, jitter, modulation range (sine and linear): 5–100 Hz, standard scan modes: off, conical (1–100 Hz), circular (.01–2.0 Hz), unidirectional (sector) (.01–50 Hz), bi-directional (sector) (.02–80 Hz), .5–10 degrees beamwidth, complex scans: off, raster (2–20 bars), Palmer (12–80 Hz in 64 steps), helical, & spiral. Pulse output: TTL. Scan output: 0 to +5 V. RS-232 interface.

General Radio 1383 Random Noise Generator: 20 Hz – 20 MHz, Gaussian noise distribution, 1 volt maximum output (open circuit), 80 dB 10 dB step attenuator.

### 3.2 Monitoring and Analysis

HP 71209A Spectrum Analyzer: 100 Hz to 40 GHz, resolution 1 Hz, dynamic range 99-96 dB, amplitude accuracy  $\pm$ 2 dB, IF gain accuracy  $\pm$ 0.9 dB, resolution bw 10 Hz to 3 MHz, noise figure @ 12 GHz 32 dB, LO phase noise @ 6 GHz – 108 dBc/Hz. IEEE-488 interface.

Tektronix TDS 5104 Digital Phosphor Oscilloscope: 1 GHz bw, 5GS/s sample rate (1 ch), 4-ch, color, floppy and CDROM drives, Calculated Rise Time 5 mV/div (typical) 300 ps, input sensitivity 1 mv – 10 v/div, 8 bit resolution, timebase 200 ps – 40s/div, LAN, serial, parallel, USB, PS2, and IEEE-488 interfaces.

HP 5371A Frequency and Time Interval Analyzer: DC – 500 MHz, 10 MHz rate, time interval range –4.0 to +4.0 seconds, 150 ps rms time interval resolution, logical triggering, 2 mV trigger level resolution, 2-channel (ch), IEEE-488 interface.

### 3.3 Support Equipment

Instrumentation Controller: Rack-mounted PC, 933 MHz Pentium 3®, 256 MB RAM, 15 GB hard drive, 4x2x24 CD-RW, 32x CDRom, 3½” floppy drive, AGP 32 MB video (1600x1200), 1 AGP, 2 ISA, and 4 PCI slots, 56K modem, 8-port serial bus extender, IEEE-488.2 interface, onboard sound, rack mount 17”.25 dot pitch-color monitor, and HP 870Cxi color printer.

ASTRO-MED MT9500 Chart Recorder: Direct-writing thermal array 200 dots per inch; 8 channels; frequency response DC – 3 kHz at 1 dB; resolution 12 bit; 16 kb/ch memory; chart speeds 1-100 millimeter (mm) per second, minute, or hour (s, m, h); IEEE-488 interface.

Trimble AccutimeII 6 channel GPS Receiver: TSIP RS-422 data output, 8-32 vdc operating voltage. A software interface application running on the Instrumentation Controller insures that the controller real time clock is set to within 20 ms of UTC, displays current latitude, longitude, altitude (LLA), local and UTC date/time, provides LLA, UTM, and MGRS coordinates via an internal DDE server to any DDE capable client application.

Anritsu ML2438A Power Meter (2): 10 MHz - 40 GHz, dynamic range -70 dBm to +20 dBm, IEEE-488.

Systems Research Labs 1400 Series Lab Modules: Audio amplifier, video amplifier, video gate, programmable operational amplifier, signal clipper, comparator/trigger.

### 3.4 Communications

Motorola MCX1000 Mobile DVP Radio: Digital voice privacy nonlinear digital scrambling, VHF 146-162 MHz, channel spacing 30 kHz, output 30 W.

## 4. SYSTEM LIMITATIONS

The VMT-B antenna systems have very narrow beam widths (12° to 1°) in order to provide the high gain required for simulating threat power levels. The video-based airborne target-tracking capability is only good up to 20 miles during clear, sunny weather.

## **5. PLANNING CONSIDERATIONS**

- 5.1 A 10- to 15-ton commercial or military tractor is required to pull the VMT-B over improved roads only. It has a ground clearance of 14 inches, is 96 inches wide, 40 feet long, and 13 feet 6 inches high. A minimum overpass clearance of 14 feet should be observed. The VMT-B has tie-down rings and can be transported by aircraft. Approximately 4 hours are required for setup and checkout. Equipment with internal reference oscillators can require up to 24 hours warm-up to meet manufacturer's specifications. However, adequate accuracy levels are usually reached after approximately 1 hour of warm-up time. The heating and cooling system on the VMT-B allows it to be operated comfortably in both cold and hot climates. Primary power for the VMT-B is 120/208 VAC, 3-phase, 4-wire, 60 Hz at 100 amps per phase. The VMT-B has an external power cable with pig tails to connect to fused power drops. The on-board 45-kW diesel generator requires approximately 25 gallons of fuel for 8 hours of operation and has a tank capacity of 100 U.S. gallons.
- 5.2 For vulnerability testing, each 8-hour shift operation requires at least two operators. Unless the VMT-B is deployed in a secure area, guards must be employed on-site whenever operators are not present. Visiting the VMT-B during its operation is discouraged.
- 5.3 A complete list of signal frequencies, modulation types, and power levels will be required for frequency authorization well in advance of the test start date. The Motorola communications equipment will require frequency authorization at locations other than Fort Huachuca.

(This page intentionally left blank.)

## SECTION 2.4 VULNERABILITY MOBILE TRANSMITTER C (VMT-C)

---

### 1. SYSTEM DESCRIPTION

The VMT-C represents the IEWTD's ECM capability for the 2 to 30 MHz band. The facility consists of a high-power HF linear amplifier, extremely versatile signal sources, and some monitoring and analysis equipment. Its primary mission is to replicate current and projected threat ECM in support of vulnerability assessments of IEW systems. Secondary missions include threat and friendly signal simulation in support of operational tests. The facility is transportable and is housed in a 40-foot semi-trailer with heating, air conditioning, and an on-board generator. Antenna options are a 32-foot whip that installs on the trailer roof or a separate trailer-mounted LPA with telescoping tower.



**Figure 2.4-1. VMT-C.**



**Figure 2.4-2. VMT-C Front Storage Area and Power Amplifier.**



**Figure 2.4-3. VMT-C SigTek ST-211 HF ESM/ECM System.**



**Figure 2.4-4. VMT-C Control and Analysis Equipment.**



**Figure 2.4-5. VMT-C HF Log Periodic Antenna System.**



**Figure 2.4-6. VMT-C Maintenance Area.**

## 2. SYSTEM OPERATIONAL CAPABILITIES

- 2.1 The VMT-C can replicate a threat jammer or virtually any HF emitter. Its possible ECM modes include: continuous, swept, barrage, signal-initiated, repeat, phase coherent repeat, playback, and a combination. A target transmission may be degraded or over-powered by noise, tones, or complex modulations. A victim receiver may be captured or spoofed by amplifying and relaying its intended signal or recording and re-transmitting a previous one. Relayed and retransmitted signals may be altered to achieve the desired effect.
- 2.2 The VMT-C has the capability to simulate friendly or threat transmitters within its frequency range and power capacity. The RF power amplifier is a 3.5 kW unit with a frequency range of 2-30 MHz; it also has a low power mode of 250 W. The VMT-C has two transmit antennas--a roof-mounted, 32-foot, base-loaded whip and a separate LPA system. This LPA system consists of a trailer-mounted 62-foot telescoping tower, a remote azimuth controller in the VMT-C, and a horizontally polarized LPA with a frequency range of 4–30 MHz and a nominal gain of 10 dBi. An on-board generator provides power for rotating the antenna and extending the tower.
- 2.3 The utility of the VMT-C is complemented by its monitoring and analysis capabilities. These capabilities may be used to capture and characterize a target emission or a VMT-C signal. The signal and data-recording equipment may be used for signal documentation and analysis, storage of the analysis or raw data, or recording of a target emission, which then becomes a source for retransmission. Any data, analysis, or documentation may be stored on hard disk, floppy disk, CDROM, or CD-RW, or can be converted to hard copy. Hard copy media include plotter output or printer listings.
- 2.4 The majority of the instrumentation can be controlled with a Pentium computer through the IEEE-488 or RS-232 buses. Instrumentation support equipment includes signal conditioning modules (amplifiers, video gate, comparator/ trigger, pulse stretcher, signal clipper), attenuators, filters, and power meters. A GPS receiver provides self-location and accurate timing.
- 2.5 An item unique to the VMT-C is the Fast Scan HF Receiver System. With a sweep speed of up to 29.184 MHz per millisecond and a frequency range of 1 to 30.184 MHz, this receiver is designed to intercept and jam frequency agile signals in the HF band.

### 3. TECHNICAL SPECIFICATIONS

#### 3.1 Transmit

Amplifier: Intech COM-4000 Power Amplifier, 2-30 MHz, Class AB linear, RF output power 3.5 kW at 1 dB compression and 3kW at the band edges, 250 W in low power mode, gain 60 dB minimum, small signal gain flatness  $\pm 2$  dB, dynamic range 60 dB minimum, harmonics  $-25$  dBi (2<sup>nd</sup>) and  $-13$  dBi (3<sup>rd</sup>), spurious outputs  $-60$  dBc, input Voltage Standing Wave Ratio (VSWR) 2.0:1 maximum, maximum output VSWR 9.0:1.

#### Antenna Systems:

Harris SB-V35B Whip Antenna with Harris RF-601A Antenna Coupler and Antenna Coupler Controller: 2-30 MHz, power handling capability 1 kW average and PEP, input VSWR 1.5:1 maximum when tuned, tuning time  $<5$  seconds in auto, will match the impedance of 15-, 25-, 28-, and 32-foot antennas.

TELEX 5025BA Log Periodic Antenna System: 4-30 MHz, gain 9 dBi (4-6 MHz) to 12 dBi (6-30 MHz), maximum input power 5 kW average (limited to 3.5 kW average by the feed cable), horizontal polarization. Electric rotator with a rack mounted controller. Tower height 62 feet, longest element 96 feet, weight 7,700 lbs. RS-232 interface.

Transmit and Jamming Modes: AM, FM, pulse, hop, and signal initiated.

#### Sources:

Rohde & Schwarz SMIQ06B Vector Signal Generator: 300kHz – 6.4GHz, 0.1 Hz resolution,  $<3.3$  ms, digital sweep. Vector (I&Q), AM, Broadband AM, Pulse, FM, Phase, ASK, FSK, 2FSK, GMSK, QAM (16-256), BPSK, QPSK, QPSK (IS-95), OQPSK, pi/4DQPSK, 8PSK, and 8PSK EDGE modulations. Predefined modulations APCO, C4FM, APCO CQPSK, CDPD, CT2, DECT, GSM, IRIDIUM, NADC, ODC, PHS, TETRA, TFTS, PWT, ICO BPSK, ICO GMSK, ICO QPSK, GSM EDGE, CDMA IS-95, and W-CDMA. Digital Standards IS-95, W-CDMA (2GPP), and more. Internal data and arbitrary waveform generators.

HP 8642A Signal Generator: 0.1-1,050 MHz; resolution 1 Hz, modulations AM, FM, pulse, and phase, spurious signals  $-100$  dBc (nonharmonic), SSB phase noise @ 20 kHz offset  $<-134$  dBc/Hz, IEEE-488 interface.

HP 8770A Arbitrary Waveform Synthesizer: DC - 50 MHz, 125 MHz internal or

10–130 MHz external sample clock, divisible by 1, 2, 4, 8, 16, 32, 64, 128, or 256; sample size = sample clock period; 131072 12-bit word memory, output -110 to +10 dBm in 10 dB steps, IEEE-488 interface.

HP 8130A Pulse Generator: 300 MHz, 2-channel; period 3.33 ns to 99.9 ms, width 1.5 ns to 99.9 ms, delay 0 ns – 99.9 ms, transition time 100  $\mu$ s to 1 ns, output amplitude 100 mVp-p – 5 Vp-p into 50 ohm, IEEE-488 interface.

HP 3325A Synthesizer/Function Generator: 1  $\mu$ Hz - 21 MHz front, 21–60 MHz rear output; sine, square, triangle, negative and positive ramps, 20 ns rise time on square waves, arbitrary function generator via HPIB providing user-defined wave-shapes, resolution  $\leq$  1 millihertz (mHz), IEEE-488 interface.

### 3.2 Monitoring and Analysis

SIGTEK ST-211 Fast Scan HF Receiver: 1–30.184 MHz, up to 29.184 MHz per millisecond scan rate, resolution 3 or 6 kHz, input amplitude measurement accuracy 1 dB from –40 to –100 dBm, monitor, dehop, and jam modes, 300 hops per second (hps) maximum in monitor and dehop modes, 100 hps in jam mode.

RACAL RA6790/GM (R-2174A(P))/URR HF Receiver: 0.5-30 MHz, resolution 1 Hz, demodulation modes CW, USB/LSB, AM, FM, dynamic range >180 dB/Hz, noise figure < 15 dB, IEEE-488 interface.

HP 8568 Spectrum Analyzer: 100 Hz – 1,500 MHz, resolution bw (-3 dB) 10 Hz to 3 MHz (1,3,10 sequence), video bw 1 Hz - 3 MHz (1,3,10 sequence), amplitude range -135 to +30 dBm, frequency response  $\pm$  1.5 dB, IEEE-488 interface.

Tektronix TDS 5104 Digital Phosphor Oscilloscope: 1 GHz bw, 5GS/s sample rate (1 ch), 4-ch, color, floppy and CDROM drives, Calculated Rise Time 5 mV/div (typical) 300 ps, input sensitivity 1 mv – 10 v/div, 8 bit resolution, timebase 200 ps – 40s/div, LAN, serial, parallel, USB, PS2, and IEEE-488 interfaces.

### 3.3 Support Equipment

Instrumentation Controller: Rack-mounted PC, 933 MHz Pentium 3<sup>®</sup>, 256 MB RAM, 15 GB hard drive, 4x2x24 CD-RW, 24x CDROM, 3½” floppy drive, AGP 32 MB video (1600x1200), 1 AGP, 2 ISA, and 4 PCI slots, 56K modem, IEEE-488.2 interface, onboard sound, rack mount 17”.25 dot pitch-color monitor, and HP 870Cxi color printer.

Trimble AccutimeII 6 channel GPS Receiver: TSIP RS-422 data output, 8-32 vdc operating voltage. A software interface application running on the Instrumentation Controller ensures that the controller's real-time clock is set to within 20 ms of UTC; displays current latitude, longitude, altitude (LLA), local, and UTC date/time; and provides LLA, UTM, and MGRS coordinates via an internal DDE server to any DDE-capable client application.

Bird 4385-832 Wattmeter: Power range 100 mW - 10 kW, 0.45-2,100 MHz, accuracy  $\pm 5\%$  of full scale incident and reflected readings, modulations AM, FM, CW, SSB/DSB, PM, IEEE-488 interface.

Kay 5436 Attenuator: 0- 10 dB in 1 dB steps and 0-70 dB in 10 dB steps.

Krohn-Hite 3202R: Two section tunable high/low pass active filter, 20 Hz to 2 MHz, high/low pass mode attenuation rate 48 dB/octave, bandpass mode attenuation rate 24 dB, maximum input 4 v peak, maximum output level 3 vrms, input impedance 100 kohm, output impedance 50 ohm.

Systems Research Labs 1400 Series Lab Modules: Summing amplifier, log amplifier, video amplifier, video line driver, comparator/trigger, dual channel gate.

#### 3.4 Communications

Motorola MCX1000 Mobile DVP Radio: Digital voice privacy nonlinear digital scrambling, VHF 146 - 162 MHz, Channel Spacing 30 kHz, Output 30 W.

### 4. SYSTEM LIMITATIONS

None

## 5. PLANNING CONSIDERATIONS

- 5.1 A 10- to 15-ton commercial or military tractor is required to pull the VMT-C over improved roads only. It is 96-inch wide, 40-foot long, and 14 feet high. A 15-foot minimum overpass clearance should be observed. It has tie-down rings and can be transported by aircraft. Approximately 3 hours are required for setup and checkout (LPA not used). Equipment with internal reference oscillators can require up to 24 hours warm-up to meet manufacturer's specifications. However, adequate accuracy levels are usually reached after approximately 1 hour of warm-up time. The internal heating and cooling system allows it to be operated comfortably in both cold and hot climates. Primary power is 120/208 VAC, 3-phase, 4-wire, 60 Hz at 100 amps per phase. It has an external power cable to connect to fused power drops. The on-board 45 kW diesel generator requires approximately 25 gallons of fuel for 8 hours of operation and has a tank capacity of 100 U.S. gallons.
- 5.2 If the LPA is to be used, a truck with a standard military style pintle hitch and an 8,000-pound towing capacity are required for transport. Eight hours and two additional personnel are required to erect, guy, and checkout the antenna. A clear area with a 57-foot minimum radius is necessary to site the antenna.
- 5.3 For vulnerability testing, operation of the VMT-C requires at least two equipment operators per 8-hour shift. Unless the VMT-C is deployed in a secure area, guards must be employed on-site whenever operators are not present. Visiting the VMT-C during its operation is discouraged.
- 5.4 A complete list of signal frequencies, modulation types, and power levels will be required for frequency authorization well in advance of the test start date. The Motorola communications equipment will require frequency authorization at locations other than Fort Huachuca.

**SECTION 2.5  
SIGNAL MONITORING, VERIFICATION,  
AND  
FIELD INTENSITY MEASUREMENT EQUIPMENT**

---

**1. SYSTEM DESCRIPTION**

The Signal Monitoring equipment represents the IEWTD's most portable test instrumentation. The primary mission of this equipment is measuring and documenting signal strengths at receiver sites during vulnerability assessments to provide jammer-to-signal (J/S) ratios. This equipment may also be used for threat signal verification in support of operational and customer tests and to determine site suitability in test planning. This equipment is typically portable and lightweight.



**Figure 2.5-1. Signal Monitoring Vehicle.**



**Figure 2.5-2. Spectrum Analyzer and Controller.**



**Figure 2.5-3. AC Generators and Rear Storage Area.**

## 2. SYSTEM OPERATIONAL CAPABILITIES

- 2.1 The Signal Monitoring equipment is a collection of portable communications and electronic measurement instruments. This equipment provides signal-strength measurements and a capability for quick reaction and extreme mobility. This equipment is normally installed in dedicated 4-wheel-drive vans (2) with onboard generators, air conditioning, heating, and telescoping antenna masts. Additional equipment is available to deploy in rented vans or in tactical military vehicles to support a total of four measurement sites. Calibrated Field Intensity Measurements can be performed by these systems **provided** sufficient advance notice is given in order to calibrate the antennas.
- 2.2 The Signal Monitoring instruments **can** include spectrum analyzers, network analyzers, receivers, and oscilloscopes. Antennas are typically passive antennas, such as whips, horns, conical log spiral, biconical, and log periodic antennas. All antennas may be calibrated to provide Field Intensity Measurements. Most instrumentation can be controlled with rack-mounted or portable PCs through IEEE-488 or RS-232 buses. Instrumentation support equipment includes attenuators, filters, and amplifiers. GPS receivers provide self-location and accurate timing. Measurement data, analysis, and documentation can be stored on computer disk (hard disk, floppy disk, CDROM, CD-RW) or converted to hard copy. Hard copy media includes printer listings and plots. Onboard 4-kW generators provide power for field operations. The measurement frequency range is from 10 kHz to 40 GHz. **The “normal” equipment load for a van is a HP 8564E Spectrum Analyzer, an AOR AR8600 Receiver, and a rack-mounted PC.**

## 3. TECHNICAL SPECIFICATIONS

### 3.1 Monitoring, Verification, Analysis, and FIM

HP 8564E Spectrum Analyzer (4): 9 kHz - 40 GHz; resolution bw (-3 dB) 1 Hz - 2 MHz (1,3,10 sequence); video bw 1 Hz - 3 MHz (1,3,10 sequence); amplitude range -139 to +30 dBm; frequency response  $\pm 1.0$  dB 9 kHz - 2.9 GHz,  $\pm 1.7$  dB 2.9 - 6.5 GHz,  $\pm 2.6$  dB 6.5 - 22 GHz,  $\pm 3.3$  dB 22 - 40 GHz; IEEE-488 interface.

HP 8753B (Options 002, 006, and 010) Network Analyzer With HP 85047A S Parameter Test Set: 300 kHz - 6 GHz; resolution 1 Hz; dynamic range 100 dB; harmonics  $\leq -50$  dBc (0 dBm); frequency accuracy  $\pm 10$  parts per million (ppm); sensitivity (3 kHz bw) - 90 dBm (10 kHz bw) - 100 dBm; 2 channels; IEEE-488 interface.

HP 8752A Network Analyzer: 300 kHz - 3 GHz; resolution 1 Hz; dynamic range 100 dB; harmonics  $\leq$  -50 dBc (0 dBm); frequency accuracy  $\pm$  10 parts per million (ppm); sensitivity (3 kHz bw) - 90 dBm (10 kHz bw) - 100 dBm; 2 channels; IEEE-488 interface.

AOR AR8600 Communications Receivers (4): 530 kHz to 2040 MHz, 50-Hz tuning resolution; 3, 9, 12, and 150 kHz; CW, AM, FM, USB, and LSB demodulation modes, AM sensitivity for 10 dB S+N/N; RD-232 interface.

RACAL RA6790/GM (R-2174/URR) HF Receiver: 0.5 - 30 MHz; resolution 1 Hz; modes of operation CW A1, A2; USB/LSB A3A, A3H, A3J, A2A, A2H, A2J; AM A3; FM F3 telephony; dynamic range >180 dB/Hz; noise figure <15 dB; IEEE-488

RACAL RA1796A HF/VHF/UHF Receiver: 2 - 1200 MHz; IF bw 300 Hz, 1.2, 3, 8, 15, 30, and 300 kHz; modes of operation CW A1A, MCW A2A; SSB R3E, H3E, J3E, R2A, H2A, J2A; AM A3E; FM F3E; noise figure <15 dB.

Tektronix 2235 Oscilloscopes (4): 100 MHz bw; sweep rate 5 ns/div to 0.5 s/div; 2-channel; 2% vertical and horizontal accuracy.

#### Antennas:

RC-292 Vertical Whip (4): 1-400 MHz

Conical Log Spiral Antenna: (2) 200-1,000 MHz; circular polarization; 50 ohms impedance.

Biconical Antenna: (2) 20-200 MHz; horizontal or vertical polarization; 50 ohms impedance; length 36-inch; diameter 21-inch

Log Periodic Antenna: (1) 1-18 GHz; horizontal or vertical polarization; 50 ohms impedance.

Horn Antenna Kit: (1) 1-18 GHz; 5 horn antennas with a reflector; horizontal or vertical polarization; 50 ohms impedance; 8-38 dBi gain.

Horn antenna sets (4) covering the frequency range of 1 – 18 GHz and 26 – 40 GHz.

### 3.2 Support Equipment

Instrumentation Controller (2): Rack mount PC, 266 MHz Pentium II MMX, 64 MB RAM, 4 GB hard drive, 1 GB Syquest removable, 3½” floppy drive, AGP video 4 MB 1600x1280, 3 ISA and 4 PCI slots, 8 port serial card, 14.4 modem, GPIB, digital sound card, 17” .25 dot pitch monitor

Trimble AccutimeII 6 channel GPS Receiver (2): TSIP RS-422 data output, 8-32 vdc operating voltage. A software interface application running on the Instrumentation Controller ensures that the controller’s real-time clock is set to within 20 ms of UTC: displays current latitude, longitude, altitude (LLA), local, and UTC date/time, and provides LLA, UTM, and MGRS coordinates via an internal DDE server to any DDE-capable client application.

### 3.3 Communications

Motorola MX350 Hand-Held DVP Radio: VHF 146 - 162 MHz, 2.5 W

## 4. SYSTEM LIMITATIONS

None.

## 5. PLANNING CONSIDERATIONS

5.1 Setup requires two technicians approximately 20 minutes. A temporary installation in a military vehicle or rental van can usually be operational within 30 minutes.

2.1 This equipment has been selected for its portability and is mostly man-portable. Typical deployment is in a dedicated 4-wheel-drive van. This equipment may be shipped by any conventional method and deployed in a van or military vehicle. Power requirement will vary with the selected equipment but in general is 110 VAC, 50–60 HZ and less than 1 kW. Dimensions and weight for the 4-wheel-drive vans are 120 inches high, 80 inches wide, 224 inches long, with a GVW of 10,500 pounds.

5.2 The Motorola communications equipment will require frequency authorization at locations other than Fort Huachuca.

5.3

**CHAPTER 3**  
**AUTOMATED INTELLIGENCE/ELECTRONIC WARFARE**  
**TEST SYSTEM (AI/EWTS)**

---

**1. INTRODUCTION**

- 1.1 The AI/EWTS will be an automated field instrumentation system that simulates an electromagnetic (EM) environment. It will include a software-driven scenario capability and associated analog and digital scripts. The primary mission of the AI/EWTS will be to support operational tests of IEW systems. Realistic testing of IEW systems' issues will require a realistic EM signature of threat forces. AI/EWTS will provide consistent, repeatable EM environments that reflect various threat deployments and scenarios under the control of the test officer.
- 1.2 The AI/EWTS system will consist of major subsystems, including the OTCC; a radio frequency (RF)-based command, control, and communications network; and an array of eleven Mobile Communications Simulator Threat Facilities (MCSTFs). The network receiver/transmitter will be integrated into the MCSTFs.
- 1.3 The OTCC is under development, and initial operational capability (IOC) is scheduled for the first quarter FY03. The OTCC will be the focal point for the conduct of operational tests and will perform such functions as command and control for scenario and script generation, orchestration of the frequency and modulation from each simulator, and monitoring of the EM signals being generated. The OTCC will also serve as a data collection and analysis center by performing near-real-time recording, analysis, and display of test data and results.
- 1.4 The communications network between the OTCC, MCSTFs, and other range assets will use a wireless Ethernet local area network (LAN) concept operating at 11 Mbs in the 2.4 GHz band. An upgrade is planned to increase the data rate to 50 Mbs.
- 1.5 The 11 MCSTFs house communications transmitters that operate in the frequency range of 2 to 1,300 MHz with a very wide variety of modulation capabilities, for example, AM, FM, SSB, PM, FDM, burst, chirp, frequency hopping, and spread spectrum. These transmitters are capable of portraying threat communications signals for use in test and evaluation of IEW assets. The power output of the transmitters is 20 watts from 2 to 30 MHz, 20 watts from 30 to 1000 MHz, and 2 watts from 1 to 1.3 GHz. The power output is capable of being adjusted in 1-dB steps over a 63-dB dynamic range. Four of the MCSTFs have been modified to include 200-watt capability from 2 to 30 MHz, 100 watts from 30 to 1000 MHz, and 50 watts from 1 to 1.3 GHz.

- 1.6 Each MCSTF operates from a time-ordered events list. This list is a script of transmissions unique to that transmitter with the full signal parameters, message content, and the time of execution. On-board storage provides the capability for a script up to 72-hours long or several scripts to be loaded and invoked. The message capability consists of analog and digital messages or digitally recorded voice scripts.
- 1.7 The initial system configuration will consist of one fixed OTCC that can be integrated into a vehicle for mobility and the 11 MCSTFs. This will allow for the orchestration of a threat regimental communications slice in the FM push-to-talk portion of the spectrum and a much larger slice when AM and point-to-point communications are simulated. Currently, each MCSTF can be operated in stand-alone mode using scripts loaded onto the local controller. The future remote and current stand-alone features, variety in modulation types, frequency synthesis of 1 kHz over the entire frequency band, allows the test director a great deal of flexibility. The software-driven automated features of AI/EWTS will provide the ability to repeat tests. Test directors will be able to repeat portions of a test with minimal cost implications or they will be able to repeat tests run years earlier on a system that has either been redesigned or modified.
- 1.8 The MCSTFs are currently in the process of an upgrade that should be completed by the end of FY02. An unmanned canister version is also in development with several of these transmitters available by the first quarter FY03. The upgrade of the truck-mounted transmitter is primarily focused on increased modulation capability. Additional modulations include: FDM up to 12 independent channels; stacked carrier up to 12 independent channels; cellular phones (TDMA, CDMA, GSM PCS, GSM DCS, NADC, PDC, PHS, TETRA); QPSK (OPSK, p/4DQPSK); PSK (8PSK, 16PSK); QAM 4, 16, 32, 64, 256. The upper frequency limit of these units will increase to 2 GHz. The new system will transmit a minimum of four simultaneous signals but can provide many more depending upon signal type. The only decrease in capability is a reduction in hop rate from 100K to 35K hops per second to greatly increase reliability. The canister versions will have 12 dedicated channels and will provide a minimum of 12 simultaneous signals, up to 20, with software management. The canister will operate up to 3 GHz but at a slightly lower RF power output than the truck-mounted systems.

**SECTION 3.1**  
**OPERATIONAL TEST CONTROL CENTER (OTCC)**  
**AND COMMUNICATION NETWORK**

---

**1. SYSTEM DESCRIPTION**

- 1.1 The OTCC is under development with an IOC of first quarter FY03. It will be a centralized command and control facility that operates at the hub of a high-speed network with interfaces to range assets, ground-truth monitoring, units-under-test, and off-range elements, such as evaluators, mission planners, and command-level (ATEC) elements. The network will use Ethernet architecture with an initial capacity of 10 Mb/sec.
- 1.2 The system will be based on the Integrated Test Operations and Control (ITOC) software. This software will control access to the network, configuration of the range elements, command and control of the test activities, and analysis of the data collected from both the ground-truth sensors and the real-time Data Acquisition System (DAS).
- 1.3 The hardware that will support the activities in the OTCC include four multipurpose computers running Windows 2000 Professional, a pair of transceivers for range network control and real-time data collection, two FSP-7 spectrum analyzers, two multibeam antenna systems for range control, and two antennas for ground-truth monitoring. A large (62-inch) display for illustrating range activities will also be included.
- 1.4 There will be four consoles in the OTCC. The Range Control Officer's (RCO) console will perform real-time command and control of the range assets as required. The RCO console will access the range elements directly and, from this position, will extract information from individual sites, access detailed data regarding status, scripts that are running, and numerous detailed information useful for understanding and displaying the on-going operations. The RCO also will control the real-time Data Acquisition System (DAS). The DAS will be a remotely operated data collection system that will be installed in the system-under-test (SUT) to monitor the SUT 1553B data bus. A software application will control the collection of data from this bus and will transmit the data, in real-time, to the OTCC on a special radio channel dedicated to this activity. The data will then be transferred to local storage on a dedicated DAS console in the OTCC. At this console, data analysis and evaluation software can be attached to the receive process and streamed to monitor software in real-time for display.

- 1.5 The Test Officer's (TO) console will be positioned next to the RCO console. It will have a geo-referenced presentation of the range and the elements on the range. The TO console will be network connected to the RCO console and will receive data from the RCO applications. The applications running in the TO console will be specifically designed to support the test activities. They will present a timely report on all range events. The TO will also be able to request special data from the RCO, which will then be automatically passed to the TO applications for processing.
- 1.6 The Ground-truth Monitoring (GTM) console will provide real-time control and monitoring of the specialized data collection equipment used to establish the presence and characteristics of targeted signal emissions. Signal characteristics, such as carrier frequency, modulation type and value, and signal amplitude, are captured and stored in a common file structure. The equipment will be synchronized with the scripted activity of the targeted range emitters and will run in an unattended, automatic manner. The monitoring units will be rapidly tuned and set up to collect the specified signals' modulation characteristics and to store these on the network drives for analysis and evaluation. This will be done in pseudo real-time with the spectral display presented on any of the network monitors.
- 1.7 The generation of scripted range activity will also be supported in the OTCC. Both the TO and RCO consoles will be able to create the resource files needed to control an exercise. The applications that support this activity will generate from 800 to 1000 scripts per hour of operation. These scripts will include all of the collateral files needed for range support, such as the GTM and the DAS.
- 1.8 The range network will normally be set up via line-of-sight operations to each individual range asset but will also incorporate relay capabilities to extend the network range, if necessary.

## **2. SYSTEM OPERATIONAL CAPABILITIES**

- 2.1 From the OTCC the test director will be able to coordinate the range activities required to produce, monitor, and verify the electromagnetic signal environment for the operational test of a SUT. The OTCC will also provide the capability to interface normal range activities, such as data collection, mission planning and rehearsal, quick-look evaluations, and other time-critical needs, to qualified outside interests using the network interface and control software in the ITOC application.

- 2.2 The OTCC will be established as a fixed installation in the Hayes Hall compound at Fort Huachuca. The system will be easily convertible to mobile configuration using a standard power source, such as a diesel generator, and a portable tower for the antenna systems.

### 3. TECHNICAL SPECIFICATIONS

#### 3.1 Operational Test Control

Controller: Commercial grade Intel P4-based computer systems configured as workstations on a 100 MB/sec network. Monitors will be 19-inch high-resolution color. Other standard office environment accessories such as printers and CD recorders, will be included.

#### Communication Link:

WILAN 120-24 Wireless Ethernet bridge configured for extended range operation: Data rate 11 Mb/sec; operating frequency 2.4 – 2.485 GHz; operating temperature range 0-40°C

#### Monitoring System:

Two Rhode & Schwarz FSP-7 Spectrum Analyzers, network controlled.

Applied Communications SRS-2500 VHF/UHF Receiving System, consisting of a CA-2100 Control Address Unit, DD-2100 Digital Distribution Unit, IX-2100 IF Switch, 6 SR-2154 VHF/UHF Surveillance Receivers; 20-1,200 MHz; tuning resolution 10 Hz; IF BW selectable from 10, 20, 30, 50, 60, 100, 150, 300, 500 kHz, 1, 2, 4, 8, 10 MHz; detection modes AM, FM, CW, LSB, USB, and pulse; IEEE-488 interface.

AEL Model APN-1202A Log Periodic Antenna (LPA): 20-1,000 MHz; beamwidth 60° Gain 4-7 dBi

Andrews Corporation Model 4ST Tower: Height of 70 feet, plus a 6-foot mast

#### **4. SYSTEM LIMITATIONS**

- 4.1 The real-time GTM system will be able to document the environment from two locations. One of these locations will usually be close to the SUT. The second location may be down-range or both units may be located down-range. In either case, both units will be accessible through the range network software (ITOC) and will be able to operate independently and unmanned.
- 4.2 The network system will initially be restricted to a range of 50 km. The range will expand to 300 km with the addition of more transceiver resources.

#### **5. PLANNING CONSIDERATIONS**

- 5.1 The OTCC will be located in a secure fenced compound. Access will require a security clearance be sent to our security office.
- 5.2 Care should be taken when choosing sites for the mobile OTCC. Extreme grades, wet locations, and areas with high grass; dry brush; or loose, soft dirt or sand must be avoided. The antenna mast should not be located within 100 feet of overhead cables, tall trees, or other obstructions. An approximate site diameter of 90 feet should be sufficient. Travel to and from the site should be confined to improved roads when possible. Short distances on well-maintained dirt roads may be considered.
- 5.3 The network transceivers do not require frequency authorization. They operate within the FCC Part 15 unlicensed band at 2.4 GHz.

**SECTION 3.2**  
**MOBILE COMMUNICATIONS SIMULATOR THREAT FACILITY (MCSTF)**

---

**1. SYSTEM DESCRIPTION**

- 1.1 The MCSTF (11 systems) are fully integrated mobile communications simulators designed to house all equipment, power, and personnel associated with operation of the system. An MCSTF consists of a Ford E-350 cutaway chassis, an environmentally controlled shelter, an onboard 14.5-kW generator, a Lambda 24 VDC, 50A power supply, a Hadron CPD Inc. RCS-4041 Transportable Communications Simulator (TCS), a rack-mounted Instrumentation Controller (PC) with color monitor, a L3/Conic Digital Communications Network System (DCNS) unit with antennas, a GPS receiver, a 30-foot telescoping antenna mast, and associated antennas. The shelter is designed for maximum operational utility and as a comfortable workplace for operational personnel. Four of the eleven TCS systems are configured as high-power (HP) emitters and use additional high-power linear amplifiers. A twelfth system (also HP), with an associated RMG, has been mounted in two standard 19-inch equipment racks. It can be used as a fixed site emitter or can be located within one of the ECM (VMT A, B, or C) facilities to act as a signal source if higher power levels are needed.



**Figure 4.2-1. MCSTF.**

- 1.2 The TCS is a microprocessor-based communications simulator capable of providing numerous types of modulation within a frequency range of 2 and 1300 MHz. The system is mounted in fiberglass enclosures within the van. The TCS is a completely software-driven emitter using four Z80 microprocessors. They provide control for all frequency, modulation characteristics, and power output adjustments. Command, status, and message data to and from the simulator are transmitted/received by the instrumentation controller (hereafter referred to as the Remote Message Generator (RMG)) via an RS-232 bus.



**Figure 4.2-2. RMG and TCS.**

- 1.3 The RMG consists of a rack-mounted 266 MHz Pentium II PC with a 4-Gb hard disk, 1.44-Mb floppy disk, CDROM, CD-RW, sound card, RS-232 and IEEE-488 interfaces, the GPS interface application, and the RMG graphical user interface (GUI) application. The RMG GUI sends system setup commands, such as frequency, modulation type, power level, etc., to the TCS and uses prerecorded voice and message files loaded on the hard disk to modulate the TCS RF emissions. In the digital modulation modes, the message data stream (ASCII text) is encoded in accordance with the command setup parameters and is used to modulate digital transmissions, such as OOK, FSK, BPSK, etc. Stored voice files are played back through the RMG sound card and are applied to the TCS audio input(s). The MCSTF-mounted GPS receiver provides location information and accurate timing for the RMG.

## 2. SYSTEM OPERATIONAL CAPABILITIES

- 2.1 Section 3.3 lists the variety of modulation types and parameters available for the synthesis of an EM environment. The test director can select parameters that reflect a wide variety of analog and digital communications equipment. The external high-speed data port (20 Mbps) provides another means to introduce digital data communications signals.
- 2.2 The antenna subsystem configuration consists of a long-wire antenna (2 to 30 MHz), discone antenna (30 to 100 MHz), and two LPAs (100 to 1,300 MHz and 1–1.3 GHz). Except for the HF long-wire, the antennas mount on a single telescoping mast that is capable of being erected by a two-man team. All elements of the antenna subsystem, including the mast, have specific storage areas within the mobile van. The mast is retracted to roof level for transport. The antenna subsystem is also capable of being erected on the ground using a multisectional lightweight mast.
- 2.3 Each mobile communications threat facility can be powered with its own generator or with three-phase commercial power.



**Figure 4.2-3. MCSTF Generator.**

- 2.4 The RMG computer is capable of storing on its hard disk sufficient data to provide numerous scenarios or scripts, even 72-hour continuous test operations. The scenario or script consists of callsigns and associated nets, frequency and modulation schemes, messages (voice or data), and time tags so that the emissions from multiple TCSs sound like realistic net traffic. Management of units is synthesized through the appropriate assignment of callsigns and frequencies to other simulators so that, to a SUT, the communications net and associated unit may appear to have moved from one position to another. The CDROM/CD-RW drives allow for additional flexibility in the transporting of scripts or in the ability to rapidly change to a new script. Test officers may use the baseline library of scenarios and scripts as is or may modify them for their specific test requirements. However, each test officer will have the software capability necessary to generate a new scenario or script for his test.

### 3. TECHNICAL SPECIFICATIONS

#### 3.1 Vehicle

Ford E-350 Cutaway Chassis; 138-inch Wheelbase; 351 CID V8 gasoline engine; dual 20-gallon gas tanks; 11-foot, 5-inch loadspace length; 78-inch interior width; 74-inch interior height; shelter heater/air conditioner unit; full insulation.

#### 3.2 Antenna Systems:

Barker and Williamson AC-1.8-30 Long Wire Antenna: 1.8-30 MHz; 100-foot wire, inverted V; maximum VSWR: 2:1 (1.4:1 average); power rating 1.5 kW; nominal gain 2 dBi.

Telex Hy-Gain 4213AD Discone: 30-100 MHz; polarization vertical; omnidirectional; maximum VSWR 3:1; power rating 500 W; nominal gain 0 dBi.

Telex Hy-Gain LP-1019BA LPA: 100-1,100 MHz; polarization vertical or horizontal; beamwidth 70°, nominal gain 6 dBi; maximum VSWR 3.5:1; power rating 100 W.

Rozendal Associates, Inc. RA-2920-1 LPA: .85–2 GHz; polarization vertical or horizontal; mid-band beamwidth 74°; nominal gain 3 dBi; maximum VSWR 2.0:1; power rating 100-W CW.

### 3.3 TCS

Frequency:	
Range:	2-1,300 MHz
Resolution:	1 kHz
Accuracy:	± 1 ppm (short-term)
Stability:	± 0.1 ppm per day
RF Power Output (50 ohm load):	
Low Power (LP) Units (8)	
2 - 1000 MHz	20 W
1 - 1.3 GHz	2 W
High Power (HP) Units (4)	
2 - 30 MHz	200 W
30 – 1000 MHz	100 W
1 – 1.3 GHz	50 W
Dynamic Range:	63 dB below maximum power output
Resolution:	1.0 dB steps
Accuracy:	+/- 1.0 dB
Spurious:	<-20 dBc (LP) <-40 dBc (HP)
Harmonics, 2nd and 3rd:	<-60 dBc

#### Signal Characteristics

Analog Modulation Bandwidth:	
External:	300–3,800 Hz
Internal Tone:	4 Hz – 40 kHz

Modulation Types:	
CW	
OOK	Key Rate: DC to 1Mbit/sec
AM DSB	Percent Mod: variable 1 to 90
ISB	Modulation Percentage for side
LSB	band modes is 80 %
USB	

Note: AM and SB modulations may be operated with suppressed carrier.  
Carrier suppression is -44 dBc minimum , -50 dBc typically.

FSK	Key Rate:	DC to 20 Mbit/sec
	Shift:	1 Hz to 10 MHz
	Mode:	2 and 4 level
FM		Mod bw: 300-3,800 Hz
		Peak Deviation: 1 Hz to 20 MHz
FDM		4 or 5 channels
	Baseband	
	Channel Spacing:	4 kHz (starts at 0 Hz)
	Mod bw:	300-3,800 Hz
	Modulation Type:	LSB or USB
BPSK		Rate: 50 to 20 M bps
		Encoding: Differential
QPSK		Rate: 50 to 20 M bps
		Encoding: Differential
VCO Hop		Rates: 1 Hz - 200 kHz
	Steps:	255
	Minimum Step Size:	1 kHz, RF Freq 2-80 MHz
		5 kHz, RF Freq 80-1300
	Maximum Step Size:	500 MHz
	Patterns:	Random, Sinusoidal, Sawtooth, and Trapezoid
Chirp		
	Deviation:	10%, of Carrier, Carrier <200 MHz, 20 MHz, Carrier >200 MHz.
	Rate:	50 Hz – 10 MHz
Burst		
	Duration:	1 µsec to 900 sec
	Mode:	All modulations
Squelch Tone		4 Hz to 40 kHz (AM and FM only)
Simultaneous/Sequential		16 Different Tone Codes
		300-3000 Hz
		Variable Pulse Duration

### Spread Spectrum

Modes	FHOP, DSSS, Hybrid
Rates	1 hop/s to 100 khop/s (FHOP) 1 Hz to 20 MHz (DSSS)
Patterns	Pseudo random and programmed

#### 3.4 Remote Message Generator

Rack-mount, 266 MHz Pentium II MMX, 64 MB RAM, 4 GB hard drive, 32x CDROM, 4x2x24x CD-RW, 3½” floppy drive, AGP video 4 MB 1600x1280, 3 ISA and 4 PCI slots, 8-port serial extender, 14.4 modem, IEEE-488 Interface, sound card, 17” .25 dot pitch-color monitor.

#### 3.5 Support Equipment

Trimble AccutimeII 6 channel GPS Receiver (2): TSIP RS-422 data output, 8-32 vdc operating voltage. A software interface application running on the Instrumentation Controller ensures that the controller’s real-time clock is set to within 20 ms of UTC; displays current latitude, longitude, altitude (LLA), local, and UTC date/time; and provides LLA, UTM, and MGRS coordinates via an internal DDE server to any DDE-capable client application.

#### 3.6 Communications

Motorola MCX1000 Mobile DVP Radio: Digital voice privacy nonlinear digital scrambling, VHF 146 - 162 MHz, channel spacing 30 kHz, output 30 W.

## 4. SYSTEM LIMITATIONS

Although the emitters radiate one signal at a time, each simulator can represent many different frequencies and modulations, as well as players, in many nets (HF, VHF, UHF). Thus, the threat array of 11 simulators represents a significant FM ground environment for testing IEW assets.

## 5. PLANNING CONSIDERATIONS

- 5.1 Care should be taken when choosing sites for the MCSTF. Avoid extreme grades, wet locations, and areas with high grass; dry brush; or loose, soft dirt or sand. The antenna mast should NOT be located within 100 feet of overhead cables, tall trees, or other obstructions. An approximate site diameter of 90 feet (150 feet below 30 MHz) should be sufficient. Travel to and from the site should be confined to improved roads when possible; short distances on well-maintained dirt roads may be considered. Two operator/technicians are required per MCSTF. Setup and checkout is accomplished in approximately 45 minutes. Power requirements are 110/208 VAC, 60 Hz, 3-phase, 4-wire, 50A/phase, or 1.5 gallons of gasoline per hour for the on-board generator. Dimensions and weight for a MCSTF are 123 inches high, 93 inches wide, 256 inches long, with a GVW of 10,300 pounds.
- 5.2 A complete list of signal frequencies, modulation types, and power levels will be required for frequency authorization well in advance of the test start date. The Motorola communications equipment will require frequency authorization at locations other than Fort Huachuca.
- 5.3

## CHAPTER 4 MOBILE THREAT EMITTER

---

### 1. INTRODUCTION/DESCRIPTION

The Mobile Threat Emitter (MTE) positions (three systems) are standard M-1038 HMMWVs that have been configured to serve as a platforms for a wide variety of tactical radios. The MTE positions are capable of travel over almost any terrain, under all but the most severe weather conditions. This allows the test officer complete flexibility in positioning his threat emitters to more realistically represent the battlefield environment.



**Figure 4-1. Mobile Threat Emitter.**



**Figure 4-2. Mobile Threat Emitter Equipment.**

## **2. SYSTEM OPERATIONAL CAPABILITIES**

Each MTE has provisions for mounting up to six tactical transceivers. Also included in the suite are one to two GPS receivers, a laptop computer to act as the controller, and a 1.7-kW DC to AC power inverter in the event AC power is required for other equipment. One GPS receiver is identical to and performs the same location and accurate timing function as those installed on all of IEWTD's emitter assets. The other GPS unit can be a very accurate 12-channel, differentially correctable set with on-the-move position data logging capability. The laptop computer, running the RMG application, and via a solid state audio interface and keyer unit, sends voice audio and keys a selected transmitter in accordance with scripted test events.

## **3. TECHNICAL SPECIFICATIONS**

Tactical transceivers that can be installed in the MTE are the R-123, R-134, R-159, R-171, R-173, AN/VRC-94(V), JAGUAR-V, and the SCIMITAR-V. Their specifications are detailed in chapter 6.

## **4. SYSTEM LIMITATIONS**

Due to the lack of sufficient antenna mounting locations on the M-1038, only four antennas are installed at any one time. With some transceiver mixes, the test mission(s) may have to be suspended for short periods of time to allow for manual antenna changeover.

**5. PLANNING CONSIDERATIONS**

- 5.1 Since these systems are self-contained and are based on a standard military vehicle, no special considerations are necessary beyond those needed for any other wheeled military vehicle. Two operator/technicians are required per MTE.

(This page intentionally left blank.)

## CHAPTER 5 COMMUNICATIONS-ELECTRONICS (CE) SHOP

---

### 1. INTRODUCTION/DESCRIPTION

The CE Shop is an installation, maintenance, repair, and storage facility for IEWTD's tactical radio assets. The primary mission of these assets is to provide emitters in support of operational tests of IEW systems. They can also provide communications links that can be used to evaluate the effectiveness of ECM systems. These radios are typically low and medium power push-to-talk radios. Some discrete radios maybe installed in the MCSTFs or other vehicles and, through the use of an automated keying device, transmit the same scripted traffic used by the MCSTF systems. Test players can also operate these radio assets in doctrinally correct, scripted scenarios. The CE Shop provides training, support, and control on these radios before, during, and after the test.

### 2. SYSTEM OPERATIONAL CAPABILITIES

The IEWTD's tactical radios may be deployed individually, paired, or in doctrinally correct formations (see figures 5-1 through 5-5). Power outputs range from 0.5 to 100 W. Modulation types include AM, FM, CW, FSK, and SSB. Some of these assets are friendly radios with enough similarity to their threat counterparts to provide an adequate test target. Many are actual threat radios, lending conclusive evidence to a test's results.

### 3. TECHNICAL SPECIFICATIONS

#### Tactical Radios:

<u>Radio Type</u>	<u>Freq Range (MHz)</u>	<u>Modulation Types</u>	<u>Power Out (W)</u>	<u>No.</u>	<u>Comment</u>
R-105	36 – 46	FM	2	3	vertical whip antenna
R-123	20 - 51.5	FM	20	6	vertical whip antenna
R-134	1.5 – 29.9	FM	5, 7.5, 15, 50	2	vertical whip antenna
R-159	30 - 76	FM	5	3	Data @ 16 kb/s
R-163-10V	80 - 120	FM	3, 10	2	Data @ 16 or 32 kb/s
R-171M	30 - 76	FM	10	2	Data @ 16 kb/s
R-173	30 - 80	FM	30	1	vertical whip antenna

AN/VRC-94A(V)	30-89.975	FM	1, 10, 50	6	vertical whip antenna. frequency agile, 100 hops/second, variable dwell, 5-60 MHz hop bandwidth embedded encryption device.
JAGUAR-V	30-87.975	FM	3, 16, 50	5	vertical whip antenna. frequency agile, 100 hops/second. Hops in 1 of 9 bands (6.4 MHz wide) or over the entire frequency range.
SCIMITAR-V	30 – 87.975	FM	.1, 5, 50		vertical whip antenna frequency agile, 250 hops/second

#### 4. **SYSTEM LIMITATIONS**

In some cases, the friendly radios do not accurately represent the output power of their threat counterpart; however, frequency range, bw, and antennas are usually close enough to be considered surrogates. In these cases, the link distances may be scaled up or down to compensate.

#### 5. **PLANNING CONSIDERATIONS**

5.1 These discrete radios require 24-VDC power and antenna-mounting provisions. These radios are typically installed in military vehicles. Once installed, deployment requires only travel time to a site, the antenna to be set up or released from its restraining clip, and the radios turned on. As tactical military equipment, these systems are very rugged and portable. This equipment may be shipped by any conventional method. The discrete radios may be installed in vehicles and driven to other test locations.

5.2

## CHAPTER 6

### GPS AND VIDEO INSTRUMENTATION

---

#### 1. INTRODUCTION/DESCRIPTION

- 1.1 GPS Instrumentation. This instrumentation system provides geographical position location information for either test planning or test execution. It can be used to survey locations for RF emitters and the SUT or to record movements of instrumented targets for testing reconnaissance systems. It consists of a Trimble Pathfinder Community Base Station, a PC with Trimble Pathfinder Office GPS Data Processing software, and 25 Pathfinder Pro XL portable receivers.
  
- 1.2 Video Instrumentation. The video assets consist of digital and analog video imaging, recording, and processing equipment vehicle-mounted in a modified S-250 shelter on the back of a HMMWV. There is also additional video equipment, which can either be vehicle-mounted or mounted in some other form of shelter. Their primary use is to document and review the performance of the SUT or the operator's display. Such systems include reconnaissance systems, intelligence processing systems, survivability systems, and other information display-oriented systems. In addition, this equipment is used to document the man-machine interface of the SUT to support the testing of manpower and personnel integration (MANPRINT) issues. This equipment consists of commercial video cameras, VHS VCRs, monitors, scan converters with HDTV VCRs, and customized digital A/D compressors/recorders.

## 2. SYSTEM OPERATIONAL CAPABILITIES

- 2.1 The GPS location recording system represents IEWTD's target location capability. It can record over 8 hours of three-dimensional location and velocity data for as many as 25 instrumented targets. The system is capable of an update rate of 1 second or more and can achieve submeter accuracy through postdifferential correction.



**Figure 6-1. GPS.**

- 2.1.1. The GPS base station is a Trimble Navigation Pathfinder Community Base Station. It consists of a Trimble Pro XR 12-channel GPS receiver with Everest Multipath Rejection Technology, an L1 antenna with groundplane, and an operating and data logging software package. It can be powered by 10–32 VDC or from a 120/220 VAC adapter. Its antenna is located on a first-order-survey point. It continually logs all in-view GPS satellite measurement data to its associated PC hard drive. Sufficient hard drive space is available to log several weeks of measurements. A typical 24-hour file consumes approximately 250 kilobytes. These measurement files can later be used to differentially and phase correct the GPS positions logged by other compatible GPS receivers, such as the Trimble Pro XL.

- 2.1.2. The Trimble Navigation Pro XL (25) is an 8-channel GPS Maxwell receiver that can compute three-dimensional positions as often as one per second. In addition, it can provide navigation information to and from up to 99 waypoints, along with velocity and satellite almanac information. The TDC1 data logger can store 1 Mb of data. In the rover-recording mode, it will record approximately 29,000 position fixes, over approximately 8 hours at 1-second intervals. The Pro XL receiver and TDC1 combination are battery-operated and man-portable. They weigh less than 7 pounds. The antenna is separate and easily mounted to a vehicle roof. Both the receiver and the data logger operate in temperature extremes and at up to 99 percent humidity.
- 2.1.3. In addition, there are three Trimble Basic Plus 6-channel GPS receivers. These are smaller, hand-held, portable units with comparable performance and built-in or external antennas but with less data storage capacity.
- 2.1.4. The postdifferential processor consists of a PC with high-resolution graphics, a large hard drive, and 10 RS-232 serial ports, associated cabling, and Trimble Pathfinder Office software. Data are downloaded from the rover data logger onto the PC hard drive. The software provides differential and phase correction routines using the satellite data collected by the CBS and the roving or remote GPS unit. Additional capabilities include data file manipulation, graphical display, plots of position data, and transfer of the data files into geographic or graphics applications software. Submeter accuracy, using both differential and phase correction, can be achieved.
- 2.2 IEWTD's commercial grade video assets consist primarily of video cameras, video cassette recorders (VCRs), monitors, NTSC scan-line converters, high-end scan-line converters, HDTV video recorders, and time-insertion equipment. The scan-line converters transform computer graphics signals to broadcast analog video for recording on conventional equipment. The NTSC converters are compatible with VHS and S-VHS recorders. The high-end converters work with high-resolution HDTV recorders.
  - 2.2.1. The time-tagging equipment uses GPS as a time reference, converts it to IRIG-B, distributes it to each recorder, and inserts it into the video image as it is recorded. The video insertion translates the IRIG-B time information into a composite video signal, providing a time-tag in every frame of the video data. Time may also be recorded on an audio track of the videotape to avoid insertion into the image while providing accurate time-tagging.

2.2.2. The video HMMWV brings a four-wheel drive capability that allows the video equipment to be used at almost any remote location. The video suite consists of three RGB processing equipment and recorders, which allows HD recording at 1280x1024 pixels. It also has three NTSC recorders, which allows S-VHS recording for up to 3 hours. All recordings are time-stamped.



**Figure 6-2. Video HMMWV.**



**Figure 6-3. Curbside.**



**Figure 6-4. Roadside.**

2.2.3. The High Speed Data Recording System (HSDRS) is a real-time, multitasking, computer-controlled, video-acquisition, compression, and recording system. It is being developed to record simultaneous streams of NTSC and up to 1600x1280 RGB video for synchronized playback in the analysis of test events. Live RGB video at full-frame rate has a data volume of 247.5 Mbytes per second, or 870 Gbytes per hour. The HSDRS, by capturing only 10 frames per second and using standard compression routines, reduces the data volume to less than 1 Mbyte per second. This RGB imagery data will be combined with the NTSC and audio data and recorded as a composite.

2.2.4. Storage will be provided on SCSI removable hard drives and high-speed digital tape. During analysis, the hard drives will provide instant access to arbitrary test events. The tapes will provide inexpensive data archiving. Operator interface, for real-time data collectors and during recording and playback, will be a standard PC. The system will provide a quick-look capability for real-time data verification. Connectivity through Ethernet will allow any workstation to replace or access the processes of any other. Overall, the system will record two RGB and two NTSC video sources. It will support four recording locations in any mix of the above sources. The recording of all these sources will be synchronized and time-tagged to millisecond accuracy referenced to GPS time. An analyst may have several sources, in synch or at arbitrary times, replayed on individual monitors or windows.

### 3. SYSTEM CAPABILITIES/SPECIFICATIONS

#### GPS Location Recording Assets:

<u>Receiver Type</u>	<u>Manufacturer</u>	<u>Model</u>	<u>No.</u>	<u>Comments</u>
Community Station Base	Trimble	Pro XR	1	Depending on conditions, and providing the rovers are within 1,000 km of the CBS, accuracy using differential correction can be better than 50 cm + 1 ppm horizontal RMS and submeter + 2 ppm vertical.
Rovers	Trimble	Pathfinder Pro XL with	25	Accuracy without differential correction is 100 meters or less, TDC1 Data Logger depending on conditions.
	Trimble	Pathfinder Basic Plus	3	Accuracy without differential correction is typically between 12 and 40 meters CEP. Within 500 km, using differential correction, 1–5 meter CEP is possible.

**Video Assets:**

<u>Item</u>	<u>Manufacturer</u>	<u>Model</u>	<u>No</u>	<u>Comments</u>
Video Camera	Panasonic	WV-CP610	9	NTSC, 480 lines out, AC, 3 lux @ F1.4
VHS Recorder	Panasonic	AG-6400	2	Portable, AC/DC
S-VHS Recorder	Panasonic	AG-7400	13	Portable, AC/DC
Monitor	Panasonic	CT-2010Y	8	High Res 640 x 480, 20 inch
Monitor	Viewsonic	P95F	8	High Res 1920 x 1440, RGB Monitor, 19 inch
Scan Converter	RGB Spectrum	Videolink HD	10	Input up to 1280x1024 pixels RGB, Pixel depth 24 bit, RS-232 control, Horiz 15-90 kHz, Vert 20-76 Hz, Output 1125 lines, 30 Hz, 33.75 kHz.
W-VHS Recorder HDTV	JVC	SR-W5U	10	1125 lines, 2 audio channels
GPS Time/Freq Receiver Time Inserter	Tru-Time	XL-DC	4	IRIG-B video time insertion
Time Code Gen	Datum	9100	4	IRIG-B, pulse, sync
Time Code Gen Translator	Datum	9300	4	IRIG-B, pulse, sync
HSDRS 31 January 2002 Delivery Date	AP Labs		2	Input up to 1600x1280 pixels RGB, 2 RGB, 2 NTSC, Associated Audio Channels, 76Hz Refresh Rate, MPEG, JPEG, Up to 30 frames/sec, 640X480 NTSC 10 frames/sec, 1600X1280 @76Hz RGB

#### **4. SYSTEM LIMITATIONS**

- 4.1 The GPS location recording system is limited to a typical 8 hour mission day due to battery power and data capacity.
- 4.2 The video assets are typical commercial units and are susceptible to extreme temperatures, humidity, dust, and shock. The high-resolution RGB recording can be performed in either analog or digital, each with limitations. The analog recording of RGB is at full-frame rate and is very faithful in resolution. However, this recording is more expensive due to the cost of the tape, and review of the tape is hampered by absence of any search/seek capability and minutes spent winding the tape to specific events. The digital system is limited to capturing a maximum of 10 frames per second.

#### **5. PLANNING CONSIDERATIONS**

- 5.1 For differential processing of the GPS location information, the base station antenna must be placed on a first-order-survey point. The portable GPS sets are rugged, all-weather units and may be shipped by any conventional method or installed in vehicles and driven to test locations. The video assets are comprised of commercial equipment and are more fragile. They require special packing for shipment and clean, mild environments for deployment. In addition, they often require fabrication of custom mounts.

5.2

## CHAPTER 7

### INFORMATION ASSURANCE TEST TOOL (IATT)

---

#### **1. INTRODUCTION/DESCRIPTION**

IATT-Illuminate is an integrated set of tools and threats that conduct live interactive and scripted information attacks on a target network. These attacks are used for three major purposes. First, they can be used as a Red Team (OPFOR) capability against blue systems undergoing Test and Evaluation (T&E) during developmental and operational tests. Sample Blue targeted systems include perimeter defenses (firewalls, routers, and intrusion detection systems) or specific C4I assets (e.g., ISYSCON, ASAS, FBCB2). Secondly, they can be used as an OPFOR capability to train network operators to recognize and defeat opposing attacks. Blue systems defense requires the detection, analysis, and response to noisy, stealthy, and/or multiple simultaneous coordinated attacks from the opposing force. Thirdly, they can be used as part of a wargaming suite to support Blue network defender “what if” analysis by simulating Blue networks under Red-launched CNA.

#### **System Configuration and Construction**

The current collection of tools within IATT-Illuminate was created using the latest open source software and network analysis. Many threats described in open sources are simply a misuse of standard network administrator tools, while others are specialized devious programs designed for intrusion or disruption. Network analysis is the process of understanding networking and exploiting information normally available in TCP/IP traffic for threat intentions.

IATT-Illuminate consists of at least one properly configured laptop computer. This laptop is designed to be portable for remote or range based field-testing. More than one laptop may be used together to provide a more extensive attack scenario capability.

Each laptop is configured with two operating systems: a base Windows 2000 OS with Red Hat Linux 7.1 running inside virtual machine software, VMWare. The configuration also includes a number of COTS products: Macromedia Flash MX, Cold Fusion MX, Communication Server MX, and Microsoft Access.

A new fully configured laptop costs about ~\$5K for hardware, software, and configuration labor. Periodic updates for new threats are usually delivered via CD-ROM. More extensive updates require depot style upgrade on a per laptop basis.

#### **Tools**

IATT-Illuminate tools fall into two categories: Free information exploitation, and system

services. Free information exploitation is the sampling of normal network traffic and organizing the data for operator analysis. Systems services are capabilities built into the tool to facilitate efficient and effective mixes and sequences of attacks.

## **Current Capabilities**

The IATT-Illuminate suite of threats and tools were selected to cover operations in all phases of attacks on realistic computer networks. These phases are:

- Information Gathering or Network Mapping – Gaining sufficient information about the target network to effectively identify appropriate targets of opportunity
- System Scanning or Vulnerability Identification – Gaining additional information about a target to select appropriate attacks. Includes operating system determination and port discovery
- Remote Access
- Infiltration – Gain access to the system covertly through a vulnerable service or access point
- Privilege Escalation – Once access is achieved, attempt to raise the level of privilege to access sensitive system, network, or mission data
- Exploitation – Using acquired access to the system, conduct operations to undermine the system
- Denial of Service (DoS) – Prevent a target or group of targets from functioning or accessing the network appropriately. DoS, often used as a default type of attack if other exploitation efforts are ineffective or compromised.

## ACRONYMS AND ABBREVIATIONS

A	-- Ampere
AC	-- Alternating Current
AI/EWTS	-- See MCSTF
AM	-- Amplitude Modulation
Ant	-- Antenna
AR	-- Army Regulation
ASCII	-- American Standard Code for Information Interchange
AV	-- AUTOVON
Az	-- Azimuth
baud	-- 1 Bit Per Second
BPSK	-- Binary Phase Shift Keying
bw	-- Bandwidth
C <sup>3</sup>	-- Command, Control, and Communications
CCD	-- Charge Coupled Device
CE	-- Communications-Electronics
CEP	-- Concept Evaluation Program; Circular Error of Probability
CG	-- Commanding General
ch	-- Channel
CONUS	-- Continental United States
cplr	-- Coupler
CRT	-- Cathode Ray Tube
CUCV	-- Commercial Utility Cargo Vehicle
CW	-- Continuous Wave
DA	-- Department of the Army
dB	-- Decibel
dBc	-- Decibel Relative to the Carrier
dBi	-- Decibel Relative to an Isotropic Radiator
dBm	-- Decibel Relative to a Milliwatt
DC	-- Direct Current
DEC	-- Digital Equipment Corporation (Company Name)
DF	-- Direction Finding
DOD	-- Department of Defense
DSB	-- Double-Sideband
DSBSC	-- Double-Sideband Suppressed Carrier
ECM	-- Electronic Countermeasures
EI	-- Elevation
EM	-- Electromagnetic
ERP	-- Effective Radiated Power
ESM	-- Electronic Support Measures
EW	-- Electronic Warfare
EWMF	-- Electronic Warfare Monitoring Facility

E-0	-- Electro-Optics
FDM	-- Frequency-Division Multiplexing
FIM	-- Field Intensity Measurement
FM	-- Frequency Modulation
FORSCOM	-- Forces Command
freq	-- Frequency
FSK	-- Frequency Shift Keying
GHz	-- Gigahertz
GPS	-- Global Positioning System
HF	-- High Frequency
HP	-- Hewlett-Packard
HPIB	-- Hewlett-Packard Interface Bus
HSDRS	-- High Speed Data Recording System
hr	-- Hour
Hz	-- Hertz
IEEE	-- Institute of Electrical and Electronics Engineers
IEW	-- Intelligence/Electronic Warfare
IEWTD	-- Intelligence Electronic Warfare Test Directorate
IF	-- Intermediate Frequency
ips	-- Inches Per Second
IR	-- Infrared
IRIG-B	-- Inter-Range Instrumentation Group - Format B
ISB	-- Independent Sideband
ISBSC	-- Independent-Sideband Suppressed Carrier
J/S	-- Jammer-to-Signal
kb	-- Kilobyte
kHz	-- Kilohertz
km	-- Kilometer
kW	-- Kilowatt
LAN	-- Local Area Network
lbs	-- Pounds
LHC	-- Left Hand Circular
LOB	-- Line of Bearing
LOS	-- Line of Sight
LPA	-- Log Periodic Antenna
LPI	-- Low Probability Intercept
LSB	-- Lower Sideband
LWIR	-- Long Wavelength Infrared
MAA	-- Mission Area Analysis
MACOM	-- Major Command
MANPRINT	-- Manpower and Personnel Integration
max	-- Maximum
Mb	-- Megabyte
Mbps	-- Megabits Per Second

MCSTF	-- Mobile Communications Simulator Threat Facility
MCW	-- Modulated Continuous Wave
mHz	-- Milihertz
MHz	-- Megahertz
Min	-- Minimum
mm	-- Milimeter
mod	-- Modulation
Ms	-- Millisecond
mv	-- Milivolt
mw--	Miliwatt
NRZ	-- Non-Return to Zero
ns	-- Nanosecond
OCONUS	-- Outside the Continental United States
OOK	-- On-Off Keying
OTC	-- Operational Test Command
OTCC	-- Operational Test Control Center
OTP	-- Outline Test Plan
PCM	-- Pulse-Code Modulation
PM	-- Pulse Modulation
POC	-- Point of Contact
PPM	-- Parts Per Million
PPM	-- Pulse Position Modulation
PRI	-- Pulse Repetition Interval
ps	-- Pico second
PSK	-- Pulse Shift Keying
PW--	Pulse Width
QPSK	-- Quaternary Phase Shift Keying
RAM	-- Random Access Memory
rcvr	-- Receiver
RF	-- Radio Frequency
RHC	-- Right Hand Circular
RMG	-- Remote Message Generator
rms	-- Root Mean Square
rpm	-- Revolutions Per Minute
RV	-- Recreational Vehicle
s,m,h	-- Second, Minute, or Hour
SCSI	-- Small Computer System Interface
SIGINT	-- U.S. Signals Intelligence
SMV	-- Signal Monitoring Vehicle
SSB	-- Single Sideband
SSBSC	-- Single Sideband Suppressed Carrier
Sys	-- System
S/N	-- Signal-to-Noise

TCS	-- Transportable Communications Simulator
TRADOC	-- Training and Doctrine Command
TTL	-- Transistor-to-Transistor Logic
TWTA	-- Traveling Wave Tube Amplifier
UHF	-- Ultra High Frequency
μs	-- Microsecond
USAEPG	-- U.S. Army Electronic Proving Ground
USAISC	-- U.S. Army Information Systems Command
USB	-- Upper Sideband
UV	-- Ultraviolet
V	-- Volt
VCR	-- Video Cassette Recorder
VHF	-- Very High Frequency
VMT-A	-- Vulnerability Mobile Transmitter A
VMT-B	-- Vulnerability Mobile Transmitter B
VMT-C	-- Vulnerability Mobile Transmitter C
VSB	-- Vestigial Sideband
VSWR	-- Voltage Standing Wave Ratio
W, w	-- Watt
WJ	--Watkins-Johnson (company name)