Kestrel TSCM ® Professional Software

"Tap Capture Plot (TCP) ™ | The Importance of Power Line (PL) Energy Heat Mapping—Part II

June 2020 | Issue 60

Technical Research and Standards Group

Paul D Turner, TSS TSI

Understanding Power Line (PL) Analytics—Part II

The ambient electrical power grid is certainly a major threat, however, it is not the only threat when it comes to the use of technologies that are little more than unintentional radiators that can essentially communicate across any conductive surface from metallic tape, telephone and network wiring, a variety of common facility infrastructure (both existing and provided by the attacker), altered, manipulated, or modified for the express purpose of compromising critical informational intelligence.

The use of PL technology is widely utilized in aircraft, fly be wire systems and sub-systems, and has been for many years, however, the use of PL technology for computer control, system wide communication and signalling has been advancing exponentially during the past number of years and will continue to become even more complex in the years to come.

Aircraft, ships and vehicles of all descriptions, currently, utilize a wide range of multiplexed signals on common wiring (and fiber-optic networks) for bi-directional communications to and from sensors, for status monitoring and to achieve direct command and control capability of systems and sub-systems, computers and modules.

The compromise of which, can have consequences well beyond the confines of an informational technical intelligence attack.

Generational Power Line (PL) Analytics

The first step in undertaking a formal | TCP ™ | baseline capture and analytical review of the ambient electrical power grid requires that the technical operator determine the | Operator Defined Target Area (ODTA) ™ | and identify the | Functional Target Area (FTA) ™ | of the facility as defined by the TSB 2000 (Technical) Standard ™. It is important to understand that new technology requires new terminology!

Remember, in a Moving Target Threat Model the Technical Operator is the Spectrum Analyzer...

The | ODTA ™ | is essentially the critical infrastructure associated with the facility, and the | FTA ™ | is the immediate and sometimes at a distance area, outside and adjacent to, above and below the target area.

Once understood, the technical operator can determine the best deployment strategy.

It is essential to work in a logical and systematic pattern to ensure that all, or as many appearance points that can be reasonably accessed, are tested and analytically reviewed with direct reference to the established | Functional Target Area (FTA) ™ | within the given time-on-target available.

There is no issue in selective deployment over a period of time to capture baseline data across a large facility, as there will never be enough time-on-target to complete extremely large areas of critical infrastructure on every deployment.

Probability of Detection (POD) is significantly enhanced when more than a single inspection is conducted, and one-off inspections have a very low probability that any given compromise will in fact be identified.

Essentially, as the technical operator increases the time-on-target over a period of time, the POD by the numbers increases significantly, based on the time-of-target over a longer period of time.

The technical operator can setup a Kestrel TSCM ® Professional Software | Signals Intelligence Support System (SISS) ™ project utilizing a Signal Hound BB60C Spectrum Analyzer and RF Recorder (recommended) and utilize the Kestrel 3D Energy Probe (3DEP-10) to extract signal level intelligence from each appearance point.

The | 3DEP-10 | is a CAT II (Maximum 250 volts) Power Line (PL) resource designed to safely remove the high-voltage component and allow regulated (unfiltered) RF to safely pass to the front end of most SDR hardware options.

The entire system can be deployed on a tablet computer, such as the | Kestrel Tactical Geo-Location Workstation (TGW) ™ | for portability, or a larger laptop computer that can be deployed on a mobile equipment cart workstation and conveniently moved from location to location.

Kestrel TSCM ® Professional Software

Tap Capture Plot (TCP) ™ | Power Line (PL) Geo-Location Heat Mapping | The Future of TSCM—Today!

Professional Development TSCM Group Inc. **Technical Security Branch (TSB)**

The entire process can be completed in a matter of minutes at the room level.

Once the hardware is setup and the project initiated, the technical operator can define the parameters of the project.

There are any number of considerations in selecting the capture bandwidth, however, it is strongly recommended that the technical operator establish a capture range from 9 kHz to 30 MHz as a standard baseline consideration, unless there is are compelling reasons to extend the deployment range to 150 MHz or even greater.

Extended baseline and analytical ranges can and should be completed over a period of time, however, the vast majority of technology threats will be entirely at the bottom end of the spectrum in the Power Line Carrier (PLC) range below 750 kHz or will be present below 30 MHz and extend beyond 150 MHz for Broadband Power Line (BPL) technology.

Should a potential threat be observed between 3 MHz and 30 MHz, the technical operator should immediately conduct a further investigation between 30 MHz and 150 MHz, as well as filtering down to a dedicated Range of Interest (ROI) to include a 9 kHz to 3 MHz.

The entire exercise of establishing a geo-location heat map reference baseline is to identify unusually high or unusual energy patterns on a particular electrical phase or at the appearance point level.

The operator need only capture about 250 traces (or less) for each appearance point tested, which can be accomplished in a few seconds across the recommend spectrum.

Band vs Resolution Bandwidth vs Time | 250 Traces			
Start (Frequency)	**Stop (Frequency)**	**Resolution Bandwidth (RBW)**	**Capture Time (Sec)**
9 kHz	3 MHz	1.2 kHz	2.573 Sec
9 kHz	**30 MHz**	**1.2 kHz**	**5.128 Sec**
30 MHz	150 MHz	1.2 kHz	9.615 Sec
9 kHz	150 MHz	1.2 kHz	11.760 Sec
9 kHz	3000 MHz	9.9 kHz	36.956 Sec

This assumes that the threat signal is present on the appearance point under test.

Once the above parameters are decided, the | Tap Capture Plot (TCP) ™ | mode can be invoked for deployment.

The first step is to open the application and the confirm that the SDR radio is initialized and ready with a recommended 10 dB of attenuation (Signal Hound BB60C) to avoid accidently overloading the radio front end.

The | 3DEP-10 | provides a minimum of 20 dB of attenuation.

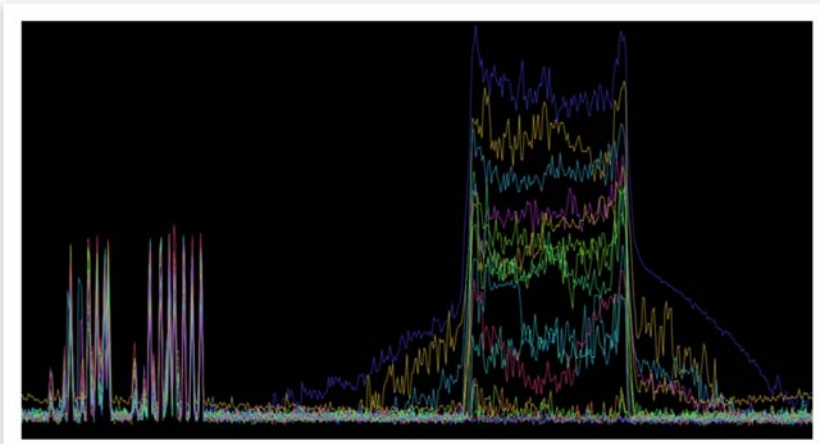
Part III of this advanced technical briefing will appear in the July 2020 edition of TSCM | SIGINT Newsletter...

Innovation is Simply the Beginning!

Visionary Software Beyond the Technology Limitations...

| www.pdtg.ca | www.kestreltscm.com | www.ctsc-canada.com |

| Paul D Turner, TSS TSI | pdturner@pdtg.ca
| Andrzej Wolczanski, TSS | awolczanski@pdtg.ca
| Gabriele Conflitti, TSS | gconflitti@pdtg.ca
| Carol Fairbrother | cfairbrother@pdtg.ca



They say that the value of art is in the eye of the beholder! Every day a new never before seen artistic spectrum is developed within the Kestrel TSCM ® Professional Software somewhere in the world. Whether impressionist, contemporary or abstract, the RF spectrum brings a commonly understood meaning for every professional technical operator who views it...

Kestrel TSCM ® Professional Software is innovative industry leading, disruptive technology, sold in 45 countries worldwide.