POWER LINE ANALYTICS

Paul D Turner *explores deployment strategies for PLC and BPL baseline monitoring and use of near real-time captured spectrum data as a powerful reference tool for comparative analysis*

Powerful defensive counter-espionage Software Defined Radio (SDR) technology has paved the way for a new analytical power line methodology.

The analytical process has decidedly shifted from the uncertainty of conducting individual appearance point reviews to a definitive algorithmic power line geo-location focused heat mapping process for the first time in history.

This new methodology involves quickly capturing the power line energy across the Operator Defined Target Area (ODTA) and the extended Functional Target Area (FTA), by testing all, or as many electrical appearance points as possible, resulting in a real-time TSCM heat map focused analysis process.

The process begins by importing a static floor plan image of the ODTA and loading a default or operator defined Power Line (PL) spectrum profile that can be based on a unique set of mission critical requirements.

An analytical heat map visualisation is a new methodology that immediately identifies potential electrical appearance points that require further focus.

The process is accomplished by deploying an innovative algorithmic energy comparative capture process across a comprehensive heat map visualisation that clearly identifies appearance point and associated electrical-phase energy patterns essential to the TSCM role.

The first step in undertaking a formal baseline capture and analytical review of the ambient electrical power grid requires that the technical operator first review and understand the facility electrical distribution and power line engineering plan.

There will always be preliminary work that needs to be accomplished, including the building of a simple block diagram from the utility demarcation to distribution panels and the end-user electrical appearance points.

It is essential to clearly understand the electrical distribution for all identified critical infrastructure that is subject to technical security inspection protocols, including those that may have been added by the threat actor.

The next step is to determine the actual Operator Defined Target Area (ODTA) and identify the extended Functional Target Area (FTA) often beyond the facility, where accessible electrical appearance points are present outside of the facility.

Electrical appearance points located outside of the facility are highly vulnerable to compromise and it is essential that all external appearance points be identified and carefully examined for signs of tampering.

Exterior appearance points include electrical outlets or easily accessible junction, terminations or distribution boxes for lighting or sign boards.

The ODTA is the critical infrastructure within the facility and the FTA is the immediate and sometimes at a distance area, outside, adjacent to, above and below the ODTA that shares a common electrical distribution profile.

It is essential that the operator work in a focused and logical grid pattern to ensure that all of the available electrical appearance points that can be reasonably and safely accessed are analytically reviewed with direct reference to the established baseline data, within the bounds of the time-on-target available.

It is not necessary to inspect every appearance point given the phase relationship between various aspects of the distribution grid, however, it is essential that the operator remember that the attacker may compromise electrical appearance points that are difficult to access or locate to minimise detection during a technical inspection.

Failure to conduct a competent inspection can result in a technical compromise remaining undetected.

One of the primary reasons often cited for not conducting power line inspections is the amount of time-on-target available. There is no issue with selective deployment over a period of time to capture progressive baseline data across a large facility. There will never be enough time-on-target to complete every aspect of the inspection process for extremely large areas of critical infrastructure during each and every deployment. The Probability of Detection (POD) is significantly enhanced when more than a single TSCM inspection is conducted for any aspect of the inspection.

Infrequent inspections have a very low probability that any given technical compromise will be identified due to the complex power line spectrum, uniquely consisting of significant masking noise artifacts.

When the technical operator increases the time-on-target, the POD by the numbers increases exponentially, based on the amount of reference data available for analysis.

There are four components required to undertake TSCM focused power line inspections: SDR hardware that extends down to 9kHz (or below); TSCM-specific software with enhanced analytical power line profiles; support for advanced algorithmic geo-location heat mapping; and a non-conductor switching common-mode power line energy probe.

The power line energy probe provides a safe connection between the radio and power line, and is used to extract signal level intelligence from each tested appearance point.

The system can be deployed on a walk-about tablet computer, for portability, or a laptop computer deployed on a mobile equipment cart and moved from location to location.

In this deployment mode, inspections provide unlimited comparative reference data-sets across multiple inspection dates and times that can identify developing trends and vulnerabilities that are not likely to be otherwise identified.

When a threat is observed below 30MHz, the technical operator should immediately conduct a further profile-based analysis to at least 150MHz

On another level, continuous power line monitoring can be deployed across a single phase or multiple electrical phases on an RF switch array utilising a single SDR radio.

Alternately, each phase can be monitored on dedicated power line energy probes and separate radios on a 365/24/7 basis at higher security levels.

The geo-location heat mapping process can be utilised to complete relatively large areas in a matter of minutes and identify suspicious energy levels and invoke a focused operator alert the same way the Over-the-Air (OTA) RF spectrum is displayed with autonomous network (email), and geo-location heat mapping alert focus.

ANALYTICAL HEAT MAP VISUALISATION IDENTIFIES ELECTRICAL POINTS THAT REQUIRE FURTHER FOCUS

There are any number of strategies and considerations in selecting the capture bandwidth, however, it is strongly recommended that the technical operator establish a capture range from 9kHz to 3MHz and 3MHz to 30MHz as a standard baseline, and extend the deployment range to from 9kHz to 150MHz or even greater when time-on-target permits.

Extended analytical ranges should be implemented randomly over a period of time; however, the vast majority of technology threats will be at the bottom end of the spectrum in the Power Line Carrier (PLC) range below 750kHz or will be present below 150MHz for Broadband Power Line (BPL) technology.

When a potential threat is observed below 30MHz, the technical operator should immediately conduct a further profile-based analysis to at least 150MHz.

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 in some cases, relative to a particular appearance point.

The technical operator need only capture on average 250 traces (or less) for each electrical appearance point evaluated, which can be accomplished in just a few seconds across the recommend spectrum.

The Band vs Resolution Bandwidth vs Time chart (overleaf) references typical capture time and bandwidth at the recommended resolution bandwidth based on an average of 250 traces utilising a high-speed radio.

Once the parameters are decided by the technical operator, the collection process can be invoked. The first step is to run the SDR application and then confirm that the radio is initialised with 10dB of hardware attenuation to avoid potentially overloading the radio front end.

There is considerable noise artifacts associated with the electrical power grid, and attenuation is an essential component in removing noise, without signal level filtering. The power line energy probe can be connected to the radio and set to a minimum of 20dB attenuation, to better regulate the RF output to the SDR radio, for the same reason. 10dB of SDR hardware attenuation and 20dB of energy probe attenuation provides excellent clarity across the energy spectrum.

Band vs Resolution Bandwidth vs Time | 250 Traces			
Start Frequency	**Stop Frequency**	**Resolution Bandwidth (RBW)**	**Capture Time (Sec)**
9kHz	3MHz	1.2kHz	2.562 Sec
9kHz	30MHz	1.2kHz	3.824 Sec
9kHz	150MHz	1.2kHz	10.592 Sec
9kHz	250MHz	1.2kHz	16.167 Sec
9kHz	1.5GHz	4.9kHz	28.338 Sec
9kHz	3GHz	9.9kHz	36.699 Sec

The heat mapping and display of all energy source levels is based on the physical location of each electrical appearance point based on an algorithmic propagation model, and displays a direct comparative reference of the energy levels across all evaluated appearance points and relative electrical phases.

The resulting geo-location heat map will identify Power Line appearance points that exhibit elevated energy levels that provide a narrow focus starting point of any anomalies that will need to be investigated further by the operator to determine the actual reason for the elevated energy levels.

Determining the relationship between elevated energy appearance points in comparison to all the other appearance points will help determine whether the presence of a Technical Surveillance Device (TSD) is indicated.

Elevated energy levels may be the result of a client-authorised (or unauthorised) friendly device, an unintentional radiator or electrical noise from office and industrial equipment may be the cause of the elevated energy levels.

It is not unusual for electrically connected equipment within the target area to directly impact the detected energy levels associated with shared electrical phases.

Obviously, the technical operator will complete a baseline collection for all appearance points in the surrounding area and expand the analysis process with focus on the electrical appearance points that exhibit unusually high, or observed changes over time, of detected energy levels.

Power Line geo-location heat mapping is a modern industry disruptive technique that brings a new standards-based capability that's consistent with a modern moving target threat model as defined by the TSB 2000 (Technical) Standard.

The ability of the modern spectrum warrior to migrate from obsolete Cold-War era techniques and embrace a powerful new methodology that is consistent with an array of modern threat technology is an essential best practice ●

Paul D Turner, TSS TSI is the President/ CEO of Professional Development TSCM Group Inc. and is a certified Technical Security Specialist (TSS) and Technical Security Instructor (TSI) with 40 years' experience in providing advanced certification training, delivery of TSCM services worldwide, developer of the Kestrel TSCM Professional Software and manages the Canadian Technical Security Conference (CTSC) under the operational umbrella of the TSB 2000 (Technical) Standard.

It is vital to identify accessible electrical points often located beyond the facility

Picture credit: Crown Copyright