Kestrel TSCM ® Professional Software

The Importance of TSCM Software Feature Integration

April 2018 | Issue 34

Technical Research and Standards Group (TRSG)

Paul D Turner, TSS TSI

Software Integration and Operability Defined

One of the key deployment advantages of the Kestrel TSCM ® Professional Software, is the ability to utilize a common user-interface, across all available shared features, functionality, and optional software modules.

This concept is a powerful technological achievement deep within the software, and is a fundamental design element founded on an entirely modernized moving target threat model, and sets a powerful new standard in deployment methodology, with the goal of advancing real-world Probability of Detection (POD).

As noted in the March 2018 newsletter.

"Defensive countermeasures must be applied in an obscure and random layered approach to have any hope of minimizing or defeating, technical vulnerabilities and compromises, within a defined high-threat environment".

The TSCM program, in practice must be implemented as a heuristic countermeasure, much like the advanced application of an anti-virus software, otherwise, the Probability of Intercept (POI) and the Probability of Detection (POD), will suffer significantly, placing the end-user entity at risk of an undetected vulnerability.

Technologically obsolete spectrum analyzers set in motion the "failure to identify" aspect these types of advanced persistent threat technologies, by inherent design limitations, and a poor deployment methodology.

The "what you see is what you get" spectrum display, can no longer adequately be relied upon to identify many of the modern day, hostile threat technologies.

When the software integrates, automates, and outputs filtered analytical spectra, and other essential measurement parameters over an appropriate period of time, a true and relevant picture emerges.

The ability to see the big picture, brings clarity to otherwise fragmented and seemingly unconnected spectral events, which simply cannot provide the technical operator with a clear analytical picture.

Signal level analytics, based only on a "snap-shot" style review of the RF spectrum, provides an uncomfortably low POD, and will almost always fail to identify significant signal relationships, patterns, and RF signatures (characterization), leaving the technical operator, and often the client, with a false sense of security.

When a common capture and analytical process is by design, made possible, all available data can be captured, displayed, filtered, and analyzed in detail, across a variety of key, real-time and post capture features, providing a powerful check and balance.

For example, the ability to capture all spectral events within the ambient RF spectrum environment, over an extended deployment period, is the only current method of advancing the POD within a defined target area.

Today's, state sponsored espionage threat technology and trade-craft, means persistent, illusive, dynamically evasive, power agile, band and frequency agile, and periodic in nature, renders obsolete techniques incapable of detecting sophisticated attacks.

The ability to deploy multiple high-speed Software Defined Radio (SDR) hardware, such as the Signal Hound SM200A (100 kHz to 20 GHz), with the ability to easily sweep the full receiver bandwidth, at speeds up to 1 THz per second @ 30 kHz RBW, provides for the first time, the ability to advance the Probability of Intercept (POI), and essentially see spectrum events, you have never seen before, utilizing obsolete spectrum analyzers.

The ability to internally digitize and process 1 billion analog samples per second, is now a reality. This means that the SM200A is sweeping approximately 40 times faster than the BB60C (at 24 GHz per second), and approximately 7000 times faster that the considerably slower Signal Hound SA44B (sweeping at 150 MHz per second).

Kestrel TSCM ® Professional Software

"Kestrel ® TSCM | Multi-Tasking By Design"

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

As defined by the TSB2000 (Technical) Standard ™, the 698 MHz to 2700 MHz (ROI) must be capture isolated at 20 kHz to 30 kHz RBW, during medium, medium elevated, high, and high elevated threat level deployment. This slightly larger than 2 GHz span, covers the vast majority of wireless technologies, and with the release of the Signal Hound SM200A Spectrum Monitoring Receiver, can be swept in under 2 mSec @ 30 kHz RBW.

This capability can be rationalized as 2 GHz of sweep bandwidth @ 30 kHz RBW, resulting in a 2 mSec sweep time, or 1 THz per second, or 7000 times faster than the SA44B and SA124B receivers, that are still in wide use for TSCM applications. The SM200A can provide a 100 percent Probability of Intercept (POI) based on the current threat reality, for a 2 GHz span @ 30 kHz RBW, resulting in a sweep speed of approximately 2 mSec.

Just as the SDR hardware is an essential operational component, the ability to apply powerful software defined capture, store and review, filter and display, and other powerful analytical display features, is essential.

You cannot analyze critical spectrum data, which you have not captured and have not written to storage for post analytical review.

This is where the Kestrel TSCM ® Professional Software takes the hardware to an entirely new level of functionality, by capturing, storing, processing, and displaying spectra in a meaningful way, that enhances technical operator situational awareness and permits operator interaction. The technical operator must be engaged, by the software capability, and not frustrated by its limitations.

A true multi-tasking, mission specific SDR application, provides the technical operator with deployment options, that allow operator assisted and unattended operation, across single or multiple locations and SDR hardware. It is essential that all of the software features provide interoperability with a common user-interface.

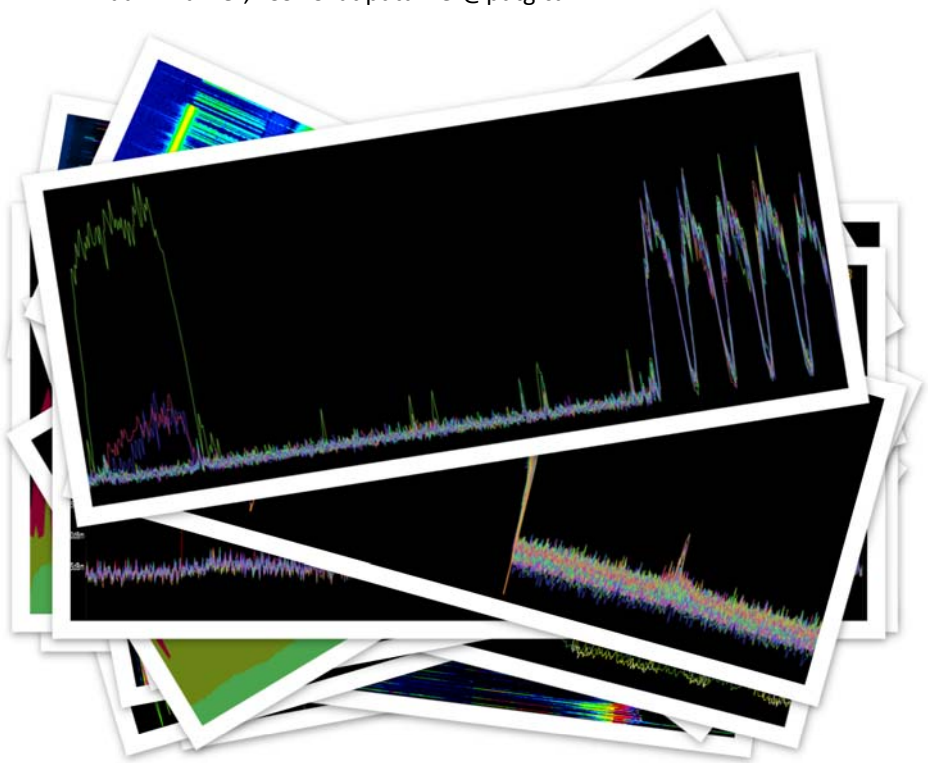
Host Computer | Updates

It is essential that technical operators spend some quality time on a regular basis to ensure that the host computer Operating System (OS), USB 3.0 drivers, network drivers, graphics drivers, installed applications, and the Kestrel TSCM ® Professional Software, are all up to date, and ready for trouble free deployment.

Whether working on an open system, or classified platform, it is necessary to define and implement a core strategy for an effective and efficient updating process, that meets the operational requirements of the technical operator. Online, or off-line, the host computer update process must be accomplished.

PDTG Inc., has developed a best practice solution for off-line platforms, that need be updated prior to deployment, or after recovery from deployment, in potentially hostile environments.

To learn more about, "what you don't know, contact the Technical Research and Standards Group (TRSG), at Professional Development TSCM Group Inc. | www.pdtg.ca | www.kestreltscm.com | or Paul D Turner, TSS TSI at pdturner@pdtg.ca



Kestrel TSCM ® Professional Software is innovative industry leading, disruptive technology, sold in 30 countries worldwide.