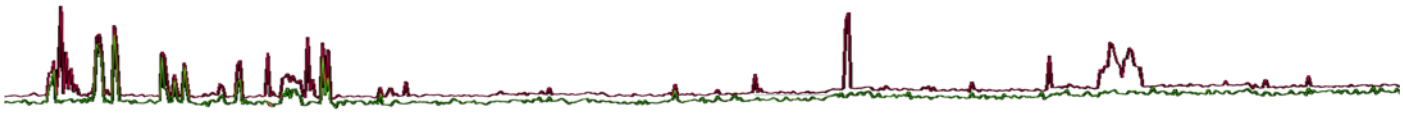




# The Art and Science of Remote Spectrum Surveillance and Monitoring (RSSM) ™

Technical Security Branch (TSB) | Technical Research and Standards Group (TRSG) | Software Development Group (SDG)

**Paul D Turner, TSS TSI**

**Professional Development TSCM Group Inc.**

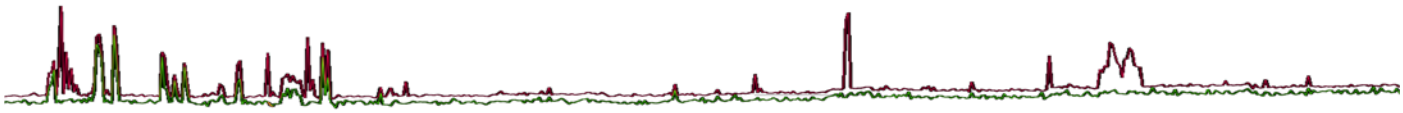
This whitepaper delineates the tactical advantages, key benefits, new detection methodology, system architecture considerations, administrative maintenance requirements, technical analysis capabilities, across various TSCM professional service delivery levels, and the requirements for a deployable, working Remote Spectrum Surveillance and Monitoring (RSSM) ™ system, as defined under the TSB 2000 (Technical) Standard ™, utilizing the Signal Hound (BB60C) Spectrum Analyzer and RF Recorder operating from 9 kHz to 6 GHz at a search speed of 250 mSec at 10 kHz RBW and the Signal Hound (SM200A) Spectrum Monitoring Receiver operating from 100 kHz to 20 GHz at a search speed of 1 THz at 30 kHz RBW.

The importance of managed Remote Spectrum Surveillance and Monitoring (RSSM) ™ often referred to as in-place monitoring in some circles, cannot be minimized in today's complex moving target threat model, when faced with a Probability of Detection (POD) at an all-time low, by means of a traditional TSCM, Radio Frequency (RF), spectrum analysis perspective.

Whether the deployment application is TSCM oriented, Search and Rescue (SAR), regulatory spectrum monitoring, telecommunications verification, counter-espionage, national security, counter-terrorism, legal intercept, tactical intervention, or in support of high-risk protective operations and protective intelligence, all of these demanding applications share the same challenging and complex RF signal environment.

The home land security, and the national security apparatus, public and private sector alike, are oftentimes faced with challenges well beyond most of the "limited capability", commercially available applications (or those of a foreign origin); and specialized resources and tools are required when operating at elevated threat levels, to ensure uninterrupted collection is maintained, and routine maintenance and automatic fail-safe recovery is possible when hardware, computer Operating Systems (OS), or even the specialized application software stops communicating, as intended.

It is not a question of reliability of hardware or software, as much as it simply inevitable given the complexity of modern-day Software Defined Radio (SDR) collection and analysis systems, and the exacting demands of the unique deployment requirements of the end-user, oftentimes deployed within challenging hostile environments.



Remote Spectrum Surveillance and Monitoring (RSSM) ™ as defined under the TSB 2000 (Technical) Standard ™, places reliance on a number of redundancies that are designed to assist in system health monitoring, network connectivity fail-over, remote network reboot capability, remote system integrity validation, and automatic application recovery, to get the system not only back on-line, but return to a data collection state, with only limited operator intervention.

A very powerful example of this concept, is the Autonomous Measurement and Collection Sub-System (AMCS) ™ capability within the Kestrel TSCM ® Professional Software, providing all of the above across a TCP/IP network utilizing but TCP/IP and file reporters.

The Signal Hound ™ family of hardware products, supported by the powerful Spike ™ software have a proven track record for reliability, within the mandate of the highest levels of technical security deployment and the (SM200A) is the next generation of SDR hardware, within the private and public sector, including corporate counter-espionage teams, government, military, and national security apparatus worldwide.

The Kestrel TSCM ® Professional Software, is available as an optional third-party, TSCM specific, and Remote Surveillance and Monitoring (RSSM) ™ ready software, providing unsurpassed, long-term deployment reliability, within a demanding spectrum monitoring role, with a strong focus on the technical operator's requirements.

The Signal Hound ™ (BB60C) Spectrum Analyzer and RF Recorder, has been the most significant disruptive technology to enter the public and private sector TSCM market since early 2009, and has forced the competition to either enter the game, or at least, attempt to change their respective business models to compete at some level, with various degrees of success.

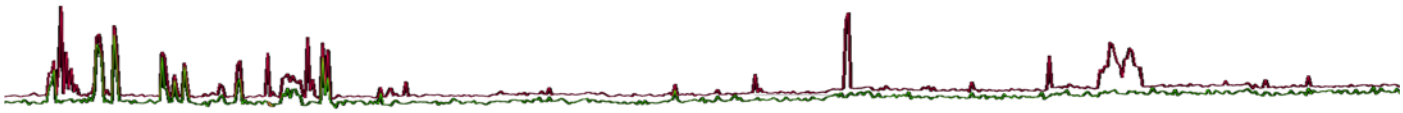
The industry has predictably taken the wrong approach and has reacted negatively towards new business threatening SDR technology, ideas, concepts, and methodology associated with a modern moving target threat model.

The next generation of Signal Hound ™ receivers, such as the (SM200A) once again will bring industry leading disruptive technology to a somewhat technically complacent competitive market.

There are many aspects that must be considered and evaluated when determining the best implementation and setup for any particular TSCM deployment, however, the two (2) most important aspects are the SDR hardware (radio) and the specialized software, which typically, does all the heavy lifting at the end of the day and is built on real-world practitioner experience.

This whitepaper focuses on the deployment of the Signal Hound ™ (BB60C) and the (SM200A) hardware, which have, and will, continue to change the spectrum monitoring landscape for years to come.

There are other SDR hardware products supported by the Kestrel TSCM ® Professional Software that provide the end-user with a range of deployment specific and unique hardware options that may better meet individual or anticipated deployment requirements.



The Kestrel TSCM ® Professional Software is designed on an entirely new deployment standard that permits traditional operator assisted RF based Technical Surveillance Countermeasures (TSCM) inspections to be conducted and defines a new moving target threat model methodology and protocol, specific to the operational deployment of the Kestrel TSCM ® Professional Software, referred to as Remote Spectrum Surveillance and Monitoring (RSSM) ™ under the Kestrel ® umbrella brand, fast becoming the new due-diligence minimum standard.

## Autonomous Measurement Collection System (AMCS) ™

Advanced features such as the Autonomous Measurement Collection System (AMCS) ™, powered by a TCP/IP Socket and Sub-System architecture, deep within the Kestrel TSCM ® Professional Software application, allows the software to operate “headless” in an embedded computing environment, bringing with it, significant operational advantages and reporting options.

Our SDK includes an open source API and remote client example for the first time allowing powerful third-party development of custom solutions.

AMCS ™ is perhaps described as one of the most powerful features ever developed for professional deployment requirements and is configured with a powerful user-defined Kestrel Configuration Script (KCS) ™ file located within the applications installation directory.

The Kestrel ® application creates the project file structure and necessary configuration to be able to immediately begin runtime collection activity when the application is started.

Client applications may be connected to the Kestrel ® software via a TCP/IP socket interface connection, to obtain the extracted data stream and basic configuration information from the Kestrel ® application.

A measure of limited control is also offered to client-side applications.

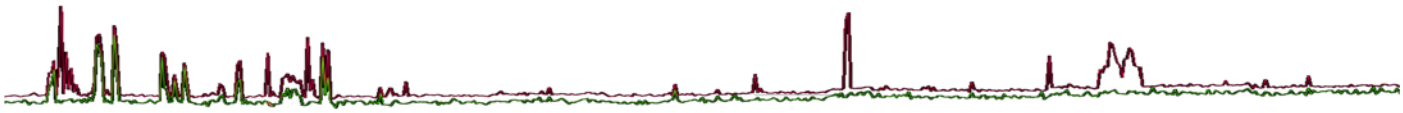
AMCS ™ comprises of a powerful sub-system within the Kestrel ® application, and this sub-system is enabled when Kestrel ® is started with a valid Activation Security Key (ASK) ™ that contains the AMCS ™ capability, referred to as OPT AMCS ™.

On initial connection of a supported receiver to Kestrel ®, a license key request will be generated in the form of a Challenge and Response (CRC) ™ code string and presented to the technical operator.

When the CRC code is provided to the Technical Support Group (TSG) of Professional Development TSCM Group Inc., this will be converted into an Activation Security Key (ASK) ™ license, enabling the AMCS ™ capability on the target platform.

This Activation Security Key (ASK) ™ may then be installed into Kestrel ®, enabling that instance of Kestrel ® on that machine and receiver to operate with the AMCS ™ capability enabled.

Only one (1) supported SDR receiver on a subject platform requires an Activation Security Key (ASK) ™ to enable AMCS ™ operation across all SDR hardware operating with that instance of the Kestrel TSCM ® Professional Software.



The AMCS ™ sub-system allows Kestrel ® to be operated in a stand-alone fashion, or hybrid capability, rendering captured data to storage on the target platform essentially permitting both TCP/IP and FILE based reporters.

The Kestrel Configuration Script (KCS) ™ allows autonomous collection to be set up and initiated immediately on application start, without the requirement to establish multiple spectrum Ranges of Interest (ROI), bands, or sub-bands.

The script is easily edited on the fly, should additional measurements or changes to the reporters be required.

Client applications can connect to Kestrel ® and obtain a continuous data feed for the specified bands, channels, measurements and other data parameters of interest.

**Remote Spectrum Surveillance and Monitoring (RSSM) ™** | Setting up a kestrel ® instance and search receiver at a remote location, permits a continuous TCP/IP monitoring data feed, obtained from the remote location. In some cases, it might be desirable to also write to file on the target system, some or all of the data for operator defined bands or even unique bands not sent under TCP/IP streaming.

Kestrel ®, when operating in this mode is suitable for use on an embedded PC platform, providing a low cost and very powerful remote spectrum monitoring solution.

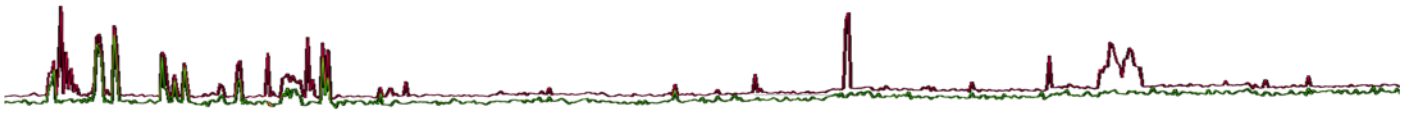
The TCP/IP stream can include full end-to-end encryption, or advantage the end-users own encryption technology and run on a proprietary network.

**Data Feed Integration** | The remote feed configuration, utilizes an open "xml" style format allowing easy integration with additional data feeds to provide a richer data stream, and offers the ability to synchronize multiple sources into a single data feed output for recovery and technical analysis in a plain-text, or encrypted format.

**Alarm and Alerting Integration** | The integration of the AMCS ™ capabilities with the unique alarm and alerting architecture found within the Kestrel TSCM ® Professional Software, provides the capability of obtaining structured RSSM ™ data, when specific events of interest occur within the ambient RF spectrum environment, thereby reducing the actual data transmission load and providing advanced "Actionable RF Intelligence" under the **Kestrel-net ™** system architecture relating to operator defined spectral measurement activity, and other operator defined parameters.

**Distributed (Managed) Remote Spectrum Surveillance and Monitoring (RSSM) ™** | Defining multiple instances of Kestrel ® within the AMCS ™ capability, and integrating, multiple independent data feeds, means powerful RSSM ™ solutions can be easily implemented at the facility level, or across national and international geographical boundaries with the inclusion of an open-source API for end-user development of remote-client applications.

**Black Box Integration** | The ability to utilize RF spectra as a sensory input to an existing "black box" system or build powerful analytical solutions can be realized when the AMCS ™ data feed is combined with other sensory inputs, including GPS data, speed, altitude, temperature, etc., with defined RF interference triggers, alarm inputs and other required data elements and parameters.



# Probability of Detection (POD)

The following professional observations were gleaned from Glenn H. Whidden's book, entitled "The Russian Eavesdropping Threat – Late 1993".

Glenn's comments and thought processes reflect times past, but also hold true in a modern moving target threat model, moving ahead a quarter century.

Glenn reveals an important observation that proves timely, against the back drop of a modern threat environment and is a concept we aggressively teach during our Technical Security Specialist (TSS) Designate Certification program, as well as our Certified Technical Operator (CTO) ™ training, and continue to actively brief our client's routinely, who often have little or no counter-espionage experience suitable for implementing a formal competent Technical Surveillance Countermeasures (TSCM) program.

The first observation from Glenn's book that echoes across various chapters, is that it does not matter how low tech a device or method of compromise may be, it will not be found, if there are no defensive countermeasures being undertaken as a routine practice.

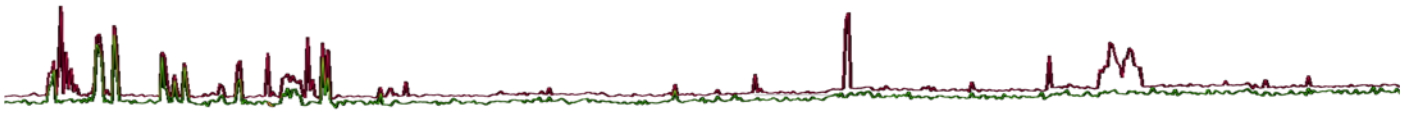
This message is as timely today in 2018 as it was leading up to 1993, and this is the core foundation of the Kestrel ® Remote Spectrum Surveillance and Monitoring (RSSM) ™ concept implemented around a modern moving target threat model as defined by the TSB 2000 (Technical) Standard ™.

It is a routine practice and concept that is essential to understand, as many operators are called to service, based on a panic contact from an end-user, who offers little time-on-target, a rush to get the job done, little or no preparation time and expectations of a 100% Probability of Detection (POD) at the end of the assignment.

All too often technical operators do nothing to inform the end-user of the technical realities resulting in lost opportunity, a false sense of security in the value afforded by the technical inspection, and significant liability for which the technical operator with suffer the consequences at the end of the day.

Very few organizations implement formal competent defensive Technical Surveillance Countermeasures (TSCM) programs pro-actively, to properly identify potential compromise, over an extended period of time.

> *"If the right person is not looking at the RF spectrum at the right time, with the right equipment resources, the mission will fail to mitigate the threat of a hostile RF compromise in the field".*
>
> *Paul D Turner, TSS TSI*



In-fact, not one of the Russian RF devices described by Glenn in his book, would not have been detected immediately, if 24 / 7 active defensive countermeasures, such as our Remote Spectrum Surveillance and Monitoring (RSSM) ™ concept was actively deployed, at the time.

The reality is, there was the lack of low cost hardware and specialized software technology at the time, which is an issue that no longer exists in today's technology rich marketplace.

However, the technical operator has to break through all the marketing hype, and the misleading concept that TSCM is a do it yourself project whether it be private or public sector.

If you are not looking at the RF spectrum 24 / 7 / 365, the Probability of Detection (POD) will be dangerously eroded well beyond the ability of a chance opportunity to detect a potentially hostile emitter and the higher the threat level, the lower the POD will likely be in a practical reality, as more sophisticated devices and methods are deployed during an attack.

Another notable observation derived from Glenn's book, is that an attacker might deploy any number of anti-detection strategies, taking defensive equipment limitations and what we now, in the present day, refer to as human factors, into account; placing a hostile device in a difficult to access or difficult to verify location that will often defeat defensive countermeasures.

There is also a sub-culture of sub-par operators that simply do not have the experience, training, or equipment to conduct an acceptable level of technical inspections and do little to achieve any level of competence, due to lack of understanding of the commitment and budget requirements over time.

You will never see them at training, conferences, or professional development opportunities as they are apparently too busy to attend.

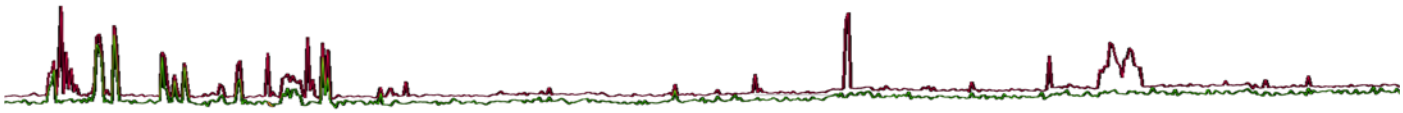
Most professional level attackers engaged in economic or state sponsored-espionage attacks are more than aware that the vast majority of organizations, pubic and private sector, do not provide adequate budgets, or "time-on-target" to be able to satisfy minimum due-diligence considerations, assuming they engage in defensive countermeasures at all!

Unfortunately, many organizations are also likely to engage sub-par operators, for many of the same reasons, including lack of knowledge, budget, etc., and buy into the marketing hype.

The less than motivated defensive operator, may rule out (in error), certain possibilities as not practical for the attacker, or the defensive operator may not be able to electronically sweep certain areas due to accessibility or other issues, for example a Non-Linear Junction Detector (NLJD) search is rendered useless in a room full of electronics, or heavy furniture may not be able to be moved easily, and other inspection tools may not reach some areas of concern.

What the operator does not now, or does not validate, becomes a serious liability and is a blue-print for failure.

The attacker has all the time needed to apply their tradecraft and the defensive operator is literally always going to be one step behind the offensive technology; the creativity and ingenuity of the attacker in real-world counter-espionage scenarios.



> *"The lesson we must all learn, is that a motivated attacker will always succeed against a less than motivated defensive operator".*
>
> *Paul D Turner, TSS TSI*

Managed RSSM [TM] deployment requires that the technical operator and ultimately the end-user, fully understand that global economic-espionage has taken a dramatic turn during the past decade, as significant changes in how corporations and governments do business, both domestically and internationally; have literally opened the flood gates of "opportunity", driven by aggressive state sponsored espionage players, engaged in everything from, economic-espionage to terrorism.

> *"Political instability globally has contributed to the advancement and success of state-sponsored economic-espionage under the banner of, where there is uncertainty and confusion, there is profit".*
>
> *Paul D Turner, TSS TSI*

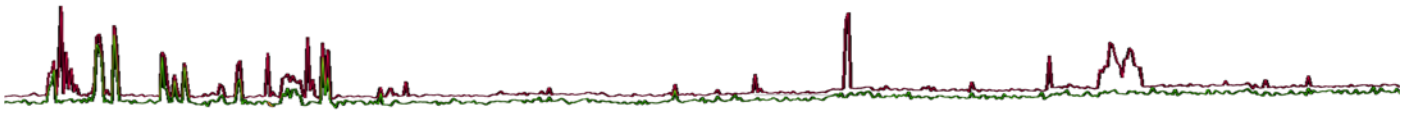
Dominating the RF spectrum environment is an essential first step in potentially identifying and addressing both of these threatening activities, which see no boundaries given the vast hostile surveillance technology available and the will and determination to utilize it.

## Modern TSCM Inspection Environment

The business work environment has also changed, with the traditional and more secure individual private office and work spaces, replaced with trendy Ad Hoc shared work spaces, significantly increasing the potential for inadvertent disclosure of proprietary information, both from an insider threat and through traditional espionage activities with virtually no controlled access to large common work areas, elevating the risk of a devastating technical compromise.

Business executives are integrating themselves into these common work areas under a so-called, open door policy, placing the organization at even greater risks of a competitive-intelligence gathering incident or a devastating economic-espionage related compromise.

These same corporate security directors and company executives would never think of turning off the company network firewall or anti-virus system at the end of the work day, but very few organizations take the threat of competitive-intelligence or economic-espionage seriously, as is evident by the randomness and periodic nature in which professional level Technical Surveillance Countermeasures (TSCM) services are requested, and ultimately delivered.



The ability of the Kestrel TSCM ® Professional Software to bring a new methodology to the technical security industry was not taken seriously by many operators, equipment manufacturers and any number of foreign origin, want-a-be competitive products that focus on the sale rather than technology.

However, moving just a few years ahead, all of the above are seen to be quietly claiming they have the capability of some sort of spectrum monitoring and are making statements derived from our core concepts, working materials, documentation and certification training.

Ironically, these foreign suppliers account for the vast majority of so-called TSCM equipment resources, and are the same countries and players involved in a very high percentage of the state-sponsored economic-espionage, and cyber security attacks worldwide.

Do you see a dangerous trend and liability concern in this growing development.

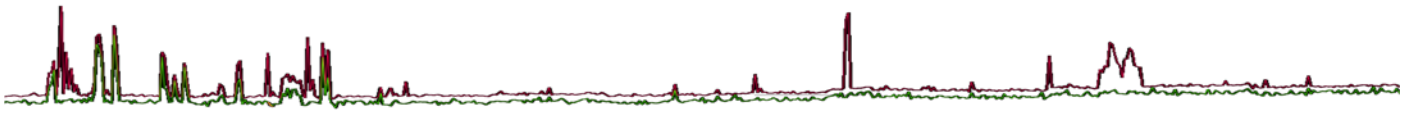
There is a serious credibility gap with the equipment supply chain, as some of the players are also engaged in selling Technical Surveillance Devices (TSD), alongside the counter-surveillance equipment resources, quietly in the background.

The reality is that it takes more than a follow-the-leader approach to bringing a new and very powerful tool such as managed Remote Spectrum Surveillance and Monitoring (RSSM) ™ to replace obsolete periodic RF spectrum analysis techniques, which are unfortunately, still being utilized by many technical operators as per the expectations and inexperience of the end-user as the only means of conducting the spectrum analysis phase of a technical inspection.

Professional Development TSCM Group Inc., is a Canadian innovator with a solid industry foundation, vast international deployment experience, and a strong technical investment in industry relevant Research and Development (R&D) and maintains a substantial financial investment in the design, engineering and development of the Kestrel TSCM ® Professional Software, for use at all known and developing threat levels, up to and including, the homeland security, and the national security apparatus, positioning Kestrel ® as an industry disruptive Canadian technology dating back to early 2009.

> *"To quote a respected Canadian government scientist, "I am amazed at how far the [Kestrel] software has progressed in just a few years. It is doubtful even the government, with a team of software engineers and several million dollars could have achieved this level of development in such a short time".*
>
> *Undisclosed Individual*

Our industry leading position as a 100% Canadian developed, source code controlled product, brings with it, a high level of integrity and credibility simply not found in any number of foreign controlled software products that may be procured internationally or marketed in Canada.



Professional Development TSCM Group Inc., recognized early on that marketing existing repackaged products or acting as a distributor of foreign controlled software was not an acceptable solution for homeland security, the national security apparatus, corporate, government, and military clients, worldwide, tasked with complex deployment requirements, given the nature and purpose of the software application and the challenges of countering economic-espionage, safe-guarding lives and enhancing national security, by the application of Signals Intelligence (SIGINT), and achieving analytically sound spectrum dominance.

With 5G technology on the horizon, spectrum domination will become an absolute necessity in the mitigation of virtually undetectable hostile technology across the radio-frequency and cyber-security domain.

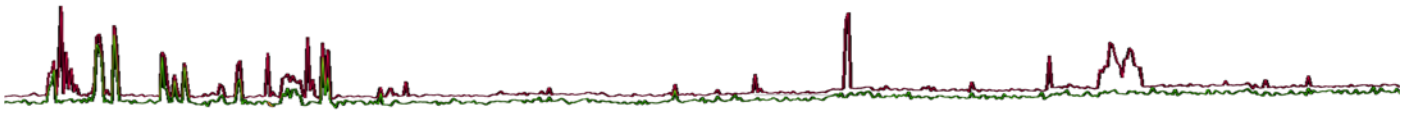
The core competitive advantage is firmly attributed to the powerful design and development methodology behind the Kestrel TSCM ® Professional Software, including an on-going product development commitment, exceeding the expectations of the professional end-user.

Signal Hound ™ SDR hardware has been a decisive factor in successfully bringing one of the most powerful SDR hardware products, and software combinations to the technical security industry for use at all known and developing threat levels at frequencies up to 50 GHz.

> *"Kestrel ® is an original, fresh approach to redefining electronic Technical Security (TSEC) at the core level and developed along the vision of future scalability and more importantly, sustainability, with witness to an expediential acceleration in threat technology and powerful advances in Software Defined Radio (SDR) hardware".*
>
> *Paul D Turner, TSS TSI*

The very nature and characteristics of modern Radio Frequency (RF) threats change on a daily basis, requiring adaptive search technology to be deployed, similar to the heuristic capability of a modern anti-virus software program to look for threats that technically have never been seen in the past, or are perhaps unfamiliar to even the seasoned technical operator by looking for certain known signal characteristics and unknown event classifications, over a period of time.

The FCC licensing database alone, currently holds more than 18 million records and hostile RF technology can easily be defined providing the attacker with virtually an infinite number of the frequency domain for use in intercepting sensitive communication and a provides significant opportunity to compromise existing communication and non-voice related radio frequency systems and sub-systems.



The real-time identification of complex signal events has taken a back seat to the implementation of long-term strategies to document and classify Signals of Interest (SOI) that may only periodically appear, and are not likely to be captured during, periodic and limited “time-on-target” inspections.

> *“The ability of the attacker to capture and store even encrypted radio communication data is also highly probable within a moving target threat model by persistent and determined state-sponsored players, holding data in storage, patiently waiting for the day the data might perhaps be possible to decrypt using accumulated intelligence and new technological tools”.*
>
> *Paul D Turner*

Such characterization might simply be to flag an unknown signal event as not fitting a known pattern of classification for the technical operator; or hand-off to an analyst to manually review, or invoke key software features, for targeted monitoring of the SOI at the signal level.

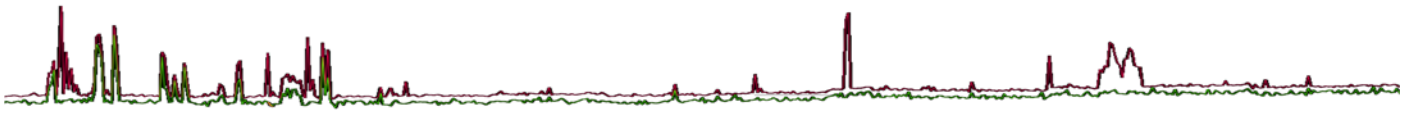
## Core Concepts | Probability of Detection (POD)

Approximately 95% of the TSCM operators surveyed are still conducting ineffective “snap-shot” style periodic Radio Frequency (RF) sweeps, believing the Probability of Detection (POD) is reasonably close to 100% (a concept often proposed by equipment manufacturers, referring to the sweep speed and other hardware factors), and operators have in-turn, convinced the end-user, this is the case, when in-fact, it is not possible without 24 / 7 / 365 capture and analysis of all spectrum data.

The ability to capture, classify, and analyze all relevant spectral data over an in determinant period of time is a fundamental core concept and requirement, given the existing new developments in threat technology emerging globally.

As a professional technical operator, there are minimum experience requirements that must be considered in order to mitigate offensive trade-craft under the banner of economic-espionage.

> *As a technical operator, it is not possible to detect, identify, or locate a threat of which you are unaware, or have no technical data to support a position on either side as to whether a compromise exists, existed, or will exist in the time-frame of an unknown future event.*
>
> *Paul D Turner, TSS TSI*



What many operators often fail to understand is that even a highly experienced and competent RF spectrum analysis conducted with the right equipment resources and the correct approach, for a period of 8 hours a month x 12 months represents only a 1% POD opportunity averaged over the course of an entire year, when not appropriately supplemented by a long-term, managed Remote Spectrum Surveillance and Monitoring (RSSM) ™ methodology.

It is all about the opportunity, to detect and identify; and this requires significant "time-on-target" which generally, is not supported by budget requirements within a traditional sweep model.

The average "time-on-target" among surveyed operators is approximately 10 hours (or less) quarterly, or 40 hours (or less) annually, yet most operators surveyed, insisted that this meets an acceptable level of due-diligence within the bounds of a competent RF inspection for most of their clients, or they stated that the end-user imposed restrictive limitations with respect to "time-on-target" primarily due to budgetary issues.

Someone will need to explain to me, just how do operators know, what they do not know and likewise, how does the end-user know, what they do not know?

My conclusion is that challenging the end-user's perception as to the nature and reality of the inspection program requirements and the application of an effective due-diligence professional service with insufficient budget and / or "time-on-target", remains unchallenged by a great many operators!

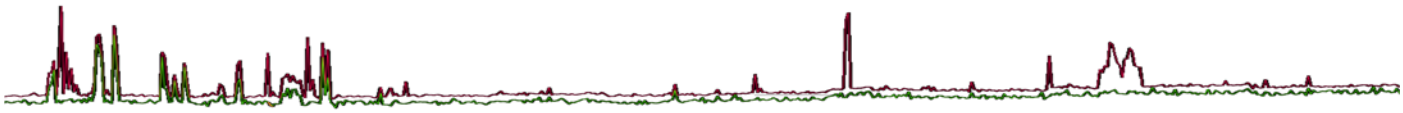
The scope of work is undertaken against the end-user's lack of experience and knowledge relating to adequately defining an acceptable level of due diligence and fails to consider the possible outcome, should a technical compromise occur.

There are very few corporations that have implemented adequate well-established Technical Security (TSEC) programs that meet an acceptable and recommended standard, or level of operational due-diligence, corporate governance, regulatory compliance, as often clearly delineated or required by corporate or business liability insurance policies.

A formal externally managed Technical Surveillance Countermeasures (TSCM) program, supplemented with in-house corporate security team involvement in managing the day to day business risks, is an essential business practice for both cyber-security risks and to adequately address technical security vulnerabilities and concerns.

When the end-user, places significant deployment restrictions on the technical operator, or the defined target area is not adequate, access control, escort limitations, time-on-target, etc., the Probability of Detection (POD) is further eroded, and the process becomes little more than a check box on some ("we did it") form for the board of directors or management.

This is not a competent inspection program at the end of the day and technical operators are encouraged to evaluate the real effectiveness of an existing approach and gently guide the business entity by making small but significant changes to the technical security program.



*The threat of economic-espionage, state sponsored espionage and competitive intelligence gathering is an invisible and insidious activity that also includes insider and employee dishonesty, or carelessness, and needs more C-Level attention than simply a best guess reluctant approach and an on-going struggle to justify, little more than a modest annual budget, compared to other corporate financial obligations and requirements at the corporate level. The reality is that economic-espionage effects all business types, and all businesses need to have a formal, scalable Technical Security (TSEC) program that is objective and free of the internal corporate culture trap.*

*Paul D Turner, TSS TSI*

Operators typically place the blame firmly on the end-users requested Scope of Work (SOW) limitations, and budget restrictions, or a restrictive bidding process, which often will specify operator resources, which are totally inadequate for the intended assignment rather than challenge the ineffectiveness of the approach or limitations of the TSCM equipment resources, or the client's strategy, program implementation standards, methods or techniques, in fear they will not get the assignment.

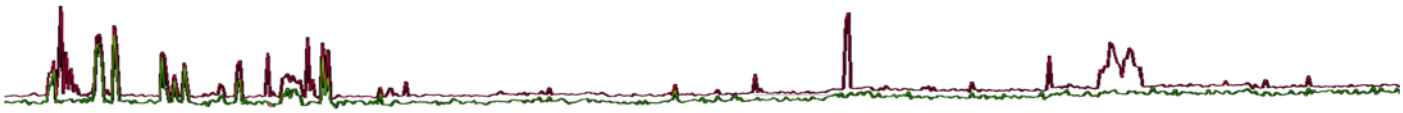
Operators need to understand the real Probability of Detection (POD) numbers, as opposed to the slick and uninformed marketing methods utilized to impress prospective client's that in some cases continue to utilize the same sub-par TSCM services, unwittingly.

When any equipment resource is deployed for, one (1) hour and the equipment resource is in-fact capable of 100% Probability of Detection (POD) and the operator has the experience to identify a hostile event from the many thousands of friendly ambient RF signals, I guess one could argue that the POD is 100%, but this is only true for the actual deployment time of in this example one (1) hour and this is where most equipment manufacturers and technical operators miss the point completely regarding the importance of Probability of Detection (POD) by the numbers.

The belief, is that such service levels or products, achieve what ultimately, are unfounded levels of Probability of Detection (POD) and therefore negatively impact the TSCM program effectiveness when POD is utilized only as a sales or marketing tool, results in providing the client with a false sense of security and instilling unrealistic program effectiveness capabilities.

It is essential that the end-user be provided with real Probability of Detection (POD) expectations as to the effectiveness of any professional services provided, and not be left with a false sense of security by the technical operator.

When the end-user and the technical operator are on the same page and the appropriate service level is implemented and maintain, there is a dramatically positive shift the in the Probability of Detection (POD) reducing the risk of an unidentified technical vulnerability or compromise.



# Key Requirements | Moving Target Threat Model

Understanding a modern moving target threat model is an essential first step in providing an adequate level of professional service for the end-user and ultimately delivering a professional services program based on an informed, or perceived threat level with the realistic objective of mitigating the risk of a technical compromise.

After significant live target field deployment related testing and evaluation, and the application of extensive lab testing, the Signal Hound ™ family of products have continued to emerge as the best receivers on the market for the low cost, field reliability and advanced deployment capabilities possible, for a wide range of RF evaluations, including TSCM, SIGINT, and RSSM ™ applications.

Our Technical Research and Standards Group (TRSG) ™ continually engages in a wide range of recognized R & D activities, academic consultation, and most importantly, professional interaction with experienced field deployed technical operators worldwide at all known and developing threat levels, and across all sectors (public and private).

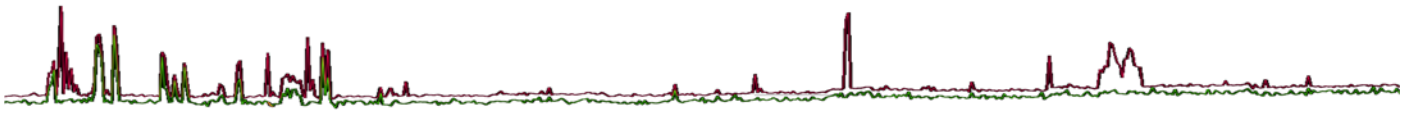
Our quest for excellence sees no boundaries and we are responsive to the technical operator's field experience during operational deployment.

When it is all about the money for the operator, (either services or equipment sales, or both) they will simply do what the client is asking for no matter how ineffective the approach, service or product may be at the end of the day.

Educating the client is an absolutely essential first step in understanding the Cost Vs Return expectations, which includes the fact that the ineffective application of the wrong professional services, operator or equipment resources, at the wrong time, actually increases the potential for an undetected compromise to continue harming the end-user, and instill a false sense of security, not to mention the financial cost of the ineffective service delivery.

> *"If the client is serious about preventing economic-espionage and / or enforcing critical wireless policies at the facility level, and preventing the compromise of electronic eavesdropping incidents, they will look to a professional technical operator for his / her expertise, advice and guidance in implementing the best possible strategy, within an appropriate budget allocation consistent with the perceived operational threat level".*
>
> *Paul D Turner, TSS TSI*

The "You don't know what you don't know" thought process, is the big unknown that many players in the industry are willing to ignore when it comes to marketing and selling technical security, and electronic sweep work to unsuspecting clients.



Defining the unknowns, is not always going to be easy, for the end-user or the technical operator, but openly addressing the expectations, limitations and misinformation builds a powerful credibility at the assignment level.

> *"Without consistent uninterrupted data collection, gaps of unknown certainty exist reducing the Probability of Detection (POD) significantly, and this in turn advances the potential and opportunity of economic-espionage to occur, costing the organization on average 1.5 million dollars per incident" in lost opportunity.*
>
> *Paul D Turner, TSS TSI*

Every 2 hours of daily, (annually averaged) missed data collection results in an 8% chance of failing to detect or identify a targeted incident of economic-espionage, based on the presence of an RF assisted eavesdropping device.

Some manufacturers and technical operators claim their equipment has a 100% Probability of Detection (POD) based on sweep speed alone yet fail to understand that 100% POD for the typical deployment of 40 hours of actual time-on-target, out of 8,760 hours (based on 365 days @ 24 hours) annually is just 0.5% POD from a modern moving target threat model perspective for the RF phase of the inspection.

This is not effective or acceptable (never was really), from a due-diligence perspective, and should raise serious liability concerns for the technical operator!

As an example, if a receiver such as the Signal Hound BB60C is sweeping a 6 GHz ROI at a frame rate of 4 FPS, this represents 250 mSec per sweep.

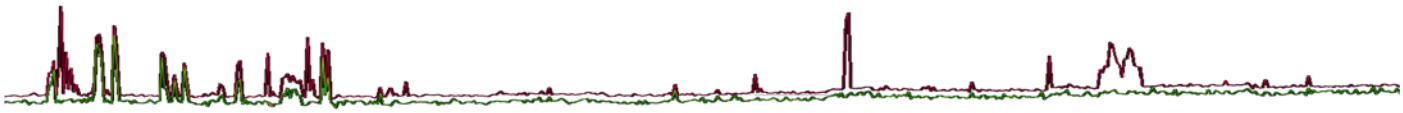
In the event that a Signal of Interest (SOI) is periodic in nature and bursting at a rate of 100 mSec every 30 minutes, what are the chances that the burst will occur while the receiver is actively sweeping that particular frequency, and at the exact moment the periodic burst occurred?

It is highly unlikely that every such periodic burst will be captured using for example, a 4-hour collection period, typical among surveyed technical operators.

A single burst may be captured at some point in time, every time, or maybe never, but it is essential that "time-on-target" be sufficient to capture the signal as often as possible, over a period of time in order to present a wide range of analytical possibilities.

If the equipment resource is not deployed 24 / 7 / 365 and the device, is by design, operated offensively than it is likely that typical defensive methods are simply going to be ineffective.

Collection for an extended period of time, for example 120-hours, 240-hours or even longer, will significantly enhance the POD for any given SOI as a factor of time.



Sweep speed is an important Probability of Intercept (POI) factor, however, as can be seen, it is not the entire picture that professional technical operators must understand.

The Resolution Bandwidth (RBW) is also an important factor to consider as the receiver is only as fast as its design speed. We can see an “apparent” increase in speed by using wider RBW settings, reducing the search Range of Interest (ROI) or both, increasing the POD, but only for the new limited by design ROI, but it does not actually increase the receiver design speed.

Another factor is the DSP Vs Time, which must be handled during the sweep process.

The narrower the RBW, the longer the processing time will be and the wider the RBW, the shorter the processing will be to compete DSP requirements.

There is an important trade off that must be realize and understood, in order to find the optimal settings for the intended mission parameters.

Time-on-Target is a critical determining factor for Probability of Detection (POD) from a field deployment perspective and the technical operator needs to look at the big picture, based on big data collection as opposed to limited “time-on-target” spectra.

This clearly is, or should be, an incentive to change the way TSCM services are delivered and perhaps more importantly, how POD is presented to the end-user from a risk mitigation perspective, in both the public and private sector.

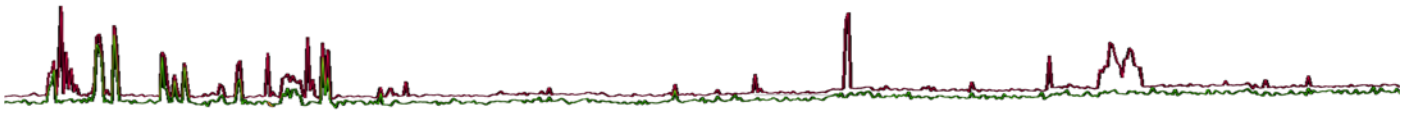
The means of this transformation is found in the core foundation of the Kestrel TSCM ® Professional Software, which is based on an entirely new technically feasible, budget friendly, moving target threat model that includes the complementary capability of Remote Spectrum Surveillance and Monitoring (RSSM) ™, now possible due to the recent acceleration in Software Defined Radio (SDR) technology advancements during the past decade, and perhaps more so in the past number of years.

However, without the powerful hardware pioneered by manufacturers such as Signal Hound the software will have nothing to analysis and it is essential that innovative new concepts and technology at the hardware and software level continue to be developed, keeping pace with known and emerging threat technology.

More important perhaps, is the necessary break from the cold war era tactics; something that most manufacturers have failed to embrace over the past decade.

Virtually every TSCM resource has followed the same dated and often obsolete design strategies, rather than evolving with the dramatic changes over the years, embracing a new moving target threat model methodology and develop the required threat detection technology.

Under the Kestrel TSCM ® brand, this methodology is referred to as managed Remote Spectrum Surveillance and Monitoring (RSSM) ™, which is new industry terminology and methodology that significantly enhances the overall efficiency and timely identification of a wireless security policy breach, or identify trends and patterns that may indicate potential breach conditions that need to be further investigated or analyzed.



Even at a professional service delivery level of 240 hours annually (20 hours / Month), the Probability of Detection (POD) is only 2.73% that the technical operator will detect and identify even a moderately sophisticated Technical Surveillance Device (TSD), which is actually operating within the current RF spectrum collection window.

Now consider all the other variables, such as inexperienced technical operator, non-optimal equipment resources or techniques, etc., and it is easy to understand why Probability of Detection (POD) by the numbers, is an essential due-diligence consideration.

Economic-espionage is rarely identified in real-time, based on a single defensive technology, method or technique.

It takes a lot of validated technical data and other experience-based intelligence collected over a significant period of time, to develop accurate threat modeling and trends.

In-fact, the very core concept of Kestrel ® Signal Analytics (KSA) ™ must include all relevant intelligence sources as part of the analytical cycle as defined by the TSB 2000 (Technical) Standard ™.

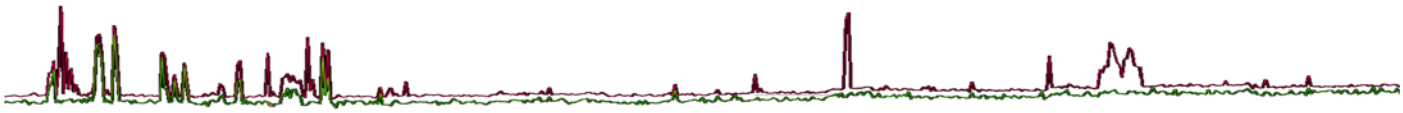
The capture of RF spectral data can be correlated against access control records, HUMINT, video surveillance systems, alarm system events and other sensory based data to bring clarity and reason to any suspicious spectral activity or used to validate patterned relationships leading to the identification of hostile emitters within a defined target facility, or geographical area.

In the past, these systems were simply not available, or integration and inter-operability was not possible, vastly limiting the potential of applying real-world analytics across multiple intelligence sources.

> *"Probability of Detection (POD) by the numbers is what Kestrel TSCM ® Professional Software, managed Remote Spectrum Surveillance and Monitoring (RSSM) ™ and Kestrel Signal Analytics (KSA) ™ is all about, and we leave the "follow-the-leader" marketing hype, to those that are in the game only for the financial consideration".*
>
> *Paul D Turner, TSS TSI*

The following POD data overview provides powerful insight that the technical operator, and ultimately, the end-user must understand and embrace in order to establish an effective Technical Surveillance Countermeasures (TSCM) program within their respective organizations.

Failure to apply a balanced and methodical approach by the organization with respect to the limiting factors or Probability of Detection (POD) will result in missed opportunity to identify all but the few obvious RF threats decidedly operating at the precise time of the inspection.



> *The 100% Probability of Detection (POD) claimed by many manufacturers and operators is likened to a fast food restaurant claiming they use 100% pure beef, when the reality is that 100% pure beef is only a single ingredient in the overall product and therefore by design is intentionally misleading, but rarely questioned".*
>
> *Paul D Turner, TSS TSI*

Again, what you don't know, you don't know and therefore you cannot build an effective strategy to detect, identify, and neutralize real-world technical compromises, without powerful analytical data in the hands of a qualified technical operator or SIGINT analyst.

This thought process, in part, explains why economic-espionage is rarely identified and organizations continue to remain increasingly vulnerable to a technical compromise, costing millions of dollars annually in lost opportunity every year globally, across Canada and the United States of America.

The threat landscape has changed in that RF vulnerabilities might be exploited by organized crime, cyber criminals and terrorists.

We are no longer simply concerned with competitive intelligence at a fundamental level and it is essential that technical operators not only recognize this reality but take proactive steps to change the approach at every level.

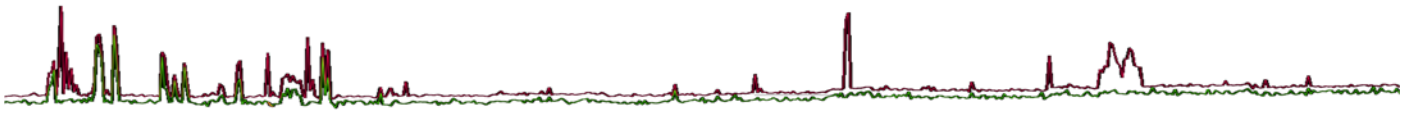
The charted data below is only part of the risk mitigation picture, with the next logical questions being, "what the perceived operational threat level for the organization is" and "what level of risk the organization is willing to accept", or perhaps what level of compromise or loss is the organization willing to gamble against the modest cost of a modern due-diligence TSCM program?

There is always a realistic trade-off between Risk Mitigation Vs Budget that neither the technical operator and / or the end-user rarely fully understands due to the lack of factual information surrounding successful acts of economic-espionage for which, the details are never known.

The few actual acts of economic-espionage that are discovered often involve high profile players that command some attention, but tend to leave the more common competitive-intelligence and vast majority of economic-espionage cases, virtually under the radar.

Fortunately, the means is now available to achieve unpreceded levels of Risk Mitigation Vs Budget, with the integration of the Signal Hound (BB60C) and the next generation (SM200A) hardware in combination with the manufacturers Spike ™ software and powerful third-party Software Defined Radio (SDR) applications, such as the Kestrel TSCM ® Professional Software and managed Remote Spectrum Surveillance and Monitoring (RSSM) ™ capability.

The concept is simple, increase the time-on-target, or go home!



# Probability of Detection (POD) | By the Numbers!

POD by intention and design must take into account factors well beyond the equipment resources deployed and ultimately include increased “time-on-target” in a modern moving target threat model, along with an entirely new deployment methodology and approach.

If you cannot reliably deploy hardware that is specifically and ideally designed to operate 24 / 7 / 365 (extended period of time), the Probability of Detection (POD) will not meet any acceptable operational level of due-diligence.

Equipment resources that are not designed for specific deployment activities, simply increases the overall liability that something will be missed.

This is why it is so essential to deploy a multiple receiver monitoring system, in a primary collection and analysis role.

This also allow the operator to monitor the ambient RF spectrum environment and the power lines within the target area at the same time.

The power lines are an important element of the overall strategy but are an after thought add on by most manufacturers who fail to understand the necessity of 24 / 7 / 365 monitoring of this dangerously evolving threat technology.

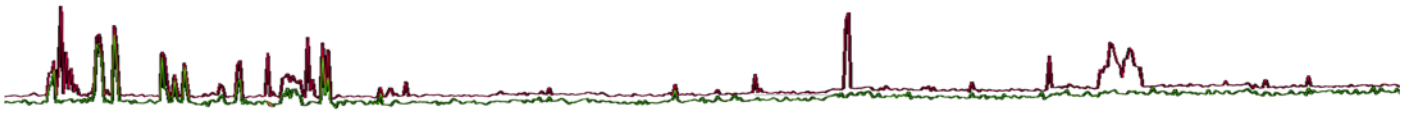
The POD chart below allows the reader to determine the POD based on the defined “time-on-target” factor, highlighting the requirement and advance a business case, for supplemental managed Remote Spectrum Surveillance and Monitoring (RSSM) ™ as a must include deployment strategy, as part of a properly conducted TSCM inspection program.

It is obvious that a combination of TSCM and RSSM ™ activities must be implemented as part of a structured and balanced approach to an effective Technical Surveillance Countermeasures (TSCM) program, to achieve an acceptable level of due-diligence at any given, or perceived operational threat level.

If we make an assumption that a moving target threat model should only cover the normal business or typical work day, plus a risk buffer of say four (4) hours for cleaning and maintenance operations, we might assume the following projection at just 50% POD assuming the threat is an RF emitter and it is active during the runtime capture time-frame, as follows.

365 days @ 12 hours = 4,380 hours annually | 8,760 hours = 50% POD

Obviously, this is simply not possible within a traditional TSCM inspection program and is only made possible through the application of managed Remote Spectrum Surveillance and Monitoring (RSSM) ™ supplementing the traditional weekly, monthly or quarterly inspection programs the organization as implemented.

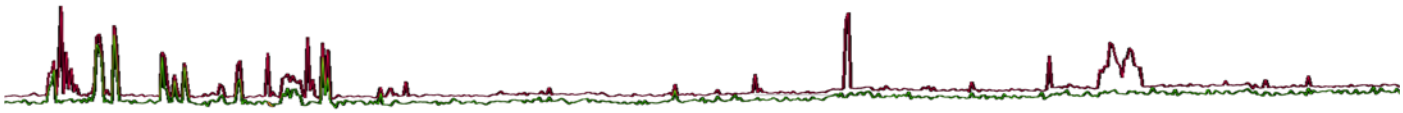


The chart provides a realistic approach and starting point, to determine the real Probability of Detection (POD) based on deployment challenges, and time-on-target limitations.

| Number of Actual Days Possible | Number of Actual Deployment Hours Per Day | Number of Annual Hours of Deployment | Base Probability of Detection (POD) (Opportunity) |
|---|---|---|---|
| 365 days @ | 24 H | 8,760 H | 100 % |
| 365 days @ | 23 H | 8,395 H | 96 % |
| 365 days @ | 22 H | 8,030 H | 92 % |
| 365 days @ | 21 H | 7,665 H | 88 % |
| 365 days @ | 20 H | 7,300 H | 83 % |
| 365 days @ | 19 H | 6,935 H | 79 % |
| 365 days @ | 18 H | 6,570 H | 75 % |
| 365 days @ | 17 H | 6,205 H | 71 % |
| 365 days @ | 16 H | 5,840 H | 67 % |
| 365 days @ | 15 H | 5,475 H | 63 % |
| 365 days @ | 14 H | 5,110 H | 58 % |
| 365 days @ | 13 H | 4,745 H | 54 % |
| 365 days @ | 12 H | 4,380 H | 50 % |
| 365 days @ | 11 H | 4,015 H | 46 % |
| 365 days @ | 10 H | 3,650 H | 42 % |
| 365 days @ | 9 H | 3,285 H | 38 % |
| 365 days @ | 8 H | 2,920 H | 33 % |
| 365 days @ | 7 H | 2,555 H | 29 % |
| 365 days @ | 6 H | 2,190 H | 25 % |
| 365 days @ | 5 H | 1,825 H | 21 % |
| 365 days @ | 4 H | 1,460 H | 17 % |
| 365 days @ | 3 H | 1,095 H | 13 % |
| 365 days @ | 2 H | 730 H | 8 % |
| 365 days @ | 1 H | 365 H | 4 % |
| 365 days @ | 0 H | 0 H | 0 % |

Even at this level, this does not take into account the modern moving target threat model environment, and the reality of on-demand transmitter remote controlled data dumps, activity controlled devices, scheduled store and forward technology and other remote control techniques and methods that are not likely actively transmitting during normal business hours, or may be deactivated during scheduled technical security inspections, including those devices that actively disguise themselves by modulation type anti-detection characteristics, by device design, programming or operation.

It is also essential to understand that there is no real OPSEC in todays countermeasures environment given the sophisticated means available to detect and identify the technical operators presence during the inspection process.



The fact is, there is no problem defeating the defensive technical operator, who is not innovative or responsive in accurately determining the risk at the end-user level and advancing POD through the application of supplemental RSSM ™ as a supplemental methodology.

Without 24 / 7 / 365 managed Remote Spectrum Surveillance and Monitoring (RSSM) ™, the identification of potentially hostile emitters, in-bound or out-bound cannot with any reasonable certainty be detected or identified, except perhaps by chance, when only periodic “snap-shot” style RF spectrum analysis is utilized.

## Strategic Tactical Advantages

Signal Hound SDR hardware provides a significant tactical advantage in providing scalability and flexibility as a powerful deployment option by design and exceptional value as a low-cost solution.

The capability of RSSM ™ deployment as a best practice to capture real-time analytical data, allows the technical operator to identify potentially hostile signal events in near real-time, on-demand, or easily analyze complex trends over a specific period of time, based on detailed historical data captured and documented within the Kestrel Project Files (KPF) ™ for playback, analysis, and formal session report generation.

A tactical advantage is gained when actionable RF intelligence is available to the technical operator or analyst.

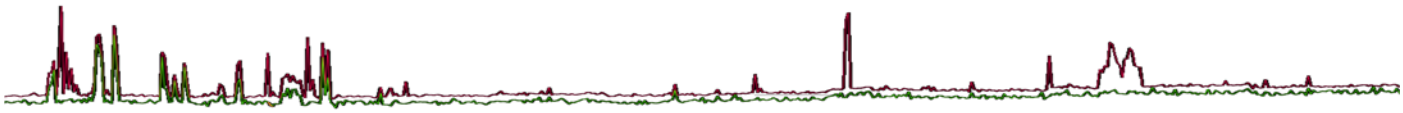
The vast majority of TSCM equipment resources currently on the market, fail to generate actionable RF intelligence and provide little in the way of meaningful spectra or analytical data.

This is unfortunately, also the case with periodic RF sweeps of a defined target area as a sole means of service delivery and therefore, definitive conclusions cannot be made as to whether or not, a comprise exists, existed, or will exist at some future point in time.

## Key Benefits

The Remote Spectrum Surveillance and Monitoring (RSSM) ™ implementation is cost effective, budget friendly solution that is fully scalable as operational deployment requirements change within the organization or professional service providers need to deploy additional resources across multiple end-users.

Signal Hound is a proven leader in bringing innovative Software Defined Radio (SDR) hardware to the industry that is responsive to the needs and requirements of professional technical operator’s at all operational deployment levels, worldwide within a US commerce-controlled environment.



The Kestrel ® TSCM Professional Software, captures date and time stamped data archival files that can be intuitively played back during post review and analysis, without the requirement of having a receiver connected.

Captured IQ files, including full demodulation capability can also be played and looped without a receiver connected during post analysis.

A significantly enhanced Probability of Detection (POD) is realized over typical periodic “Snap-Shot” style RF inspections when these are conducted as the only means of signal level analytics.

RSSM ™ captures, monitors and reports significant spectral events within the ambient RF spectrum, even when the technical operator is not present; 24 hours a day autonomously, without the need for operator intervention for days, weeks or months at a time.

RSSM ™ permits the technical operator to monitor any number of independent remote collection locations in real-time utilizing Live View Analysis (LVA) ™, or review data as historical files on demand.

## Detection Methodology and Strategy (DMS) ™

Traditional periodic TSCM inspections are and will remain a critical element in safe-guarding against economic-espionage and illegal forms of competitive-intelligence gathering activities.

However, the field is changing at a dramatic pace with the pending 5G technological shift to a everything wireless playing field.

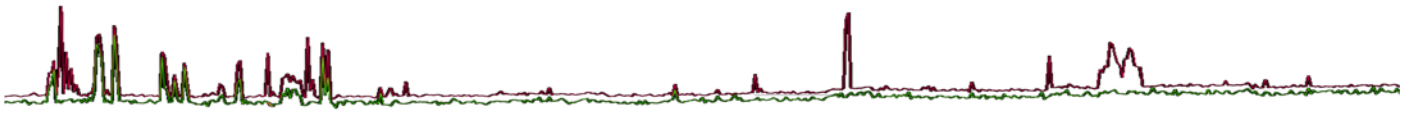
The DMS ™ strategy must provide for and include 24 / 7 / 365 data capture for critical infrastructure, or at the very least, extended periods of Remote Spectrum Surveillance and Monitoring (RSSM) ™ across all critical infrastructure at the facility level, multiple sites or even multi-national operations.

The continuous or extended capture of the ambient RF spectra, and the target area power grid, provides the capability for real-time and post analytical review on a historical basis.

Spectra event filtering and automatic flagging of significant spectra events, facilitates streamlined technical operator review and technical analyst hand-off, on demand dramatically improving the Probability of Detection (POD).

Automatic Export Control (AEC) ™ and Command Line Programming (CLP) ™ provide advanced data filtering of significant events and opportunity for analysis of targeted Signals of Interest (SOI) that present themselves during the extended collection process.

The export of triggered IQ in multiple formats permit the analysis of real-world signal events that can be resolved for actionable intelligence extraction and provide an opportunity for exploitation for the purpose of Signals Intelligence (SIGINT).



## System Platform | Architecture

The deployment of a Remote Spectrum Surveillance and Monitoring (RSSM) ™ system at the base level involves a single area of critical infrastructure such as a primary boardroom, or small to medium executive office suite, consisting of approximately 2500 to 5000 square feet as identified within the TSB 2000 (Technical) Standard ™, for each Near-Field Omni-Directional or targeted use of a directional collection antenna, depending the on facility occupancy and structural configuration of the space.

The system can also be deployed external to the facility or defined target area, as a geographical reference to better determine if any particular signal event is ambient or related to the target facility.

However, simple (A-B) is not a recommended practice for determining whether or not a SOI is ambient or a threat risk within the facility.

There are a number of trade-craft techniques that can be utilized to provide misleading spectrum information when (A-B) is the only determining factor.

The ability to detect and identify targeted Electro-Magnetic Pulse (EMP) conditions, or intentional Radio Frequency (RF) flooding is fully supported when deployed in potentially hostile environments at the national security level.

At the entry level, or recommended test deployment level a single < RSSM ™ Sensor > can be deployed, and later relocated as requirements, or program parameters change, or it becomes strategically necessary to expand the collection environment.

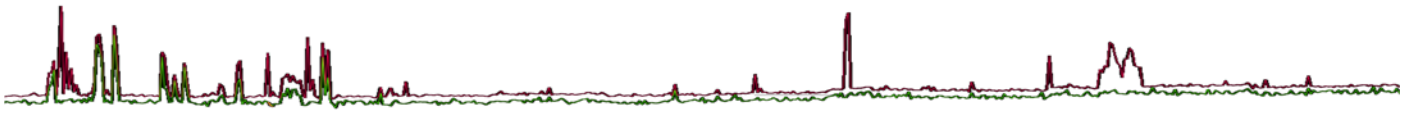
The Kestrel ® RSSM ™ concept is fully scalable as tactical, business requirements, or the perceived threat level changes bringing yet another level of budgetary control to the implementation roll-out.

The term < RSSM ™ Sensor > in Kestrel ® terminology, describes and includes a suitable high-speed Software Defined Radio (SDR) receiver, such as the Signal Hound ™ (BB60C) 9 kHz to 6 GHz @ 24 GHz per second (4.2 FPS) at 20 kHz RBW across a 6 GHz Range of Interest (ROI), the Signal Hound (SM200A) 100 kHz to 20 GHz @ 1 THz per second (50 FPS) at 30 kHz RBW across a 20 GHz Range of Interest (ROI), or any number of other supported receivers or analyzers, a suitable collection antenna such as the, infrastructure ceiling mounted KestrelPod ™ Ultra-Wideband Surveillance Antenna.

The recommended host computer platform should be an Intel Core i7 7700HQ (or higher) with 16 GB to 32 GB RAM for professional unattended applications for days, weeks, or months of active runtime deployment, we strongly recommend a suitable mid-level gaming laptop with at least 1 TB SSD such as the Samsung EVO PRO SSD.

The RSSM ™ system can be configured into a Rapid Deployment Kit (RDK) or tactical drop kit should transportability be required by the end-user such as during protective operations.

Collection antennas can be preinstalled in critical areas of the facility and monitoring hardware can be installed or connected quickly at any location (on-demand) when the antennas, cabling, LAN or fiber-optic link infrastructure is already installed within the facility.



The KestrelPrey III | Advanced RF Locator ™ can be deployed as a low-profile walk-about, full featured spectrum analyzer with the deployment of the Kestrel Log Periodic (KLP) Kit minimizing the requirement for a separate broadband receiver.

Transitioning from an operator assisted collection strategy to locate and neutralize mission is easy to accomplish, with a powerful walk-about RSSI based, direction-finding spectrum analyzer complete with signal level RSSI trending and an IFB mode, to very quickly locate the emitter.

The ability to detect, identify, track, and locate potentially hostile signal events that have been first detected and filtered for investigation by the RSSM ™ system, or during Location based Differential Signal Analysis (LDSA) ™ or Time Differential Signal Analysis (TDSA) ™ and then easily transition to a familiar user-interface to localize the emitter is vastly more efficient than a having to setup a broadband detector with different settings.

A reliable high-speed network connection, consisting of a dedicated DSL, Gigabit LAN, Wi-Fi, or 3G, 4G LTE Modem is required for remote system communication which significantly improves the timely valuation of Signals of Interest (SOI).

Autonomous operation via an advanced software project activity scheduler permits receiver and band level automation programming allowing the RSSM ™ system to run autonomously in an operator defined pattern collection mode, for operator review at a later time when the site can be safely accessed.

LAN connectivity can be backed-up by a Wi-Fi network roll-over to provide a measure of fail-safe redundancy.

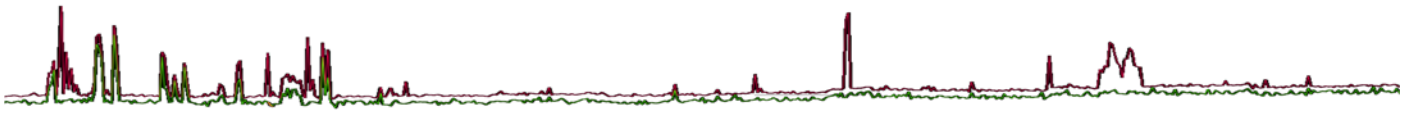
Our powerful Autonomous Measurement and Collection System (AMCS) ™ architecture provides an opportunity to run Kestrel in an embedded “headless” runtime environment and stream multiple source data feeds.

The AMCS ™ feature is supported with a Software Development Kit (SDK) complete with example code and an open API for custom solutions, or the technical operator can simply use our ready to deploy AMCS ™ Client application.

Rapid Deployment Kits (RDK) can be installed virtually anywhere for temporary collection requirements at special events, in support of protective operations, tactical scenarios, embassies, consulates, strategic meetings and other application specific deployment in potentially troublesome areas and left totally unattended and unmonitored for a period of time autonomously, automatically collecting and recording RF spectrum data for later review by the technical operator, or accessed remotely for on-demand analysis.

Larger scale RSSM ™ systems may include multiple < RSSM ™ Sensors > across several areas of critical infrastructure, independently or on a shared network infrastructure.

In larger distributed RSSM ™ collection systems monitoring may be deployed across multiple buildings, multiple sites or geographical regions or span national borders as required.



The following key points are the primary concerns that must be addressed for both small and large scale systems.

## Power Management

**Uninterruptable Power Supplies (UPS)** | Momentary power supply interruptions or extended power outages will shut down the system making it impossible for remote recovery. It is recommended that AMCS ™ or PC BIOS programming be adjusted for sites requiring autonomous operation to ensure a measure of fail-safe auto recovery is established.

**RF | EMI | Surge Protection** | Power surges, power abnormalities and high energy spikes can cause significant disruptions, or damage to sensitive network-based components resulting in data corruption or loss. Surge protection is strongly recommended.

**Ethernet Enabled Power Bars** | The addition of an IP based Ethernet enabled power bar installed after the UPS provides the ability to remote power cycle the entire system or specific system components.

## Network Connectivity

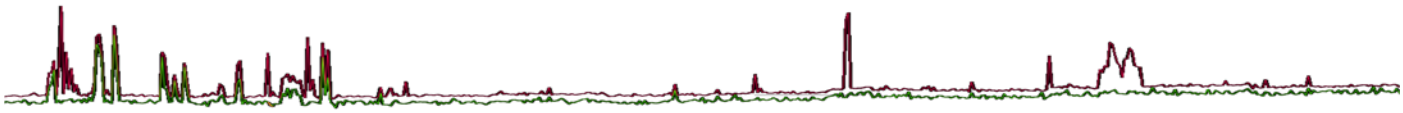
**Digital Subscriber Line (DSL)** | A dedicated high speed LAN connection is required to effectively stream high bandwidth data to and from the remote host computer and provides an adequate level of security by isolating the RSSM ™ system from the target facility network. It is essential that the router and other network equipment be maintained on UPS backup.

**4G LTE** | High speed modems can be utilized as a fail-safe rollover backup, or deployment as a primary wireless communication network.

**Wi-Fi** | Remote monitoring systems can be configured to roll over to a secondary wireless network connection (if available) to provide redundancy in the event that the primary LAN connection is interrupted or lost.

## Autonomous Operation

**Project Activity Scheduling** | In the event that communication is lost with the remote site the system state cannot be altered by the technical operator. Project level activity scheduling is an essential software feature permitting autonomous operation of the system, without the need for operator intervention by automatically following a predetermined schedule, starting and stopping hardware, bands or sub-bands without technical operator intervention.



**Artificial Intelligence (AI)** | The use of Artificial Intelligence (AI) at the fundamental core level of integration allows advanced interaction between various software modules and components necessary for the capture, processing, alerting, and hand-off of critical data elements for the technical operator analytical process.

## Remote Desktop Software (RDS)

**Remote Desktop Software (RDS)** | TeamViewer ™ offers a commercial or corporate licence and provides unlimited remote client connectivity access that allows remote system reboot, remote programming and operation, file transfer, demodulation audio streaming and full spectral visualization over a highly secure encrypted connection.

**Encryption** | TeamViewer ™ includes encryption based on 2048 RSA private / public key exchange and AES (256 bit) session encryption. This technology is based on the same standards as https: / SSL and meets today's standards for security. The key exchange also guarantees full, client-to-client data protection. This means that even the TeamViewer ™ routing servers are not able to read the data stream.

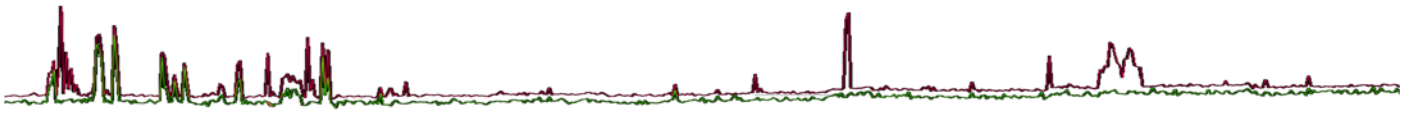
**Code Signature** | All program files are secured using VeriSign code signing technology. This allows you to verify the origin of the executables you have received.

**Access Protection** | In addition to the Partner ID, TeamViewer generates a session password that changes with every software start in order to provide additional security against unauthorized access to a remote system. Security relevant functions like file transfer require additional manual confirmation from the remote partner. Also, it is not possible to invisibly control a computer. For data protection reasons the person sitting at the remote computer has to be able to detect when someone is accessing the machine.

**Two-Factor Authentication** | Two-factor authentication adds an additional security layer to protect TeamViewer ™ accounts from unauthorized access with access control through white listing. With two-factor authentication a code generated on a mobile device is needed in addition to < username > and < password > in order to sign in to a TeamViewer ™ account. The code is generated via a time-based, one-time password algorithm. The code is protected by SRP and is thus safe from man in the middle attacks.

**Real-Time Analysis** | Activity at the remote site can be monitored, reviewed and analyzed in real-time by the technical operator, including functional access to all controls features and live streaming of demodulated audio and video.

**Remote Programming** | The ability to remotely setup project files, alter collection parameters or define detection limits and meet reporting requirements can all be managed remotely.



**Remote Host Computer Updates** | The ability to routinely accomplish remote updating for the operating system, application software, receiver firmware or even the remote desktop software is an essential capability and fully supported.

## Automatic Export Control (AEC) ™

**Periodic (Loss or Exceedance) Export** | The ability to export critical signal event data to CSV format based on operator defined time periods provides an essential component that includes small manageable files for easy storage and network transfer. Third-party software can be utilized to convert CSV data to graphical representation models in the form of charts and graphs.

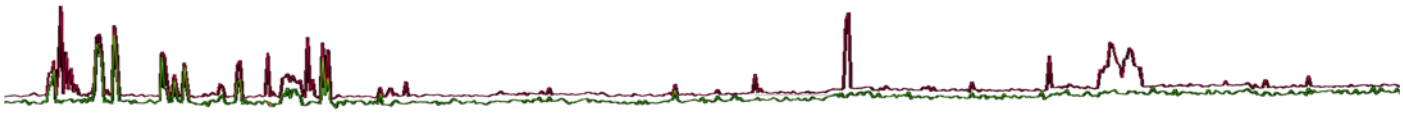
**Triggered (Loss or Exceedance) Export** | Perhaps just another variation on the export of CSV formatted content that is based on a trigger, rather than time, however, the importance of this capability cannot be minimized for managed Remote Spectrum Surveillance and Monitoring (RSSM) ™ assignments. Particularly, during extended deployment the ability to export both the Spectra and RSSI values allows the technical operator to manipulate data sets for deeper analysis with a cumulative series of event triggered CSV files.

**Triggered (IQ Sample) Export** | Perhaps the most essential part of the analytical equation is the ability to trigger on spectral events and record an actual CSV IQ or KIQ sample of the captured event. The capability further exists to capture up to 10 seconds of pre-event and post-event data to confirm that no associated events such as remote control devices preceded or followed immediately prior to, or after the Signal of Interest (SOI) appeared or disappeared.

## Remote System Integrity (RSI) ™

**Intrusion Detection Module (IDM)** | The ability to generate an operator defined, random RF signal burst using a remote operated wideband RF Vector Signal Generator (VSG), strategically positioned within the target area, utilizing a technique similar to rolling code encryption is maintained at the RSSM ™ remote monitoring site and is under the full control of the technical operator to confirm and verify the RSSM ™ system is active and capable of detecting the targeted Signals of Interest (SOI), across the Range of Interest (ROI) serviced the IDM.

**System Resource Monitor (SRM)** | The SRM serves as a PC and application health monitoring resource and includes a storage drive status monitor than automatically alerts and can stop collection before the storage drive runs out of space.



## Administrative | System Maintenance

RSSM ™ systems are remotely positioned and require careful planning and implementation as well as an understanding of remotely maintaining the host computer for peak efficiency and trouble-free operation, particularly at potentially inaccessible locations, is critical.

It is essential to ensure that all of the remote system components are powered by an Uninterruptable Power Supply (UPS) for a measure of fail-safe operation.

It is recommended that the technical operator consider a laptop computer and USB 3.0 powered receiver, which can provide a measure of backup power and surge protection in the event that momentary utility outages occur.

Remember to ensure the Network connectivity is part of the power backup strategy.

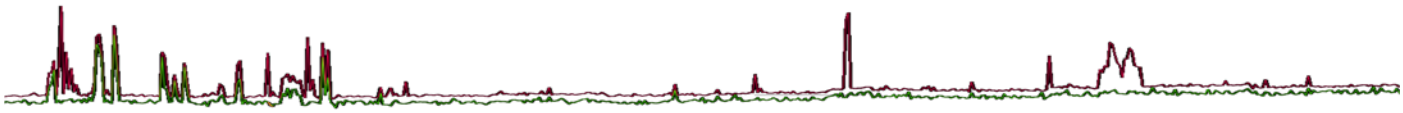
Utilizing a Remote Desktop Software (RDS) that permits remote system host computer reboot, OS maintenance and full system programmability of the system is essential.

## Technical Analysis | Kestrel Signal Analytics (KSA) ™

The most important aspect of continuous RSSM ™ deployment is learning the application of targeted data filtering and event trigger capture to bring clarity to complex data.

It takes some time to determine the normal ambient RF spectrum environment and some tweaking of the capture process will likely be required.

> *"Kestrel Signal Analytics (KSA) ™ significantly enhances the ability of the technical operator to understand the complex spectra captured, advancing the Probability of Detection (POD)".*
>
> *"Kestrel Signal Analytics (KSA) ™ brings a powerful new analytical approach to how captured Signals of Interest (SOI) are processed during real-time analysis and historical post event review".*
>
> *"The RF spectrum is increasingly complex and it is often difficult, impossible or not desirable (for legal reasons) to extract the actual intelligence due to the type of modulation, use of encryption or privacy concerns.*
>
> *"Kestrel Signal Analytics (KSA) ™ looks at the signal analysis problem differently by processing captured signal level activity against an Analytical Traffic Analysis (ATA) ™ profile, specific to the target area".*



There are a number of important tools that can be utilized to control file management size and complexity and strategically filter captured data for clarity.

The following is a small sampling of just some of the tools found within the Kestrel TSCM ® Professional Software, utilized to condition, characterize, capture, filter and display potentially hostile Signals of Interest (SOI) for operator analytics.

## Project Activity Scheduler

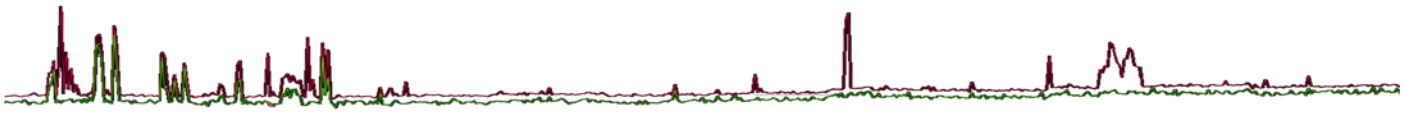
- Project Activity Scheduler
  - Receiver level | Start | Stop | capability
  - Spectrum (band) level | Start | Stop | capability
  - Operator defined | Maximum Duration | custom programmability
  - Unlimited number of operator defined events
  - Working Time Zone Off-Set
  - Trace Count Control
  - Trace Time Control
  - Trace Limit Alarm

## Write Compression

- A significantly reduced Kestrel Project File (KPF) ™ storage footprint is realized
- Improved PC memory utilization and system resources prioritization
- Enhanced allocation of host computer system resources
- Clarity and focus of distributed spectral energy profiles
  - Captures (1/n=?) traces record as a single Kestrel Super Trace (KST) ™
  - Powerful compression algorithm with enhanced Real-Time Event (RTE) and Waterfall Display (WFD)
- Significantly enhanced playback and analysis of normally complex historical data sets is realized when (1/n=?) compression is utilized by the technical operator.

## Minimum Detection Amplitude (MDA) ™

- Operator defined triggered threshold | Exceedance | alerting capability
- Full colour classification Automatic Threat List (ATL) generation
- Manual ATL export to CSV format
- Automatic export of MDA ATL via optional Automatic Export Control (AEC) ™ | OPT AEC |
- Advanced Signal Combining Technology (SCT) ™



## Dynamic Alert Annunciator (DAA) ™

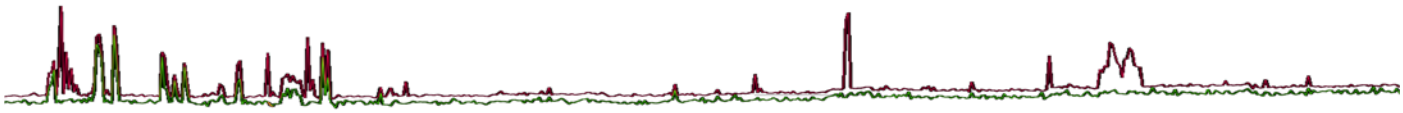
- Unlimited operator defined Dynamic Alert zones
- Triggered signal | Exceedance | detection
- Triggered signal | Loss | detection
- RED (Fail) | GREEN (Pass) Visual Annunciator
- Export DAA data to CSV format
- Real-Time Alert Condition Statistics data display
- Automatic Export Control (AEC) ™ | OPT AEC enabled

## Automatic Export Control (AEC) ™ | OPT AEC

- Operator defined Periodic Export of any supported alert trigger
- Provides a measure of Fail-Safe Data Backup
- Operator defined Write Storage location
- Export ALL or Export NEW programmability to CSV format
    - Minimum Detection Amplitude (MDA)
    - Spectrum Baseline Logging (SBL)
    - Dynamic Alert Annunciator (DAA)
- Triggered event CSV Export
    - Export Spectra
    - Export RSSI
    - Export IQ

## Automatic Recording Mode (ARM)

- Sustainable Write Storage Management
    - REC Active | ARM Disabled | All data written to storage media
    - Automatic Spectrum Analyzer Mode (SAM) ™ | Data <u>not</u> recorded to storage media
    - Automatic Recording Mode (ARM) | Only triggered event data is recorded
- ARM Mode | Only Dynamic Alert Annunciator (DAA) triggered events are recorded
    - Triggered event recording up to 60 Seconds prior to event appearance
    - Recording of active signal event duration
    - Recording up to 60 Seconds after event termination



## Time Differential Signal Analysis (TDSA) ™

- Single Collection Location
  - Supports time block trace comparative analysis and dynamic filtering
  - Compare time blocks that span hours, days, weeks or months
  - Supports runtime capture and analytical filtering on the fly
  - Supports post review and analysis filtering on the fly
  - Dynamic operator defined period selection for better analytical focus
  - Supports operation across multiple LDSA ™ locations
  - Supports operation across multiple radios

## Geographical Area Review (GAR) ™ | Data Comparative

The ability to access and import comparative Peak Envelope Capture (PEC) ™ data from other relevant geographically co-located RSSM ™ systems, brings significant value to the analytical process by allowing the technical operator to directly compare historical Kestrel Project File (KPF) ™ data from multiple related or unrelated collection sites.

This is accomplished utilizing the < Load Compare Bands > feature to import any available Antenna Collection Location based < Peak Trace > spectral reference data for comparative purposes from any collection site.

Obviously, nearby collection sits that are geographically significant offer enhances reference data that can be utilized at the current collection site.

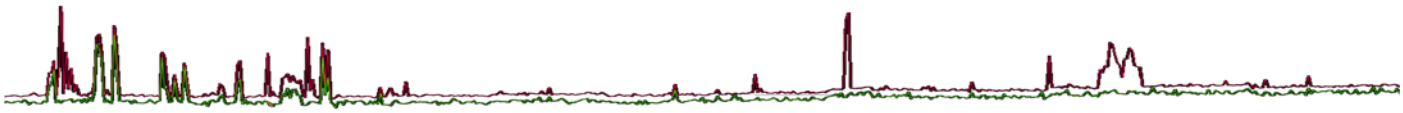
Imported historical data from other Kestrel Project Files (KPF) ™ is persistent within the current file and can be utilized for comparative purposes until removed.

This has not effect on the data integrity from any collection site for which data is imported for comparative purposes.

## Geographical RSSM ™ Management (GRM)

Kestrel Central Visualizer ™ is yet another powerful tool on the horizon and is currently under development in full tactical support of multiple geographically based < RSSM ™ Sensors > on a closed LAN network or across the Kestrel ® cloud (Internet) infrastructure.

The larger the RSSM ™ system becomes, the more critical data filtering (signal level classification and characterization) and the use of Kestrel Analytics ™ will become.



The use of < Targeted Event Triggering > serves as a powerful data filtering tool when the target area is governed by a formal wireless policy prohibiting all or certain types of wireless devices within a well-defined security zone.

This permits the technical operator to quickly identify unusual patterns and characteristics within the ambient RF spectrum environment.

However, the issue is arguably more complex when wireless technology is an integral part of the day to day operation as it is decidedly more difficult to resolve friendly from hostile emitters within defined target areas.

However, trends and patterns in spectral activity will surface over time permitting the operator to identify potentially hostile emitters, separate from those authorized.

## Professional Service Level (Recommended)

The recommended service level is based on an entirely new threat model that includes the following approach and Scope of Work (SOW) elements, consistent with the perceived threat level anticipated or ultimately determined for each organization.

## Remote Spectrum Surveillance and Monitoring (RSSM) ™

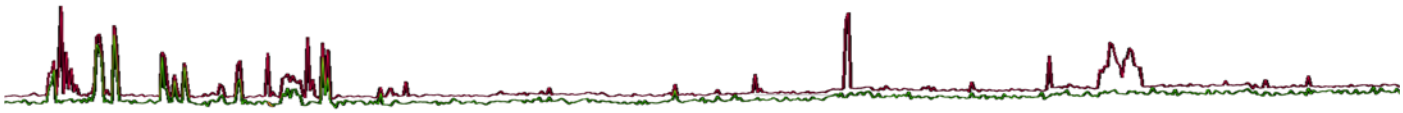
- Critical Infrastructure (Continuous < 24 / 7 / 365 > Monitoring)
  - < Boardrooms > < Executive Office > < Security Zones >
  - Continuous Spectrum Surveillance < Days > < Weeks > < Months >

Targeted Ad Hoc (Random Periodic Due-Diligence < 72 H / 120 H / 240 H > Monitoring)

  - < Events > < Off-Site Meeting > < Hotel Rooms > < Executive Residence >
  - < Off-Site Workers > < Disaster Recovery Sites > < Internal Investigations >
  - < Non-Critical Areas >

## Power Line Monitoring < Sensor Based >

- Critical Infrastructure (Continuous < 24 / 7 > Monitoring)
  - < Boardrooms > < Executive Office > < Security Zones >
- Targeted Ad Hoc (Periodic < 72 / 120 / 240 > Monitoring)
  - < Events > < Off-Site Meeting < > Hotel Rooms > < Executive Residence >
  - < Off-Site Workers > < Disaster Recovery Sites > < Internal Investigations >
  - < Non-Critical Areas >



## Threat Considerations < Device Type >

The following threat probabilities describe the < type > < characteristics > that may be associated with the potential compromise.

- Analog (Audio) Transmitter | Probability | High-Threat
  - Presence of Remote Control | Medium-Threat

- Digital (Audio) Transmitter| Probability | High-Threat
  - Presence of Remote Control | High-Threat
  - Complex Modulation | High-Threat
  - Encryption | Medium-Threat
  - Anti-Detection Capability | Medium-Threat

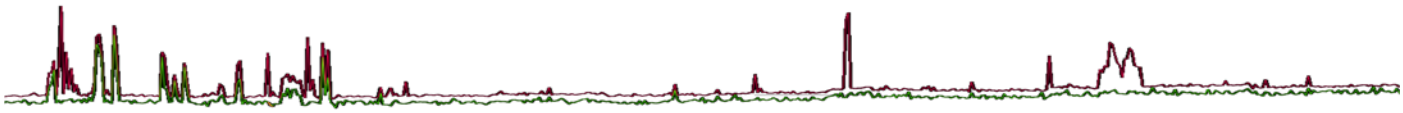
- Digital Audio Recorder | Probability | High-Threat
  - High Compression Codec | Probability | High-Threat
  - Encryption | Probability | High-Threat
  - Presence of WI-FI or Bluetooth | Probability | High-Threat

- Broadband Over Powerline (BPL) | Probability | High-Threat
  - Presence of Multiple Nodes | Probability | High-Threat
  - Presence of < Data > < Video > < Audio > | Probability | High-Threat
  - Encrypted Data | Probability | High-Threat

- Analog | Power Line Carrier (PLC) | Probability | Medium-Threat
  - Presence of < Audio > < Signalling > | Probability | High-Threat

- Digital | Power Line Carrier (PLC) | Probability | Medium-Threat
  - Presence of < Audio > < Signalling > | Probability | High-Threat

- Optical | Visible Light Communication (VLC) | Probability | Medium-Threat
  - Presence of < Data > < Audio > | Probability | Medium-Threat
  - Use of Hybrid Technology | Probability | Low-Threat



- Optical | Infrared | Probability | Low-Threat
  - Presence of < Audio > | Probability | High-Threat

- Analog (Video) Transmitter | Probability | High-Threat
  - Presence of Embedded Audio Sub-Carrier | Probability | High-Threat

- Digital (Video) Transmitter | Probability | High-Threat
  - Presence of Embedded Audio Sub-Carrier | Probability | High-Threat
  - DECT | FHSS | DSSS | FSK Modulation | Probability | High-Threat
  - Encryption | Medium-Threat

## Traditional Inspection | Deployment (Mandatory)

- Periodic RF Spectrum Analysis “Snap-Shot” Localized Inspections (Critical Infrastructure)
  - Technical Security (TSEC) value is limited to < Live Event > monitoring
  - RSSM ™ direct data comparative (Strongly Recommended)

- Power Line Analysis “Snap-Shot” randomized inspections (Critical Infrastructure)
  - Technical Security (TSEC) value is limited to < Live Event > Monitoring
  - RSSM ™ direct data comparative (Strongly Recommended)

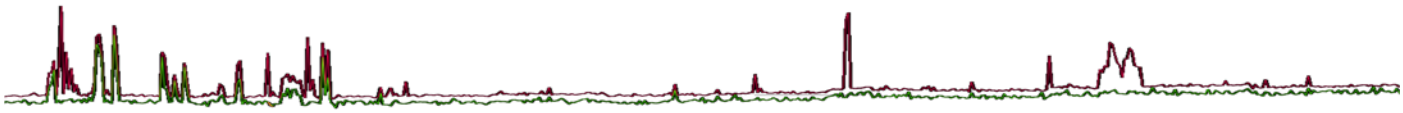
## Additional Inspection Priorities (Not All Inclusive) | Beyond RF

The following information is offered as additional related inspection parameters that must be considered along with the Radio Frequency (RF) collection and analysis.

It is by no means inclusive and other professional protocols are required to round out a detailed competent technical inspection.

**Physical Inspection Protocol** | There are some aspects of a Technical Security (TSEC) program that require the operator to periodically access the target area for the purpose of completing a detailed physical inspection.

It is strongly recommended that a formal physical inspection protocol be initiated on a periodic basis as a due-diligence best practice and immediately prior to, and after any sensitive meetings or events that are scheduled to take place within protected areas of the facility.



When the Kestrel ® Remote Spectrum Surveillance and Monitoring (RSSM) ™ is the primary collection method it will become necessary to provide base training for an on-site individual to conduct periodic physical walk-through inspections of the target area between those completed by the technical operator.

**Counter-Intelligence Review** | Human factor elements are generally the most significant threats to the in-house protection of proprietary information.

The vast majority of vulnerability findings are not electronic in nature, but rather insider threats and human factor compromises that might only be identified by the physical TSCM inspection program.

The RSSM ™ concept is designed to effectively seek out Radio Frequency (RF) emitters and must be supplemented by a carefully implemented periodic TSCM physical security inspection protocol.

The Counter-Intelligence (CI) review looks at the facility from a people-flow perspective, looking at how sensitive information is processed, handled, stored and utilized both on-site and off-site.

A review of garbage and recycling practices and base level penetration testing is required to determine the security posture of the facility.

**Thermal Imaging** | The application of a thermal imaging review of the target area can quickly identify pinhole cameras and other similar powered devices emitting thermal properties.

However, devices, such as those that may be buried inside walls or other cavities can often be identified, even when they are not powered utilizing a thermal imager, as there will potentially be a significant differential in temperature of a device against the ambient background temperature due to air-flowing across different types of materials inside a wall or other structure.

It will often be necessary to thermally condition the target area and thermally tune the radiograph image to gain the most benefit.

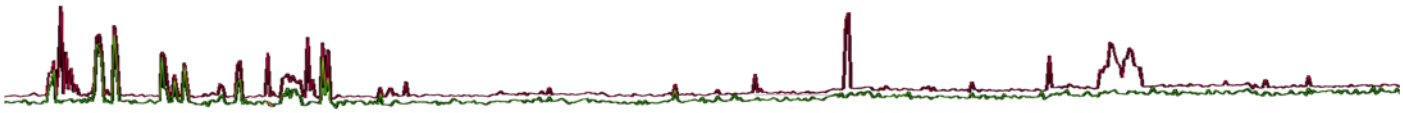
Thermal tuning is often over-looked by technical operators due in part by a lack of theoretical and practical training in conducting thermography.

**Non-Linear Junction Detection** | An NLJD is a very powerful TSCM equipment resource, yet it is just one more tool utilized to examine the target area.

There has unfortunately been considerable hype in the past few number of years as to which technology is better, generally from a non-objective sales perspective and certainly not from the perspective of an experienced field operator.

The industry standard was at or below 900 MHz and newer technology extended into the 2400 MHz (and higher) transmit range.

The push to move to the 2400 MHz was recognized early by our Technical Research and Standards Group (TRSG) ™ that 2400 MHz was not capable of detecting all technical threats, just like the 900 MHz NLJD was not capable of detecting all threats.



Every type of application and structure is different and it is absolutely essential that operators maintain competing technologies for this reason.

At least two (2) NLJD manufacturers have now reintroduced additional 900 MHz products back into the market with updated technology after all the 2400 MHz hype.

It is for this reason that professional level technical operators maintain competing technologies and ignore the marketing hype.

The most important aspect of any equipment resource, is that the operator must deploy a range of competing technologies and never rely on any one technology, expecting conclusive results.

**Active (Wired) Microphone Identification** | The threat of wired microphones is significant within a modern and perhaps one of the more challenging aspects of a technical inspection.

Wired microphones may be found on virtually any unused wire pair entering or leaving the target area and may or may not contain local side amplification.

**Fiber-Optic (Microphone) Technology** | The threat of fiber-optic technology has become a serious threat within a modern threat model has more and more fiber-optic technology has entered the consumer and commercial market.

The ability of the technical operator to first understand the level of adversary likely encountered is a function of understanding the perceived threat level faced by the client.

**External (Infrared) Laser Interception** | The technology remains a valid concern in a modern threat model, however, it is not a strong contender on the economic-espionage stage, given significant deployment limitations.

The presence of optical threats is relatively easy to detect and identify the source, whenever the technology is active.

The method is somewhat passive in nature and no intrusion into the target area is required.

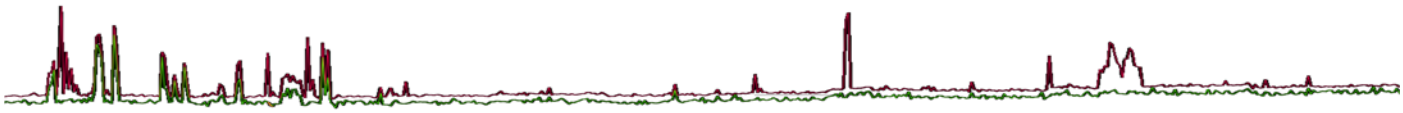
Obviously, this method would require a clear optical path into the target area, such as a window or a reflective object within the target area.

**High Speed Video (Audio) Interception** | A relatively recent discovery includes the ability to recover target area audio by use of high-speed video capture of room audio stimulated objects within the target area.

This capability only requires visual access into the target area, a high speed camera and a computer based algorithm, so the system is totally passive in nature.

**Telephone Network Analysis** | The examination of the telephone network is complex and time consuming with a mix of analog, digital, wireless, and VoIP technology.

There is no single equipment resource to accomplish this task across all of the different technologies and network equipment currently in use, including cloud based telephony services.



There are a number of excellent resources available that are utilized extensively across the telecommunication industry that deliver excellent results.

**Computer Network Analysis** | Like the telephone network in many ways the computer network is complex and requires very specialized examination at both the physical and forensic level.

Physical inspection is generally the easy part of the inspection and experience indicates that the vast majority of vulnerabilities and discovered compromises can be identified by a strong physical inspection protocol, along with the application of solid RF Spectrum analysis protocols.

*Have a question about the use of Signal Hound products or the Kestrel TSCM ® Professional Software for Remote Spectrum Surveillance and Monitoring (RSSM) ™? Give us a call!*

*Paul D Turner, TSS TSI*

*President | CEO*

*+1 647-293-7384 or visit us online at [www.pdtg.ca](http://www.pdtg.ca)*