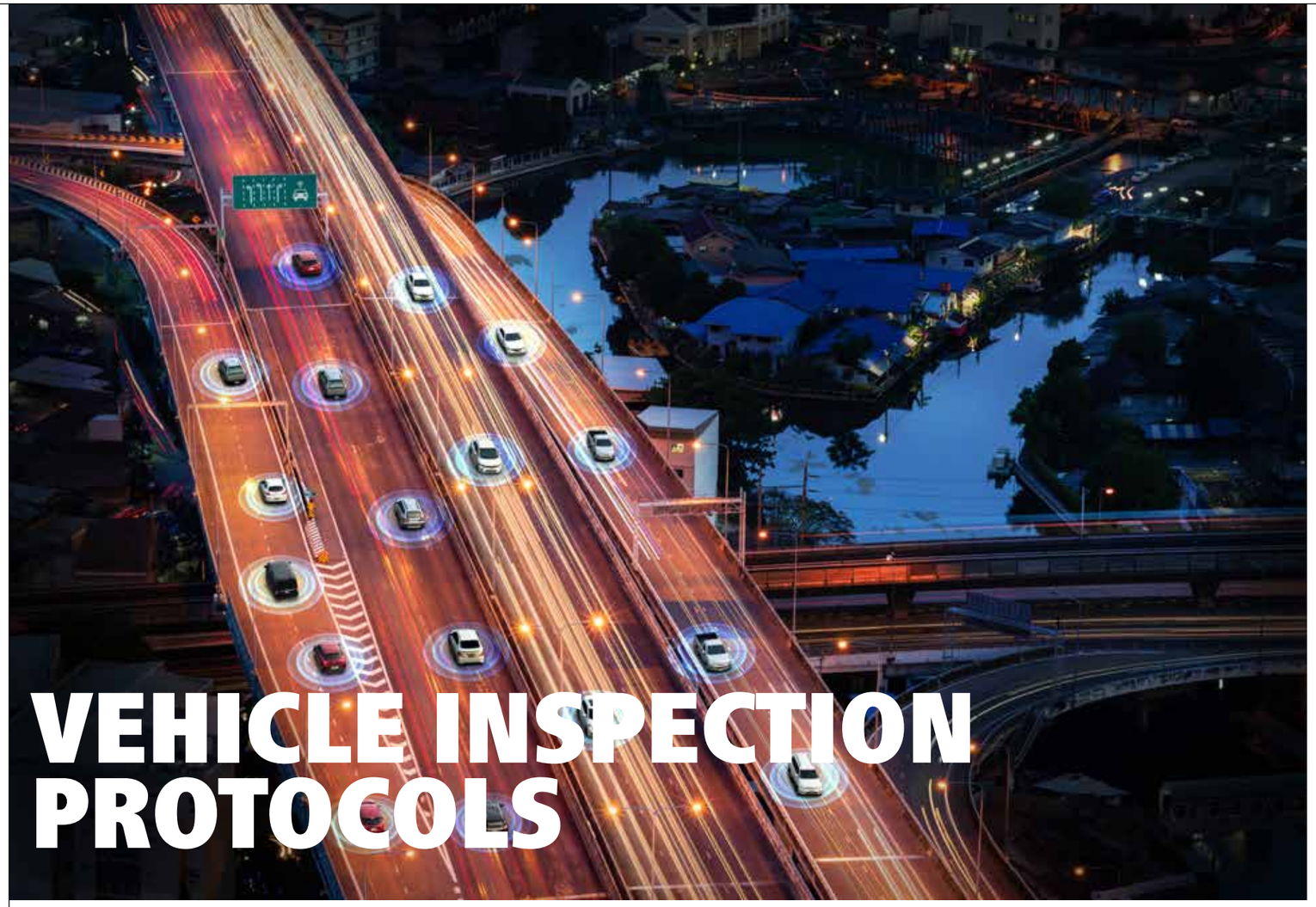


VEHICLE INSPECTION PROTOCOLS

PD Turner *outlines the search methodology steps essential for TSCM Vehicle Search Specialists (VSS)*

During the past decade, vehicles have decidedly shifted from open analogue-copper-based technology to a highly embedded sensor-based digital computer relationship. This notable shift involves wireless transmitters, complex digital and optically embedded software and firmware sub-systems that are no longer restricted to just internal command and control, but also for a wide-range of outbound wireless communication.

This complex shift in vehicle technology has created significant technical challenges for both offensive operators at the law-enforcement level and mostly defensive TSCM-VSS operators with upward of 600 sensors and multiple computer processors. The implied level of complexity has left the vast majority of TSCM operators working in an experience void – placing competent technical inspections outside of an effective competency level necessary to secure against existing and dangerous modern threat technology vulnerabilities.

The discipline of high-risk protective operations is perhaps our greatest challenge in the sense of an absolute requirement to not only function within a traditional TSCM role to identify generally low-level tracking devices, but we are also seeing significantly greater hostile intentions at the technology level.

In a modern threat environment we must also guarantee that the vehicle is cleared of Improvised Explosive Devices (IEDs) – a task which the majority of technical operators are simply not qualified to undertake; while state-sponsored threat actors engaged in espionage, car-jacking, ambush and kidnapping, political unrest, criminal protest and terrorist activities; malicious vehicle hacking, spoofing and vehicle take overs of critical, steering, acceleration and braking sub-systems round out the risks.

The highest protected assets are compromised or subjected to a so-called technology failure globally on a daily basis

Interception, exploitation, surveillance and tracking are all possible as vehicle attacks are becoming more common as threat actors become more technically savvy. Embedded factory and after-market hardware, software and firmware vulnerabilities, both by-design intentionally and thousands of unintentional and undocumented vulnerabilities can be exploited during an attack.

A professional radio-frequency suppression enclosure is now considered an essential component for permanent, fixed vehicle inspection facilities and temporary vehicle search requirements – such as those conducted during organised protective operations. The number of required TSCM vehicle inspection processes continues to evolve and each emerging process requires additional working steps and, perhaps more importantly, considerable time on task.

A radio-frequency suppression enclosure permits the deployment of the active countermeasures concept, far beyond industry-wide misconceptions about the detection of advanced vehicle-based surveillance and tracking technology. A typical high-level, high-risk TSCM vehicle inspection can easily span 24 to 48 hours of time-on-task, however – fortunately – a considerably shorter period of time is required for basic, due diligence inspections.

The time-on-task required to accomplish today's vehicle inspections continues to increase and the TSCM-VSS must seek official Vehicle Search Specialist (VSS) certification while respecting a standards based process or be willing to accept the implied liability and risk associated with the safety of those under our protection. The VSS must assess and apply a formal standards-based approach requirement as a basic due-diligence, advanced inspection protocol or a fast tactical inspection – each with inherent concerns, benefits and levels of risk-mitigation.

The challenge for law-enforcement in the concealment of authorised devices is that the mission is offensive in nature and the vehicle may be subjected to intense defensive inspections by unknowing criminal actors or TSCM operators.

During research for this feature, I conducted an internet search and found reference to what appears to be a private sector operator in the UK and one in the US openly advertising residential and vehicle sweeps specifically to detect authorised law enforcement-based surveillance and tracking devices. The vast majority of private sector operators are very careful not to compromise active law-enforcement activities and the likelihood that properly selected and installed devices will not be surfaced by private-sector operators with limited training, technical resources or the required time-on-task. Alternatively, the mission may be entirely defensive as a due-diligence countermeasure in search of little more than low-cost, poorly installed devices that are relatively easy to surface.

Given the emerging technology shift, the use of a radio-frequency suppression enclosure and the deployment of Dimensional Geolocation Heat Mapping (DGLHM) is a powerful and proven capability when conducted within a standard-based, total Energy Capture (TEC) process for vehicle-related inspections.

The inclusion of a standards-based combination of mandatory and optional vehicle inspection steps must be strictly consistent with the operator's risk assessment and specific mission requirements. Operator-based VSS certification involves all aspects of a formal TSCM inspection protocol well beyond the radio-frequency process. However, a competent RF inspection is by far the most essential technical requirement from as low as 9kHz and well into the mmWave region to cover 77 to 81GHz. It is essential to understand that this minimum frequency capability requirement is fast accelerating to even higher frequencies well into the THz region of the electro-magnetic and photonic spectrum.

ALL ELECTRIC AND AUTONOMOUS VEHICLES BRING COMPLEX NEW TECHNOLOGY THREATS

As part of a standards-based approach, there are 14 essential steps required to surface upward of 95 percent of radio-frequency threats. Each of these requires specific operator training to fully understand the complex process and therefore each of the recommended steps must be considered as a separate module from a training perspective.

Each process step requires specific actions to be performed by the operator to condition and evaluate the vehicle under inspection to identify and ultimately exploit potentially hostile physical surveillance devices or what is becoming more common – the compromise existing vehicle software and firmware metadata.

The lack of the physical presence of a surveillance device generally results in the operator finding nothing and clearing the vehicle for service when too much emphasis is focused on physical sweep protocol.

The provided steps assume a high-risk mission, adequate time-on-task, the deployment of an RF suppression enclosure and a competent, well-trained TSCM-VSS operator. They are as follows: Step 1: Geo-Graphical Area Review (GAR) single point or reference capture merge; Step 2: No Vehicle Present (NVP) suppression tent single point reference capture; Step 3: Vehicle Rest State (VRS) vehicle locked (Faraday isolated key fob); Step 4: Key Fob Approach (KFA) approach vehicle with key fob; Step 5: Vehicle Electrical State (VES) electrical state (key fob unlock/open door; Step 6: Enable Accessory Mode (EAM) enable vehicle ignition to accessory on; Step 7: Ignition Running Mode (IRM) enable vehicle ignition to on (engine running); Step 8: Vehicle Test Drive (VTD) take the vehicle on a parameter-based test drive; Step 9: Timed Test Run (TTR) 10 to 30-minute test run (minimum); Step 10: Distance Test Run (DTR) 1 to 5km distance (minimum); Step 11: Speed Test Run (STR) | 60 to 80km/h speed (typical average speed); Step 12: Ambient Capture Option (ACO) in-the-wild reference capture (optional); Step 13: Immediate DSA Capture (IDC) vehicle running immediate DSA capture; and Step 14: Spectrum Comparative Analysis (SCA) complete a detailed analytical review

Picture credit: AdobeStock

DIMENSIONAL HEAT MAPPING

Jumping ahead several days into the TSCM-VSS operator certification process are the results of active surveillance devices missed by field operators who failed to deploy a radio-frequency suppression enclosure and follow a standards-based approach.

We are seeing current and emerging vehicle manufacturers moving to entirely new levels of Software Defined Vehicle (SDV) integration. The majority of the SDR-based sensors and controllers are multiplexed across a complex sensor package and a vast array of Electronic Control Units (ECU), including fiber-optics and multiplexed digital signals.

THERE ARE 14 STEPS TO SURFACE UPWARD OF 95 PERCENT OF RADIO-FREQUENCY THREATS

The danger is in the programming and potential unintentional vehicle operator inputs that can surface unexpected behaviour and consequences. Vehicle and external support infrastructure might fail or be compromised in hacking and DoS attacks.

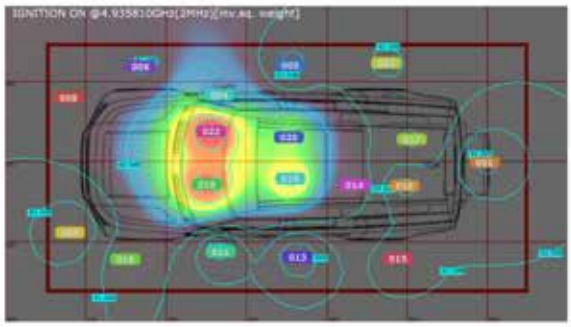
TSCM vehicle inspections need to involve radio-frequency analysis across a nearly 100GHz spectral range. Cyber-related vehicle attacks have risen at progressive rate of more than 90 percent since 2010 with motives including malicious intent, financial crime; and nuisance related hacking! Even the best software coding practices are likely to result in vehicles that are infected with thousands of unique software and firmware bugs or vulnerabilities. Sniffing attacks can potentially find vulnerabilities and allow the compromise of critical operational and passenger safety systems.

There is really no one source of quality assurance when sourcing components across a complex global supply chain and multiple manufacturers of the same components randomly installed in the same model vehicle. The VSS operator must therefore have a strong working understanding or ultrasonic sub-systems, remote keyless entry, GNSS-GPS, satellite communications, cellular mobile networks, WI-FI, Bluetooth, RADAR signature analysis, LIDAR, ultra-wideband – including air-tag and radar technology – optical visual and infrared spectrum.

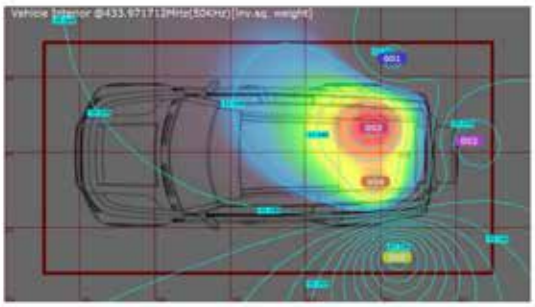
The VSS operator must understand tire pressure monitoring systems, tele-start remote control heating, gesture control and passenger monitoring, wireless power transmission and charging, vehicle information and communication systems, near-field communications and radio frequency identification integration.

Electric and autonomous vehicles bring complex new technology threats including, dedicated short-range communication (cellular and off-network), universal garage door openers, eCall, on-Star C-V2X, V2X, V2P, intelligent traffic systems and, cyber-security sub system attacks such as the manipulation of vehicle systems, forced acceleration, unintended braking or aggressive steering due to threat actor hacking ●

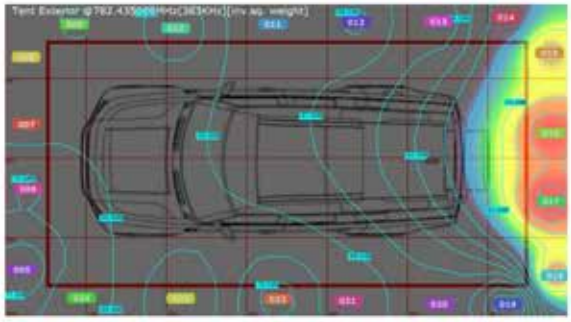
Paul D Turner, TSS TSI is the President/ CEO of Professional Development TSCM Group Inc., and is a certified Technical Security Specialist (TSS) and Technical Security Instructor (TSI) with 46 years' experience in providing advanced operator certification training; delivery of TSCM services worldwide; developer of the Kestrel TSCM Professional Software and manages the Canadian Technical Security Conference (CTSC) under the operational umbrella of the TSB 2000 (Technical) Standard.



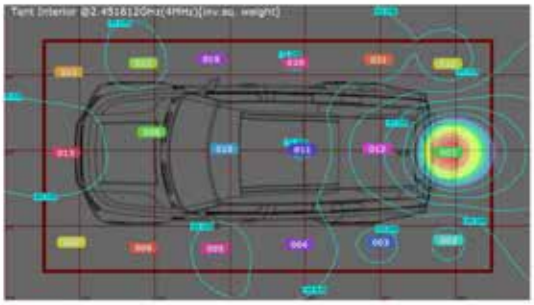
Detected video transmitter without audio identified at 4.9 GHz, clearly within thevehicle passenger side area with the antenna orientation causing propagation outward to the right side of the vehicle.



This demonstrates the effectiveness of the radio-frequency suppression enclosure against false positive emissions and external intermittent ambient signals, allowing a clear picture of the vehicle-under-inspection.



The operator incorrectly, deployed an NLJD before the radio-frequency analysis against an anti-detection capable audio transmitter, effectively shutting down the device preventing any further RF detection. When the instructor reset the device, the emission was easily identified by the operator within the radio-frequency suppression tent.



Detection and localisation of a 2.4 GHz surveillance transmitter with video and audio components, with the antenna hidden in an external spare tyre mount. The transmitter was hidden inside the tail gate door structure and missed without the radio-frequency suppression tent due to the extensive 2.4 GHz ambient signal environment.