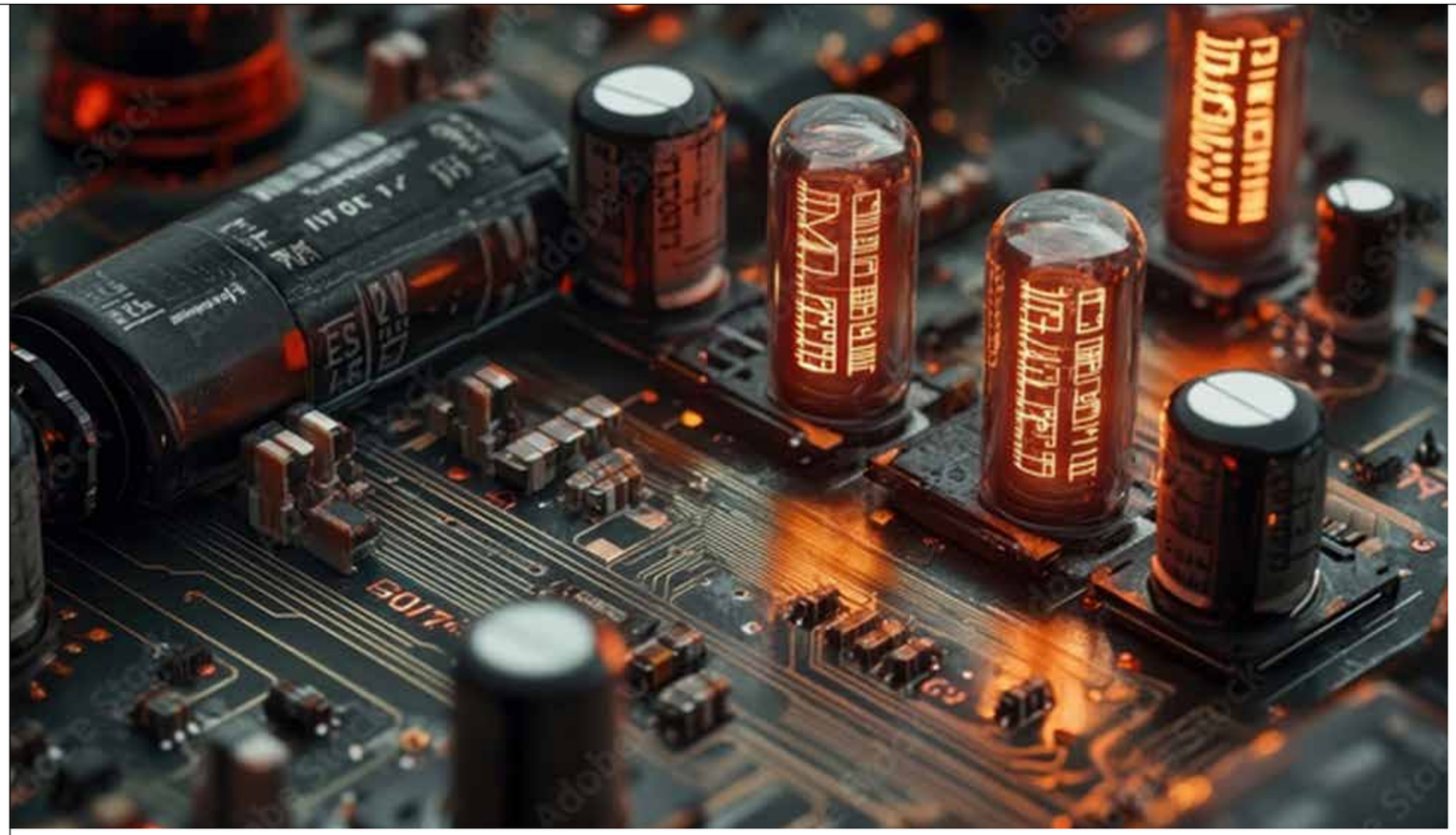


Picture credit: AdobeStock

FIGHTING BACK

PD Turner *highlights the challenges for the world of TSCM when it comes to Wireless Power Transmission*

The wireless transmission of power is an emerging, yet century-old technology that poses a significant concern for technical operators worldwide. A well-concealed low probability of detection (LPOD) surveillance or tracking device can stay 'power-active' without batteries or the use of an alternate infrastructure-based power-source indefinitely. Devices can just as easily be powered on-demand, utilising a radio frequency (RF flooding) signal that may not exhibit recoverable intelligence, in parallel with the wireless charging component to enable the device, appearing as just another ambient noise source. The wireless charging emission does not necessarily need to be highly directional in practice, making the localisation of the actual surveillance transmitter to a specific area extremely difficult when the only detectable signal is the wireless charging transmitter.

Depending on the nature of the actual IoT sensor type or surveillance technology deployed, the output emissions from the device might also be controlled by the threat actor to further minimise detection. The device might utilise a mesh-network to significantly extend the range and enhance the intercept quality of the device emissions once power-active; and may support the ability to utilise extremely low transmit power levels consistent with today's low power and extended operating times. This means that a low probability of detection (LPOD) device on a carrier frequency closely aligned or embedded within the wireless power transmission will make detection difficult for the operator.

The surveillance side of the threat actor device might utilise the same or embedded frequency that is used by the wireless power carrier frequency in a more sophisticated attack profile. The inability of the TSCM operator to detect the device in the absence of a battery technology and the absence of tell-tale indicators of a connection to the local power grid makes the detection of a well-placed and well-shielded remote-control-command, store and forward device exponentially more difficult to identify by traditional TSCM methods, when no infrastructure power or battery, is required to power it.

The ability to transmit energy means that it would be possible to power an unlimited number of IoT sensors and triggers – or 'technical surveillance devices' simultaneously – within a target localised area, or wider environment and selectively enable individual devices or all of them at the same time, supporting battery-free wireless technology via targeted highly scalable wireless charging zones that will blend in with a growing number of perhaps legitimate wireless charging emissions.

From a military perspective, and unfortunately equally so for terrorist and espionage activities, the ability to wirelessly air-power or recharge a UAV or any remote-controlled air, land or sea vehicle containing tactical or improvised munitions can have unique advantages for military and law-enforcement applications. At the same time, such capability might have very unfortunate consequences in the wrong hands. In such a scenario the ability to extend the operating deployment range and loitering time-on-target is not only possible, but a very dangerous new reality.

A UAV low battery condition would see the aircraft automatically navigate to, and simply hover over, a so-called 'charging nest', on a roof top or difficult to access area, while remaining airborne to recharge, and therefore, not require the asset to land for a battery swap-replacement. A UAV might fly a circular arc mission profile, while remaining in the charging zone of a range-limited line-of-sight wireless ground-based power emitter.

Commercial and military aircraft might fly along a traditional airway with directed energy transmitters along the route of travel and used to provide the necessary electro-magnetic energy for charging batteries while airborne; powering electric motors; act as navigation beacons; enable weapon systems; or power personal electronics. Autonomous vehicles can recharge while moving along a roadway containing embedded wireless chargers, eliminating the current requirement and considerable lost time consumed at charging stations.

These devices bridge the gap between traditional capacitors and rechargeable batteries. A super capacitor can replace the device battery. Super-capacitors are powerful energy storage devices that are sometimes referred to as ultra-capacitors or electro-chemical capacitors. Traditional capacitors store energy electrostatically, whereas super-capacitors store energy through the electrostatic field and advantage electrochemical reactions to achieve energy storage. For example, Li-ion batteries generally have a 1,500 to 2,500 life-cycle before they begin to lose their efficiency and operate at a reduced capacity.

Super-capacitors have a much higher life-cycle rating, comparatively exceeding a million cycles and do not have the same efficiency loss as battery technology, making them ideal for long-term dormant surveillance devices when combined with wireless charging capability. There are no chemical reactions as they store energy through an electrostatic field process. They are ideal for applications that need frequent charging and discharging, and require fast peak demand power bursts while providing a longer lifespan with minimal loss of performance over an extended period of time.

Super-capacitors have a high life-cycle rating and do not have the same efficiency loss as battery technology, making them ideally suited for long-term dormant surveillance devices

A WELL-CONCEALED LPOD SURVEILLANCE DEVICE CAN STAY 'POWER-ACTIVE' WITHOUT BATTERIES

Super-capacitors use two primary components in practice that differ from traditional capacitor technology and are ideal for surveillance devices that use a C2 signal, advantaging the fast peak power burst capability. An electrode that consists primarily of activated carbon provides a larger surface for storing energy. An electrolyte liquid or gel conducts ions between the electrodes and when voltage is applied to a super-capacitor, ions from the electrolyte accumulate on the surface of the electrodes – creating an energy layer. This allows super-capacitors to accumulate and store a large amount of energy in a small volume, based on surface physics rather than a chemical reaction. Super-capacitors can charge and discharge at a much faster rate than battery technology.

Super-capacitor technology is continuously evolving and integrated into various wireless devices of specific concern to the TSCM professional. Super-capacitors can easily integrate with radio-frequency and inductive wireless charging technology and the emerging development of integrated wireless charging micro super-capacitors combine energy storage and wireless charging capabilities.

Super-capacitors are being utilised in military and in defence applications, including the advancement of surveillance and espionage activities. They can power threat technology by providing quick bursts of energy and ensuring they remain operational for extended periods without the need for frequent charging. Super-capacitor technology can power compact communication devices used for transmitting digitally encrypted intelligence. These attributes highlight the versatility of super-capacitors in threat technology with the ability to provide reliable power in a compact storage footprint, for field deployment.

Theory and application aside, let's review the expected emission characteristics of a wireless charging device in use today for your iPhone, Smart Watch, Air Card, or other wireless charging enabled IOT devices. Scale, output power and propagation conditions are the primary factors that dictate just

how far a wireless charging platform will be effective for real-world applications. Our data provides an observational starting point to better focus the operator's recognition of where to look and what to look for, when conducting a mission-oriented spectrum analysis for the detection of unknown devices, beyond the device's actual hostile emissions and intelligence-bearing signals.

The mission is to separate the ambient noise from potentially low-level short-range emissions that do little more than contribute to the spectral noise floor, as emitted from the wireless charging device or in reality might be numerous wireless charging emitters coexisting in the same space. Our TSCM lab evaluated three wireless charging devices – each emitted a detectable energy burst at approximately one second intervals, with harmonic artifacts visible to 150MHz with two discernable spectrum signatures that must be explored to understand the operating principles of wireless charging technology. The observed results were achieved utilising software-defined radio hardware and a professional TSCM software package to evaluate the characteristics of the wireless charging devices.

The peak power (1 Sec) burst rate values in dBm (see table) provide the most important detection parameters from a TSCM perspective as the actual charging mode characteristics tend to appear only as an undulating elevated noise floor rather than a high-burst amplitude spike that is present prior to and terminating during the charging mode.

The importance of using positional zoom control and extremely narrow resolution bandwidths allows the operator to gain insight as to whether it is noise or a signal. Peak power for this wireless charging device was a centre-frequency of 143.508911kHz with harmonic artifacts at power levels consistent with distance from direct inductive contact to 12 inches. Our experiment matrix produced data for a low-power 15 Watt wireless charger without the presence of a paired device. It is important to understand that 12 inches is not a detection limitation, but rather an arbitrary lab matrix to estimate the power versus distance versus detection bandwidth of the charger.

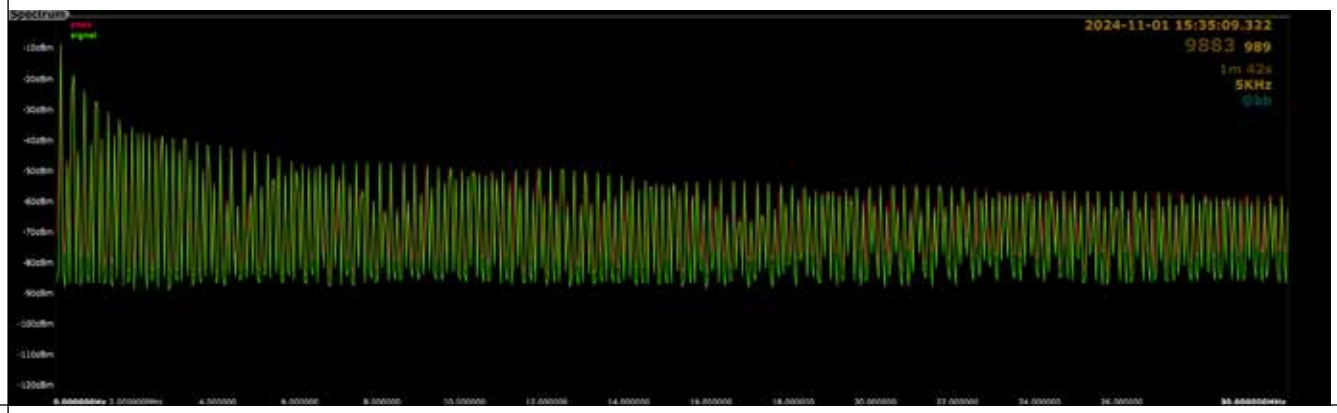
An iPhone was placed in contact with the wireless charging pad, during which time a continuous non-bursting signal presence was observed and the burst-event polling signal stopped. Spectrum characterisation is problematic from a TSCM perspective, as the polling burst event is easily observable whereas the active charging cycle spectrum signature becomes considerably more difficult to identify. The noise floor was elevated by 17dBm across the 150MHz test range. The iPhone produced a Near-Field Communication (NFC) burst during the transition between the charger polling and charging mode. The NFC burst was clearly observable at 13.560104MHz and terminated once the wireless charging phase commenced. The 13.560104MHz signal did not appear when the iPhone was placed near the detection sensor probe and only appeared when the iPhone was in direct inductive contact with the charging pad. Loss of charging continuity occurred when the iPhone was lifted approximately half an inch above, or moved adjacent of the centre of the wireless charger and resumed the one second burst cycle, and the iPhone NFC burst triggered to end the charging cycle.

A continuously visible sinusoidal signal appeared and remained present during the charging process with an obvious phase-shift overlap that by design provides a more even power-transmission delivery and higher efficiency rating. Polling bursts, pairing handshake using near-field communication, device authentication and active charging mode mask what is otherwise an easy charging experience for the user, but in reality involves a decidedly complex smart technology even at the consumer level. It is essential that the TSCM practitioner obtain regular spectrum analysis and analytics training to include complex new concepts and technology that have TSCM implications far beyond the intended nature of the technology ●

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 45 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.

Electro-Magnetic Probe (1GHz)	Range of Interest (ROI)	Resolution Bandwidth (RBW)	Peak Power (1 Sec) Burst Rate	Peak Power @ Frequency
Contact	9kHz to 150MHz	308Hz	-8.82dBm	143.508911kHz
Air Gap 1"			-17.56dBm	
Air Gap 3"			-46.27dBm	
Air Gap 6"			-61.74dBm	
Air Gap 9 "			-71.74dBm	
Air Gap 12"			-79.54dBm	

Our data provides an observational starting point to better focus the operator's recognition of where to look and what to look for when conducting a mission-oriented spectrum analysis for unknown devices



Picture credit: Professional Development TSCM Group Inc.