EXECUTIVE SUMMARY

Power Line Exfiltration (PLE) Threat Analysis and Remediation

Customer engaged AEI on August 3, 2020 to investigate and identify a potential threat by which an individual would monitor the grounding conductor of the TDC Modular Data Center to gain valuable insight about the systems and IT Equipment installed in the module. Knowing that this is not a commonly understood threat, AEI further engaged Bantam Clean Power to help understand the threat and to perform a measurement and verification activity to determine if there is a threat and determine a resolution path.

On August 25th -27th, 2020 AEI and Bantam Clean Power performed measurement activity and verification on a Mobile Tactical Data Center (mTDC) located in Phoenix, Arizona to understand the baseline operation of the functioning IT equipment. Following the measurement of the baseline conditions, a device installed on the supply side of the IT equipment was then evaluated to measure the effectiveness of PLE remediation.

The following points identify the baseline measurements, signal path, and remediation plan.

Initial Measurement/Baseline

- Point of measurement is between the IT Equipment (ITE) power supply and PDU
- Thirteen individual pieces of IT hardware demonstrated that they are communicating self-generated electrical signals in the form of current frequencies onto the AC Mains power line;
- Furthermore, all thirteen individual pieces demonstrated that generated electrical signals are communicated onto the ground wire which is connected to the mTDC grounding path.
- Signals are primarily present in the low frequency range of 100 Hz to 1 MHz but are present at many other frequencies above and below this range.

Signal Propagation

- The ITE-generated signals on ground are detected at the ground bus of the TDC in the electrical panel which is less than twelve inches from the exterior service doors.
- Signals on the ground buss are also captured at the IT Transformer grounding buss bar and the external ground wire on the outside of the mTDC.

Remediation Measurement

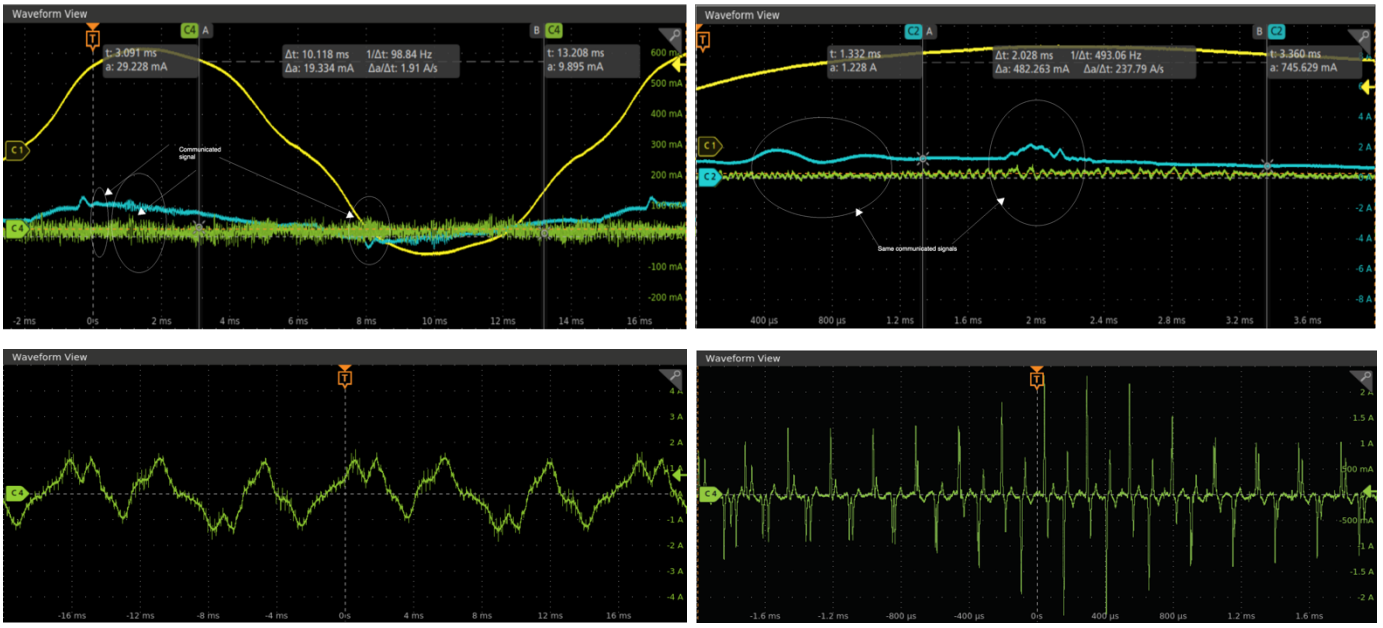
- Points of measurement are a) between the ITE power supply and PP3750 and b) between the PP3750 and PDU.
- Once installed between the ITE and Power Distribution Unit in the racks, the remediation device (Bantam Clean Power model PP3750) is shown to
    - Reshape or waveshape the current signals present on the AC Mains;
    - Remove and prevent any electrical current signal communication (inductive coupling) from AC Mains to Ground (PE).

Conclusion of Signal Propagation

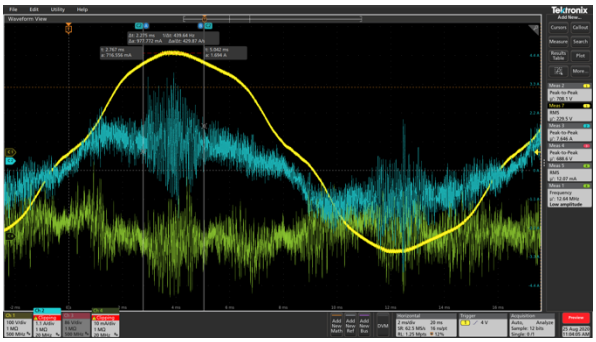
The measurements taken confirm that switching signals generated by ITE which propagate onto ground can be measured on the AC Mains Line current at CB2A but are also measurable at the ground buss junction at the circuit breaker panel. Further, communicated switching signals from all ITE (as well as supporting equipment) is measurable on the IT transformer buss junction and also on the external grounding path cable of the mTDC.

Below is an example of switching signals being propagated from ITE to the External grounding path. Signals originating at Rack 3, IT7 (R3-IT7) are detectable at the Circuit Breaker (CB2A) panel. Going farther upstream on the ground buss (GND images) reveals more switching signals present that should also contain those detected at the origin.

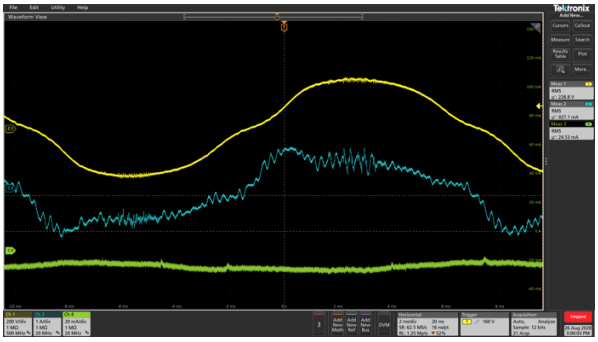
Examples of ITE Generated Signals and the Application of the Remediation Device (PP3750)



The following excerpts highlights IT equipment of particular interest, specifically a network firewall.



Baseline image of R2, IT 1



Remediated Load side of PP3750 and R2, IT1 which illustrates the blocking of generated signals from travelling upstream