ENGINEERING

SECURESMART™ CYBER EMISSIONS MONITOR

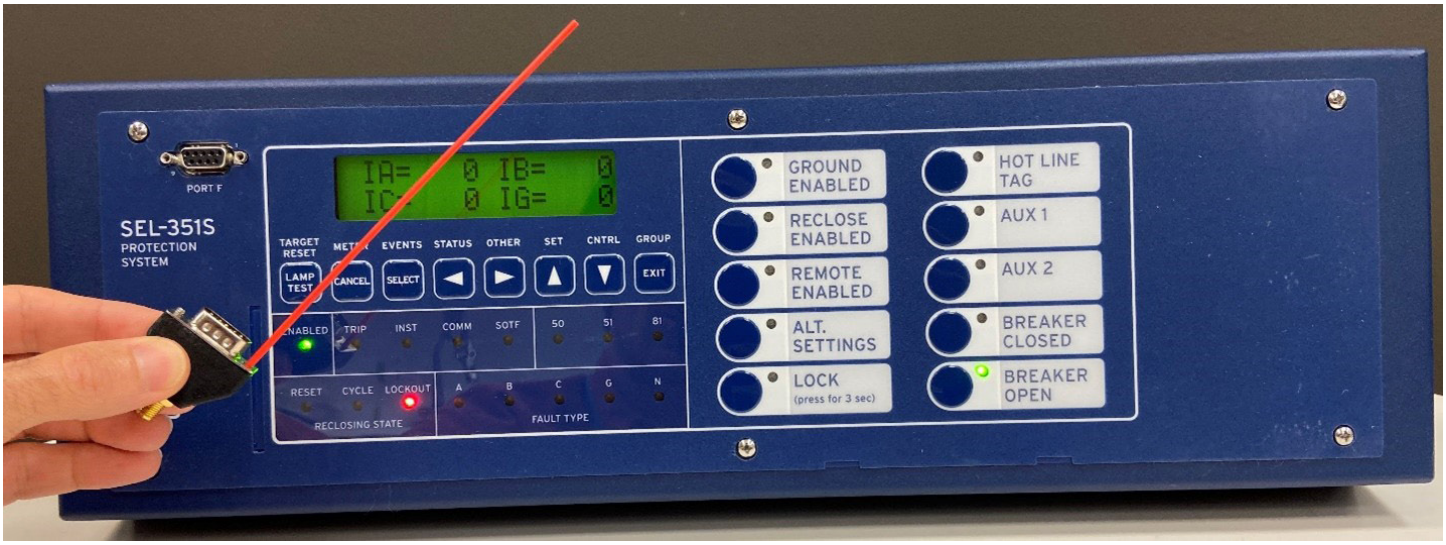
Air-Gapped Monitoring for Control System Devices that's Intelligent, Autonomous, and Undetectable

Peraton Labs' Cyber Emissions Monitor assesses the real-time cyber integrity and operational health of industrial control system equipment via non-intrusive monitoring of unintended radio frequency (RF) emissions. Part of Peraton Labs' SecureSmart™ Critical Infrastructure Protection Solution line, Cyber Emissions Monitor uses machine learning to analyze RF emissions, correlate emissions with device behavior, and detect anomalies. As a fully air-gapped solution, Cyber Emission Monitor performs covert detection of compromises—a hacker cannot tell that equipment is being monitored, much less infiltrate the monitoring system for nefarious purposes.

Industrial control systems (ICS) are increasingly targeted in cyberattacks. Most control system devices are purpose-built embedded computers with limited ability to support the host-based agents and cyber monitoring techniques typically used in IT environments. The situation is further complicated by long service life, as production utility equipment may be in service for decades. Additionally, such equipment often protects or manages critical infrastructure subject to FERC[1]-approved NERC[2] Reliability Standards, where the introduction of active cybersecurity agents can affect site compliance or introduce new risks with an expanded attack surface.

For these reasons, ICS cybersecurity is frequently confined to a physical and electronic security perimeter. This leaves utilities dependent upon the limited substation protection systems in place and without the benefits of continuous monitoring for cyber integrity.

Recent advances in signal processing and machine learning are enabling new cybersecurity solutions that evaluate the integrity of control system equipment in an "air gapped" manner. Peraton Labs' Cyber Emissions Monitor, part of the SecureSmart Critical Infrastructure Protection Solution line, is a novel anomaly detection system that assesses the integrity and operational state of ICS equipment based on non-intrusive monitoring of device RF emissions. All electronic processors produce weak, unintended emissions that can be measured as electromagnetic leakage, sound, and power consumption fluctuations. Cyber Emissions Monitor analyzes and correlates these emissions with device behavior to determine if a device is operating within its normal modes or if its processes, code, or configuration have changed. Because there is no electrical path between the Cyber Emissions Monitor and the device being monitored, it provides true, non-intrusive monitoring that does not extend the attack surface.



[1] Federal Energy Regulatory Commission
[2] North American Electric Reliability Corporation

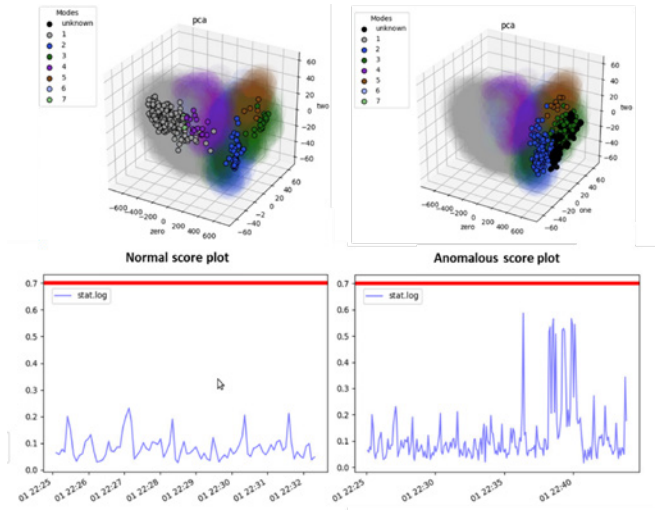
HOW IT WORKS

For substation protection relay and Remote Terminal Unit (RTU) applications, SecureSmart Cyber Emission Monitor uses a small antenna known as CyberStraw that attaches to a device serial port. The CyberStraw collects weak RF emissions produced by the controller's processor as it executes its program instructions. The sequence of instructions, memory access, and I/O operations performed by the controller generate a unique time-based spectral pattern. Through advanced signal processing and machine learning techniques, we distill the principal components of observed patterns to identify various modes of normal behavior in a baseline model. Once the model is created, Cyber Emissions Monitor continuously monitors the device's emissions, classifies its model behavior, and compares against the established baseline. If there are sufficient model behavior differences, an alert is generated to warn of a device anomaly.

CyberStraw sensor

Some examples of the device changes that can be detected by this technology include:

- Malware that introduces a new sequence of firmware instructions
- Launch of a new task or program process
- Issuance of management commands
- Changes in device configuration that cause a different instruction sequence to be executed.
- A change in firmware version



Monitor GUI showing 3D visualization of the device side effects with score plots for normal and anomalous behaviors.

Because Cyber Emissions Monitor senses electric and magnetic fields generated by opening and closing of transistors at the chip level by opcode execution, concealing malware and adversary behavior is extremely difficult. While most new cybersecurity technologies are challenged with application to legacy equipment, Cyber Emissions Monitor is well suited to new and older system alike because of its sensor versatility and the louder emissions generated by legacy equipment.

ABOUT SECURESMART

The SecureSmart Critical Infrastructure Solution line is a suite of industry-leading technologies that defend critical infrastructure and smart energy systems with novel cybersecurity, operations monitoring, and system troubleshooting capabilities for substation systems, supervisory control and data acquisition (SCADA) networks, and Advanced Metering Infrastructure (AMI) and Distribution Automation (DA) field networks. Our flagship SecureSmart continuous monitoring solution is industry-proven with deployments by U.S. utilities since 2013 to monitor, troubleshoot, and maintain multi-service and converged advanced metering infrastructure (AMI) and distributed automation (DA) networks comprising thousands of access points, collectors, and energy controllers.

WHY PERATON LABS

At Peraton Labs, we innovate new technologies and apply them to real-world problems to create novel, breakthrough solutions. Our experts lead applied research in cybersecurity, communications, wireless signal processing, data sciences, and machine learning, providing customers with transformative insights and solutions. As part of Peraton, we deliver trusted and highly differentiated national security solutions and technologies that keep people safe and secure.

Contact us at info@peratonlabs.com and learn more about Peraton Labs Cyber Emissions Monitor technology, and our service offerings for cyber integrity in ICS and SCADA systems.

Peraton