Cyber integrity in SCADA systems
November 2020
Real-time cyber risk problem owned by every critical infrastructure operator

Undetected malware and compromised systems can lie within supervisory control and data acquisition (SCADA) protection systems, poised to strike at an adversary’s command. This reality forces critical infrastructure operators to recognize an underlying, persistent cyber and reliability risk with the feeder, bus and transformer protection systems in their transmission and distribution substations. The genesis of this risk is the specialized, real-time nature of protective relays, remote terminal units (RTU) and automation systems, and their construction—hardware architectures and real-time operating systems that are largely not supported by traditional information technology (IT) cybersecurity defensive tools and scanning agents. These high value equipment targets are critical to energy delivery operations and their cyber integrity is just as important as the cyber integrity of IT systems. To illustrate this point, consider a wide area SCADA network failure. Most operators would resort to manned substation operation. However, even in this state of operation, the operator would still have to trust the cyber integrity of their protective relays to continue delivering power with infrastructure protection.

The problem facing critical infrastructure operators is how to assess the cyber trustworthiness of real-time protective relays, RTUs and real-time automation controllers on regular basis. Existing cyber mitigation methods focus on traffic monitoring, which detects only some of the threat vectors and leaves substantial risk. System resiliency / redundancy as risk mitigation only works if the attack has not already spread to encompass alternative systems. Critical infrastructure operators need to challenge and establish confidence in the cyber integrity of their control system daily—instead of assuming that their system is trustworthy until an event indicates otherwise.

New technology presents risk reduction opportunity

Perspecta Labs’ SecureSmart™ EnergyDefender solution provides innovative technologies to assess the cyber trustworthiness of real-time SCADA assets by analyzing “non-TCP” channel sources to mitigate this risk with timely, concrete and objective evidence to attest to cyber integrity. EnergyDefender establishes cyber integrity using a multi-axis approach that analyzes cyber emissions, binary integrity and the engineering reasonableness and validation of running settings in conjunction with protocol and traffic analysis in support of defensive cyber operations and hunt cyber-weapons in SCADA environments.

SecureSmart EnergyDefender was developed by Perspecta Labs with support from two Defense Advanced Research Projects Agency (DARPA) national security programs—Rapid Attack Detection, Isolation, and Characterization Systems and Leveraging the Analog Domain for Security—and tested, in collaboration with the Department of Energy, on the most advanced cyber range constructed by the government on Plum Island during the Liberty Eclipse exercises. In addition, Perspecta Labs’ SecureSmart solution has been designated a Cyber Catalyst® technology by the eight largest providers of cyber insurance. Critical infrastructure operators may receive an insurance benefit by deploying Cyber Catalyst-designated solutions in their infrastructure to enhance their overall power grid resilience posture.

Cyber Catalyst is a program created by Marsh, a leader in insurance brokering and risk management. The program brings together eight leading cyber insurers focused on identifying cybersecurity solutions that can help organizations of all sizes better navigate the cybersecurity marketplace. The designation of Cyber Catalyst is awarded to cybersecurity solutions that participating insurers believe can have a meaningful impact in assisting organizations in combating cyberattacks. The insurers, Allianz, AXA, AXA XL, Beazley, CFC, Munich-Re, Sompo International and Zurich North America, conduct a comprehensive vetting of submitted products and services, including technology advice from Microsoft, to determine a product’s worthiness of the designation. https://www.marsh.com/us/campaigns/cyber-catalyst-by-marsh.html
Introducing EnergyDefender

EnergyDefender is unlike any other SCADA cyber integrity system on the market today. It is a distributed sensor-based system that analyzes substation assets using a multi-axis approach, collects independent telemetry and provides intervention solutions to defend and recover from a cyberattack. EnergyDefender’s vector analysis components run concurrently to assess cyber emissions, binary integrity, device configuration and power telemetry consistency in conjunction with protocol and traffic analysis. The results are united through a probable cause, threat-reasoning engine that provides guidance on malicious scenarios.

A unique feature of EnergyDefender is its dual user interface to best support the different needs of information technology and operations technology personnel. EnergyDefender’s NOC / SOC-oriented interface provides a real-time, key indicator dashboard, communications sessions mapping, IP device role identification, anomaly and control operation alerts and malicious scenario hypotheses familiar to information technology cybersecurity staff. EnergyDefender’s unique Asset Readiness human-machine interface (HMI) is built upon a one-line diagram familiar to system operators and protection system engineers and provides OT-level scan and intervention actions. It corroborates multiple sources of telemetry, not just the EMS reported telemetry, to provide a best estimate of the energy state of buses and feeders, identifying inconsistencies and misreporting devices. It analyzes relay and RTU point values extracted from SCADA traffic, substation secondary telemetry, distribution feeder state detected by SecureSmart advanced metering infrastructure (AMI) / distribution automation (DA) field probes and the AMI outage detection system. It applies advanced grid state analysis using grid physics, Bayesian inferencing techniques and circuit logic deduction to identify power inconsistencies and misreporting relays, controllers and RTUs.

Through EnergyDefender’s Asset Readiness HMI, system operators are provided with a suite of active scan diagnostics and recovery tools to inspect the binary integrity of relays and Linux- and Windows-based RTUs and relays, validate and compare relay configurations, perform a reasonable engineering analysis on relay settings independent of the configuration of record and issue relay commands and emergency control operations from a central interface. EnergyDefender performs novel, passive cyber emission analysis of control systems RF and side-channel emanations from protection systems and applies machine learning to determine if processor code execution has changed from known baselines to detect the presence of malware.

EnergyDefender’s built-in intervention capabilities enable critical infrastructure operators to respond to an active cyberattack. EnergyDefender’s sensors perform double duty by coming online in an on-demand fashion to replace a damaged substation RTU and perform energy layer traffic intervention under the control of operators. For software-defined network and preconfigured substation deployments, EnergyDefender’s intervention solutions are installed remotely without substation dispatch. Other EnergyDefender capabilities include automated point map validation, live traffic viewing, a traffic capture repository and a telemetry historian.
Technology components

Below are short briefs about the Jolt, cyber emission monitor, reasonable engineering analyzer, relay binary integrity analyzer, RTU surrogate and active defense components of EnergyDefender.

Jolt grid state cyber analyzer

The EnergyDefender Jolt module is a grid state analyzer that localizes controllers compromised by sophisticated cyberattacks by examining inconsistencies in component data reported by relays, RTUs and control system devices. Jolt passively extracts grid state information from the control center and substation telemetry and applies the constraints of a physical energy model with inferencing technology and deductive reasoning to detect telemetry inconsistencies and misreporting devices. Unlike a traditional information technology intrusion monitoring system, Jolt interprets the energy measurements in Distributed Network Protocol 3 (DNP3) / IP, DNP3 / Serial and IEC 61850 generic object-oriented substation events (GOOSE) traffic. It also correlates multiple sources of telemetry besides SCADA, including direct relay metering, SecureSmart AMI / DA probe telemetry, AMI outage detection and substation secondary telemetry sources.

Scenario 4: Deceptive RTAC with OOB reporting + SecureSmart in substation

Second SecureSmart probe deployed
Additional measurement flows are probed

Figure 3: EnergyDefender OT scan HMI

Figure 4: Example Jolt dashboard
Cyber integrity in SCADA systems

Cyber emissions monitor

The cyber emissions monitor component is a highly portable, anomaly detection system that can assess the integrity and operational state of protection system equipment based on nonintrusive monitoring of device radio frequency (RF) emissions in a substation and other industrial control systems. All electronic processors produce unintended side effects such as power consumption, electromagnetic leakage and sound. Our solution analyzes and correlates these side effects with device behavior to determine if a device is operating normally or if it has been compromised. To view a video demonstration of the cyber emissions monitor, visit https://www.perspectalabs.com/critical-infrastructure.

Relay reasonable engineering analyzer

The relay reasonable engineering analyzer is an automated tool that assesses the integrity of relay configurations against malicious changes to their protective functions and configuration error. It acquires the running configuration on a relay and performs six classes of analysis beginning with a gold or default configuration comparison. The tool performs an independent analysis on protective controls settings, point maps, deadbands and scaling, common current transformer ratio / potential transformer ratio engineering values, settings combinations, minimum protective functions, logical inconsistencies and control equation expression analysis. It details, classifies and compares inconsistencies against available baselines and provides guidance to assess and correct each one. The relay reasonable engineering analyzer also performs relay-to-relay configuration comparisons.

Relay binary integrity analyzer

The EnergyDefender relay binary integrity analyzer is an automated tool that assesses the integrity of relays by interrogating the relay using CAL level commands and special techniques. The tool offers both a “lite” and a “deep” scan level. The lite scan checks running program integrity and memory while the deep scan checks for persistent threats in FLASH memory and the bootloader. For some relays, the relay binary integrity analyzer can also create and install firmware images remotely over an Ethernet interface, without requiring direct access to front panel serial ports. Examples of checks include running thread analysis, vector table analysis, command table analysis, program and data integrity analysis, and “blank” memory analysis.

RTU surrogate intervention

The RTU surrogate is a cyber-monitoring, sensor-based solution that performs double duty as a monitoring sensor and a surrogate substation. It provides the option to turn a cybersecurity sensor into an emergency RTU function. The RTU surrogate can come online to perform the functions of a substation RTU in cases where a secondary or emergency RTU function is needed to replace an unrecoverable RTU or when an RTU will take an extended time to recover. It also responds when RTU replacements are not available (e.g., a large-scale cyberattack). Combined with our software defined networking technology, the RTU surrogate can be installed without a substation dispatch.
Active defense intervention

EnergyDefender’s active defense component is a traffic intervention solution that protects “cleaned” substation assets or isolates suspect assets that cannot be taken out of service. Active defense drops / prevents delivery of traffic that is deemed malicious or traffic that warrants additional authorization controls (e.g., control operations, breaker open / breaker close). When implemented as a cyber monitoring, sensor-based solution with software defined networking, active defense can be installed between any substation assets without dispatch.

Critical infrastructure operator evaluation

Various utilities are planning 2021 pilot projects of select EnergyDefender technologies. Participating utilities will deploy EnergyDefender within their energy infrastructure to evaluate the technology efficacy, business benefits and risk reduction opportunity to meet their specific organizational needs.

The EnergyDefender technology pilot projects involve participants and stakeholders representing utility energy management systems, system operations, protection engineering, security operations and cybersecurity. Objectives for the pilots are:

- Validate EnergyDefender cyber integrity technology and its efficacy in the utility’s environment
- Evaluate the quality and value of cyber analytic data generated by EnergyDefender and determine how best to integrate it with the existing utility cyber monitoring solutions
- Understand the EnergyDefender technologies strengths for application to the utility’s transmission / distribution substations
- Formulate a best mode of deployment within selected substations (e.g., instrumenting all equipment or substation feeder relays) based on pilot results, benefits and cost factors
- Evaluate both fixed and portable solutions to support continuous monitoring and ad-hoc security team field analysis
- Identify solution compliance and policy challenges for deployment within the different utility policy-controlled SCADA segments
- Identify the system installation requirements in substations
- Identify which EnergyDefender components utilities have the most interest in potentially deploying
- Evaluate different monitoring hardware configurations to assess benefit-to-cost tradeoffs
- Assess overall solution cost and value, and plan next steps for a broader deployment as appropriate

The EnergyDefender technology pilots will also help determine whether the system introspection enabled by this solution is well-suited for performance by the utility’s staff, and if so, which work groups / organizations should access, manage and control the technology. The pilots may establish that separate components of the technology should be distributed among information technology and operations technology groups. The pilots will likely stimulate discussion on the need for a new cybersecurity role within the energy management center that could support energy operation decision-making by informing operators on the integrity state of assets.

EnergyDefender pilot scenario

A three-phase EnergyDefender technology pilot and deployment scenario is envisioned for most utilities. Phase one will involve two instrumented substations, each with approximately 15 monitored devices of common relay models used in transmission and distribution substations. For the cyber emissions monitor component, two different sensor hardware platforms—one in each of the instrumented substations—will be evaluated for cost-benefit and performance analysis. In addition, a mobile EnergyDefender field analysis kit will be provided to the utility’s security operations to supplement existing cyber analysis and forensics capabilities. The timeline for phase one is estimated to be six months and will include two months for preparation, equipment acquisition, stakeholder coordination, installation and system turn-up, three months of active asset monitoring and one month for post-pilot analysis.

Assuming the phase one results are favorable, the EnergyDefender technology will then be deployed to three additional substations for phase two (currently planned for late 2021) using the selected emission hardware platform. At the same time, a project and budget plan will be submitted to cover the remaining medium impact substations in 2022 as a phase three activity.
Conclusion

Perspecta Labs’ innovative EnergyDefender solution effectively reduces utility operations technology risks. EnergyDefender helps critical infrastructure operators answer the questions, “Can I trust my control system today?” and “What evidence do I have to affirm the trust I place in the system?” By measuring cyber integrity of critical infrastructure assets through “non-transmission control protocol (TCP) channels” and performing analysis in an evidence-based manner, EnergyDefender’s technologies enable a utility operator to challenge and establish their confidence in the cyber integrity of the utility control system on a daily basis—rather than assume the system is trustworthy until an event proves otherwise.

EnergyDefender’s capabilities encourage questions and stimulate discussion about how this technology can be deployed, what groups / organizations within a utility should have access and control of it and whether cybersecurity should have a role in day-to-day system operations within the energy command center. These crucial topics are being explored in our pilot projects.

Contact us to learn more about the 2021 Perspecta Labs EnergyDefender technology pilots or to learn more about cyber integrity in SCADA systems.