EnergyDefender

Comprehensive critical infrastructure and industrial control systems defense

EnergyDefender from Perspecta Labs, part of the SecureSmart™ critical infrastructure solution line, is a critical infrastructure and industrial control system (ICS) defense tool used to detect, troubleshoot and remediate supervisory control and data acquisition (SCADA) systems and telecom issues before system operations are impacted. By blending continuous monitoring, cybersecurity and secondary operations systems into a single solution, EnergyDefender enables operators to monitor the cyber health, performance and trustworthiness of energy management system (EMS) and SCADA systems and continue operations if primary system telemetry is interrupted.

Key benefits:

- Detects, diagnoses and troubleshoots problems in SCADA, distribution automation (DA) and advanced metering infrastructure (AMI) field systems to provide daily operations benefit
- Improves system operation, optimizes communication performance and increases availability
- Corroborates various sources of telemetry to identify inconsistencies and perform anomaly root cause analysis for cybersecurity
- Enables emergency operations when primary SCADA and EMS are down
- Defends utilities against sophisticated protective relay, remote terminal unit (RTU) and automation controller cyberattacks
- Provides powerful capabilities beyond vendor tools for an effective response/recovery from targeted ICS cyberattacks

How EnergyDefender works

SecureSmart's EnergyDefender deploys patented sensors in traditional control networks and wireless field networks to passively intercept control traffic and generate independent ground-truth telemetry. Intelligent applications can perform deep-packet analysis, time series traffic analysis, protocol and session state analysis, endpoint behavioral analysis, and telemetry consistency analysis of multiple traffic streams from physical to application layers.

Perspecta Labs employs artificial intelligence approaches based on probabilistic reasoning in its grid state inferencing capability for power and black-start recovery modeling with root cause analysis. Employing Bayesian Network techniques, combined with grid physics models, EnergyDefender is able to account for partial information and incomplete power grid sensing to capture the effects of cyber causes of outages. A secondary human-machine interface provides independent present-state conditions based on independent telemetry sensors and consistency analysis to facilitate utility decision-making even when EMS or primary telemetry is unavailable.

SecureSmart: A Cyber Catalyst solution

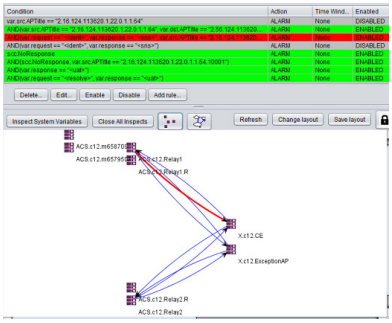
The SecureSmart critical infrastructure solution line has been designated a 2019 Cyber Catalyst solution for cyber risk reduction and efficiency. The Cyber Catalyst by Marsh℠ program is designed to help organizations make well informed decisions about cybersecurity products and services to manage their cyber risk. The SecureSmart critical infrastructure solution line is a collection of industry-changing technologies that help defend critical infrastructure and smart energy systems with comprehensive integrated operations, engineering, security monitoring, anomaly detection, protection, analysis and troubleshooting capabilities for EMS, SCADA systems, and AMI and DA field networks.

perspecta LABS

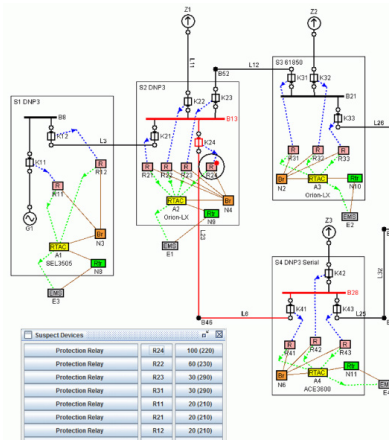
securesmart™

perspecta LABS

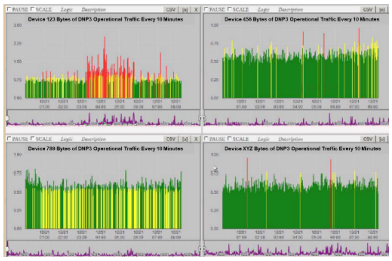
secure**smart**



SCADA monitoring and anomaly detection dashboard



Detecting deceptive real-time automation controller with out-of-band reporting



Example TrafficProfiler time series SCADA indicators

This research was developed with funding from the Defense Advanced Research Projects Agency (DARPA). The views, opinions and/or findings expressed are those of the author and should not be interpreted as representing the official views or policies of the Department of Defense or the U.S. Government.

Key monitoring and analysis features

- Real-time key performance indicator and asset readiness dashboards monitor primary telemetry and asset integrity
- Traffic and protocol analysis tracks EMS/SCADA communications sessions and detects irregularities to uncover hidden problems, misreporting and configuration errors
- Advanced grid state analysis technology detects inconsistencies in real-time energy measurements via Bayesian Inferencing and circuit logic deduction logic and performs automated telemetry reconciliation across multiple controllers and substations
- Remote automated binary integrity and configuration scanning technology evaluates and attests to the integrity of protection system relays and RTUs
- Remote automated point map validation and RTU point translation analysis technology evaluates and attests to end-to-end DNP3 control element reporting
- Continuous SCADA traffic capture and a historical traffic repository enable troubleshooting, system tuning and forensics similar to an energy historian

Key intervention features

- A relay recovery kit for emergency recovery of severely damaged relays and supply chain attacks
- Binary forensics analysis capabilities to perform code analysis on RTUs and protection relay firmware
- Novel RTU surrogate technology provides secondary or emergency RTU functions to replace primary RTUs that have failed or been maliciously disabled

A utility risk mitigation solution

SecureSmart's EnergyDefender solution mitigates cybersecurity, power reliability and business risks of:

- Security and configuration flaws in the wireless, software, network and hardware components of field operations technology
- Loss of primary telemetry and reversion to emergency operation
- Unauthorized control of cyber-physical assets that could result in safety and physical consequence
- Compromise of personally identifiable information and privacy data
- Operator revenue loss and theft of service
- Cybersecurity-triggered service outages that might result in regulatory fines and reputation harm
- Ransomware attacks
- Unauthorized use of operator assets and networks for illegal activities, crime, and terrorism
- Severely damaged protection systems resulting from a cyberattack

To learn more, visit perspectalabs.com/critical-infrastructure

perspectalabs.com | info@perspectalabs.com
150 Mount Airy Road
Basking Ridge, NJ 07920