CYBER INTEGRITY IN SCADA SYSTEMS

ENERGY DEFENDER™ BY PERATON LABS - THE INDUSTRY’S MOST SOPHISTICATED MULTI-AXIS CYBER INTEGRITY AND RECOVERY SOLUTION FOR REAL-TIME SCADA SYSTEMS

Peraton | LABS

REAL-TIME CYBER RISK FACED 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, such as electric utilities, to recognize an underlying, persistent cyber and reliability risk with their feeder, bus, and transformer protection systems in 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. Their construction - hardware architectures and real-time operating systems - are largely not supported by traditional information technology (IT) cybersecurity defensive tools and scanning agents. Serial substations and serial wide area networks (WAN) are inaccessible to all IT monitoring solutions, As high value equipment targets critical to energy delivery operations, their inaccessibility creates significant risk. To mitigate the risk, many operators will resort to staffed substations in case of a major incident that takes out the wide area SCADA network. However, this action is ineffective if the protective systems within the substation have been compromised by a cyberattack.

The problem facing critical infrastructure operators is how to assess the cyber trustworthiness of real-time protective relays, RTUs, and real-time automation controllers (RTAC) on regular basis. EnergyDefender provides utilities with a way to monitor their serial substations, all the communication between relays and RTUs/RTACs, and between RTUs and the Emergency Manager System (EMS) so there are no more serial blind spots. Existing cyber monitoring 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.

INNOVATIVE TECHNOLOGY REDUCES RISK OF CYBER ATTACKS THAT COMPROMISE SCADA INTEGRITY

Peraton Labs' SecureSmart™ EnergyDefender™ solution provides innovative technologies to assess the cyber trustworthiness of real-time SCADA assets by introducing "non-Transmission Control Protocol (TCP)" channel sources to deliver timely, concrete, and objective evidence to attest to cyber integrity. EnergyDefender uses 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 to support of defensive cyber operations and hunt cyber-weapons in SCADA environments.

SecureSmart EnergyDefender was developed by Peraton 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, Peraton Labs' SecureSmart solution has been designated an inaugural Cyber Catalyst[1] technology by the eight largest providers of cyber insurance. Critical infrastructure

[1] 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 combatting cyberattacks. The insurers, Allianz, Axis, AXA XL, Beazley, CFC, Munich Re, Sompo International and Zurich North America, conduct a comprehensive vetting of submitted products and services,

operators may receive an insurance benefit by deploying Cyber Catalyst designated solutions in their infrastructure to enhance their overall power grid resilience posture.

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. It 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.

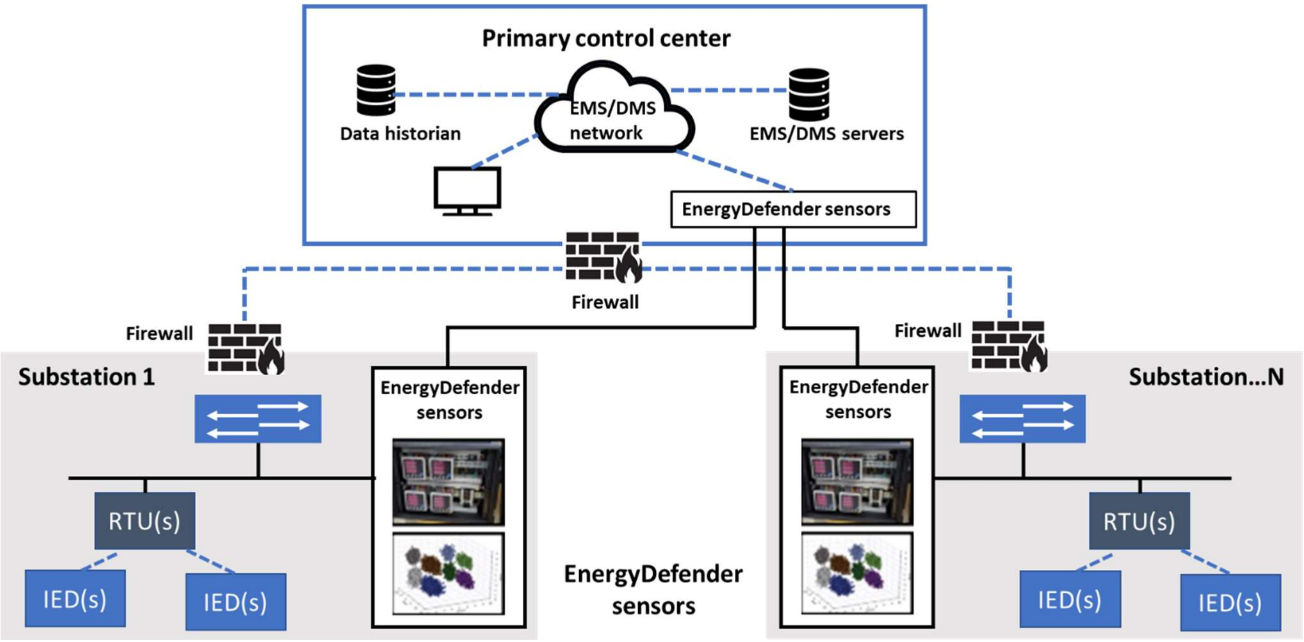


Figure 1: EnergyDefender high level architecture

A unique feature of EnergyDefender is its twin user interface to support the needs of both IT and operations technology (OT) personnel. EnergyDefender's Network Operations Center (NOC) / Service Operations Center (SOC)-oriented interface provides a real-time, key indicator dashboard, communications sessions mapping, Internet Protocol (IP) device role identification, anomaly and control operation alerts and malicious scenario hypotheses familiar to IT 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.

including technology advice from Microsoft, to determine a product's worthiness of the designation. Marsh Reveals Inaugural Class of Cyber Catalyst Designated Solutions.

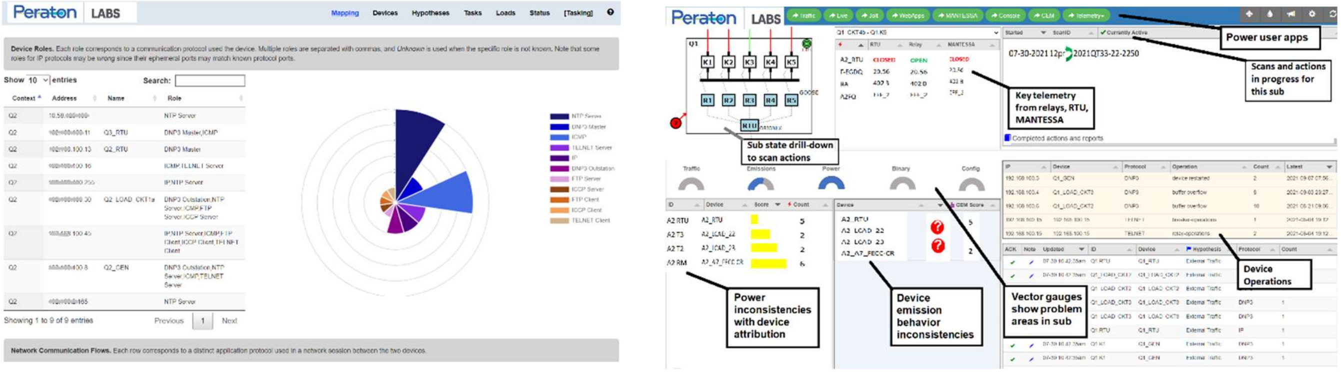
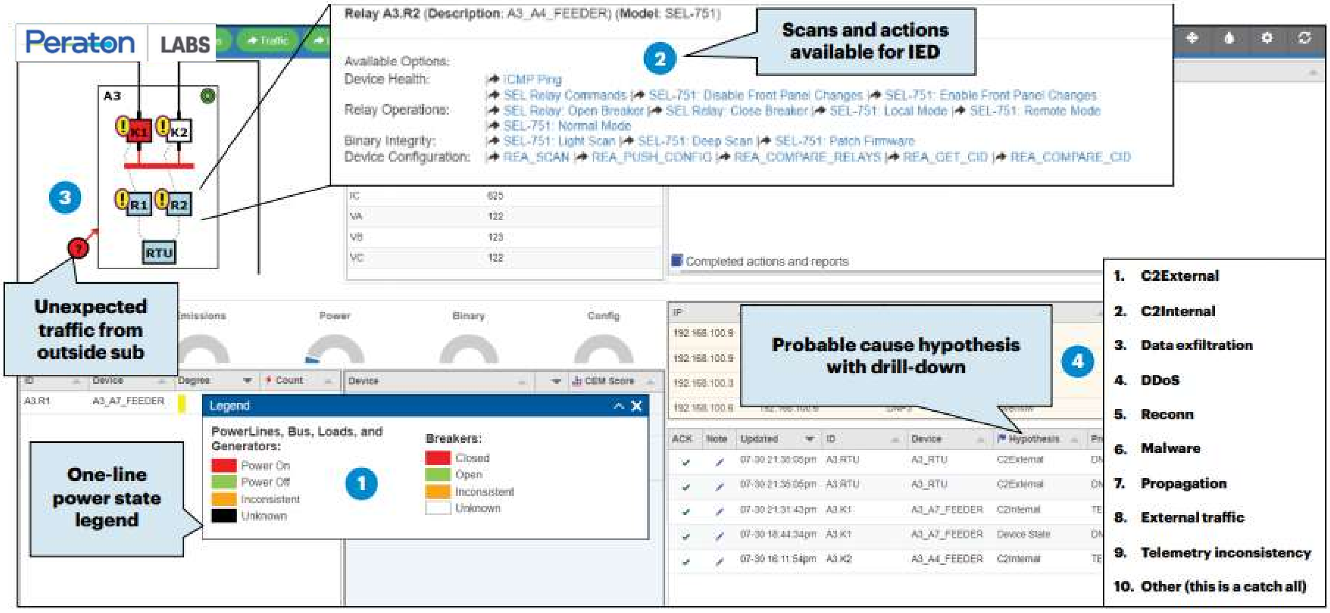

Peraton LABS
Mapping
Devices
Hypotheses
Tasks
Loads
Status
[Tasking]
Power user apps
Scans and actions in progress for this sub
Key telemetry from relays, RTU, MANTESSA
Sub state drill-down to scan actions
Device Operations
Vector gauges show problem areas in sub
Power inconsistencies with device attribution
Device emission behavior inconsistencies
Traffic
Emissions
Power
Binary
Config

Figure 2: EnergyDefender IT and OT HMI Interfaces

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 sidechannel 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.


Peraton LABS
Traffic
A3
K1
K2
R1
R2
RTU
3
Unexpected traffic from outside sub
2
Scans and actions available for IED
1
One-line power state legend
4
Probable cause hypothesis with drill-down
Emissions
Power
Binary
Config
Completed actions and reports

Relay A3.R2 (Description: A3_A4_FEEDER) (Model: SEL-751)

Available Options:
Device Health: ICMP Ping
SEL Relay Commands | SEL-751: Disable Front Panel Changes | SEL-751: Enable Front Panel Changes
Relay Operations: SEL Relay: Open Breaker | SEL Relay: Close Breaker | SEL-751: Local Mode | SEL-751: Remote Mode
SEL-751: Normal Mode
Binary Integrity: SEL-751: Light Scan | SEL-751: Deep Scan | SEL-751: Patch Firmware
Device Configuration: REA_SCAN | REA_PUSH_CONFIG | REA_COMPARE_RELAYS | REA_GET_CID | REA_COMPARE_CID

IC	625
VA	122
VB	123
VC	122

Legend

PowerLines, Bus, Loads, and Generators:
🟥 Power On
🟩 Power Off
🟧 Inconsistent
⬛ Unknown

Breakers:
🟥 Closed
🟩 Open
🟧 Inconsistent
⬜ Unknown

ACK	Note	Updated	ID	Device	Hypothesis
✓	✎	07-30 21:36:05pm	A3.RTU	A3_RTU	C2External
✓	✎	07-30 21:36:05pm	A3.RTU	A3_RTU	C2External
✓	✎	07-30 21:31:43pm	A3.K1	A3_A7_FEEDER	C2Internal
✓	✎	07-30 18:44:34pm	A3.K1	A3_A7_FEEDER	Device State
✓	✎	07-30 16:11:54pm	A3.K2	A3_A4_FEEDER	C2Internal

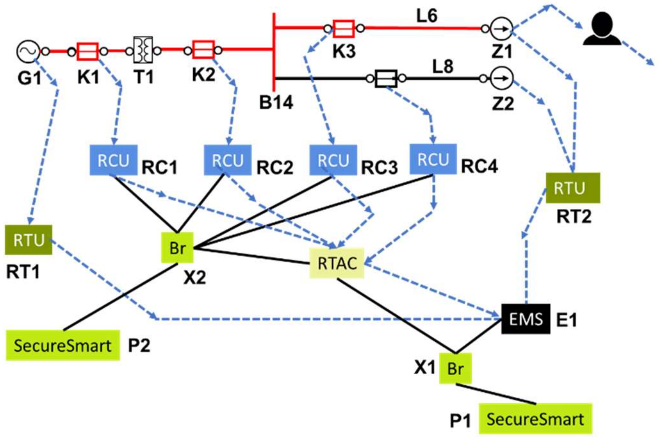
1. C2External
2. C2Internal
3. Data exfiltration
4. DDoS
5. Recon
6. Malware
7. Propagation
8. External traffic
9. Telemetry inconsistency
10. Other (this is a catch all)

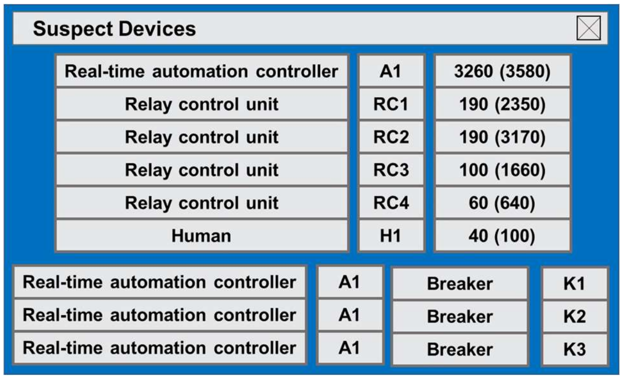
Figure 3: EnergyDefender OT scan HMI

TECHNOLOGY COMPONENTS

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.




Suspect Devices

Real-time automation controller	A1	3260 (3580)
Relay control unit	RC1	190 (2350)
Relay control unit	RC2	190 (3170)
Relay control unit	RC3	100 (1660)
Relay control unit	RC4	60 (640)
Human	H1	40 (100)

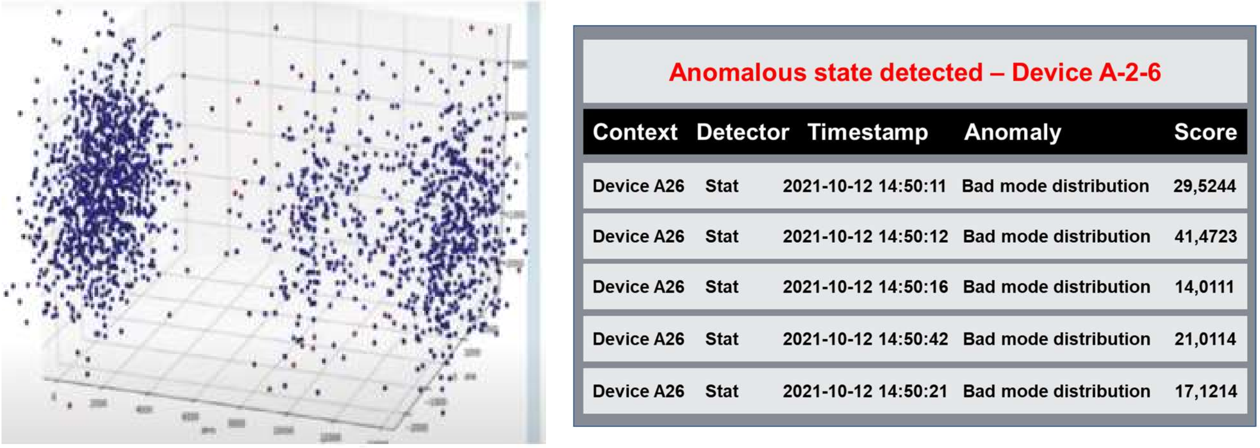
Real-time automation controller	A1	Breaker	K1
Real-time automation controller	A1	Breaker	K2
Real-time automation controller	A1	Breaker	K3

Figure 4a: Deceptive RTAC with OOB reporting and SecureSmart in substation

Figure 4b: Example Jolt dashboard

CYBER EMISSIONS MONITOR

The cyber emissions monitor component is a non-intrusive, side channel anomaly detection system that assesses the integrity and operational state of protection system equipment based on monitoring of device radio frequency (RF) emissions. All electronic processors produce unintended emanations during normal operation, such as power fluctuations, electromagnetic leakage and sound. The cyber emissions monitor models the emanations using sophisticated signal processing and machine learning 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 CEMA - Peraton Labs .



Anomalous state detected – Device A-2-6

Context	Detector	Timestamp	Anomaly	Score
Device A26	Stat	2021-10-12 14:50:11	Bad mode distribution	29,5244
Device A26	Stat	2021-10-12 14:50:12	Bad mode distribution	41,4723
Device A26	Stat	2021-10-12 14:50:16	Bad mode distribution	14,0111
Device A26	Stat	2021-10-12 14:50:42	Bad mode distribution	21,0114
Device A26	Stat	2021-10-12 14:50:21	Bad mode distribution	17,1214

Figure 5: Example cyber emissions monitor dashboard

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 inconsistences 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.

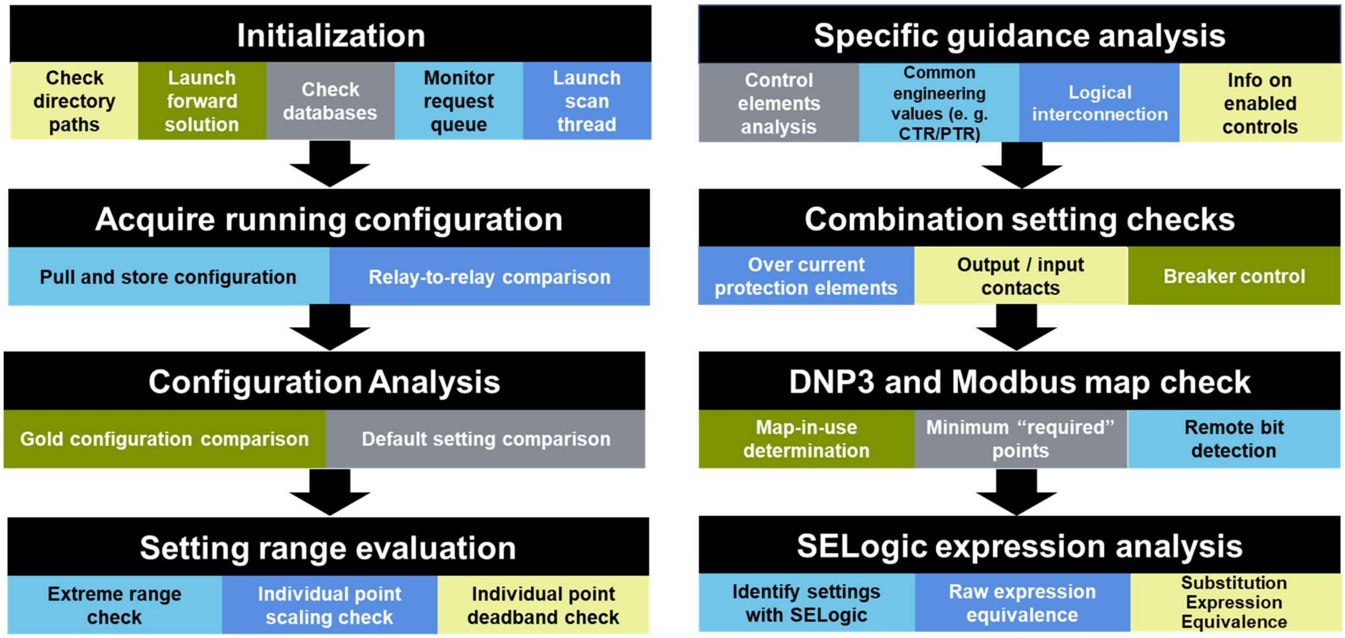

Initialization
Check directory paths
Launch forward solution
Check databases
Monitor request queue
Launch scan thread
Acquire running configuration
Pull and store configuration
Relay-to-relay comparison
Configuration Analysis
Gold configuration comparison
Default setting comparison
Setting range evaluation
Extreme range check
Individual point scaling check
Individual point deadband check
Specific guidance analysis
Control elements analysis
Common engineering values (e. g. CTR/PTR)
Logical interconnection
Info on enabled controls
Combination setting checks
Over current protection elements
Output / input contacts
Breaker control
DNP3 and Modbus map check
Map-in-use determination
Minimum "required" points
Remote bit detection
SELogic expression analysis
Identify settings with SELogic
Raw expression equivalence
Substitution Expression Equivalence

Figure 6: Relay reasonable engineering analyzer flow

RELAY BINARY INTEGRITY ANALYZER

The EnergyDefender relay binary integrity analyzer is an automated tool that assesses the integrity of relays by interrogating the relay memory using manufacturer commands. 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

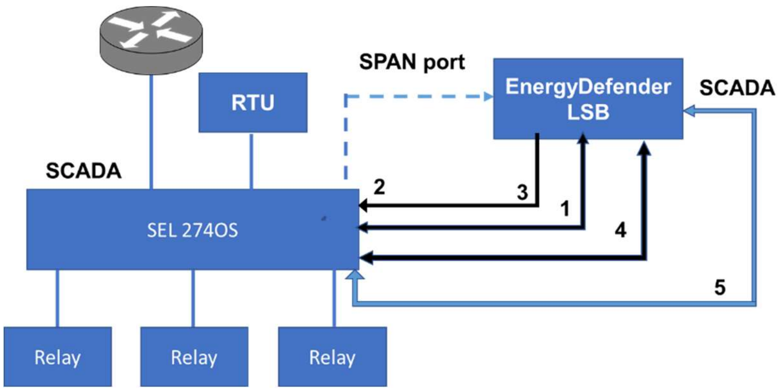


Figure 7: RTU Surrogate and Active Defense

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

EnergyDefender technologies have been deployed by utilities within their energy infrastructure for cybersecurity protection and as an operations troubleshooting and service assurance solution. EnergyDefender technology pilot projects and operational trials to trials to evaluate technology efficacy, business benefits and risk reduction involve participants and stakeholders representing utility energy management systems, system operations, protection engineering, security operations and cybersecurity. These operational pilot projects have validated EnergyDefender’s efficacy in utility environments and demonstrated its capabilities to:

- Deliver accurate, real-time assessments of ICS cybersecurity trustworthiness and asset readiness
- Unify analysis of traffic, power, binary integrity, configuration and device emanations with malicious scenario reasoning
- Provide emergency SCADA situational awareness and SCADA intervention solutions for recovery

- Support daily operations, reduce risk and provide service and system recovery capability for defensive cyber operations

The operational trials have also provided useful insight and information on options and approaches to integrate EnergyDefender in utility environments and with existing utility cyber monitoring solutions, including:

- Comparing different modes of deployment within selected substations (e.g., instrumenting all equipment or substation feeder relays)
- Evaluating both fixed and portable solutions for continuous monitoring and ad-hoc security team field analysis
- Identifying solution compliance and policy challenges for deployment within the different utility policy-controlled SCADA segments
- Determining the system installation requirements in substations

TAKE THE NEXT STEP WITH AN ENERGY DEFENDER PILOT

Utility SCADA systems are under constant threat of devasting cyberattacks. Current solutions cannot defend the full attack surface, leaving this critical infrastructure highly vulnerable. EnergyDefender provides cyber integrity for SCADA systems with active defense and demonstrated value in operational utility networks. Take the next step to protect your SCADA cyber integrity with an EnergyDefender pilot. The typical pilot scenario is a six-month effort, comprising 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. Two substations would be instrumented, 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 is provided to the utility's security operations to supplement existing cyber analysis and forensics capabilities.

CONCLUSION

Peraton 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 Peraton Labs EnergyDefender technology and our service offerings for cyber integrity in SCADA systems.

Peraton | LABS

LEARN MORE AT

PERATONLABS.COM

150 Mount Airy Road
Basking Ridge, NJ 07920