SECURESMART™ APPLICATIONS FOR DISTRIBUTION AUTOMATION

CYBERSECURITY AND OPERATIONS MONITORING

Distribution Automation (DA) and Supervisory Control and Data Acquisition (SCADA) Field Area Networks (FANs) are a large part of utilities' Smart Grid infrastructure, supporting a more automated, intelligent, reliable, and flexible grid. These networks present unique operational and cybersecurity challenges. Peraton Labs innovated its novel SecureSmart™ monitoring solution to provide packet-level visibility and analysis that detects the unforeseen, unanticipated, and unexpected - those "That shouldn't be!" cases unseen by DA vendor management systems. SecureSmart provides high-value applications for real-time performance monitoring, troubleshooting, and cybersecurity analysis to help utilities realize their corporate availability and reliability goals and manage their DA networks to a performance standard. SecureSmart enables root cause analysis of mis-operations with reduced time to resolution, eliminates unnecessary truck rolls, and enables service level assurance management while getting the benefit of the industry's best field FAN cybersecurity intrusion detection solution.

Peraton | LABS

SECURESMART™ SOLUTON FOR DISTRIBUTION AUTOMATION

Peraton Labs' novel SecureSmart™ monitoring solution provides packet-level visibility and traffic analysis to detect the unforeseen, unanticipated, and unexpected in Smart Grid advanced control and communication technologies.

SecureSmart delivers actionable traffic-level insight into connectivity problems and misbehaving, malfunctioning, or misconfigured nodes, which are invisible to vendor management systems. Peraton Labs' SecureSmart is a full-packet capture and analysis system with advanced applications to troubleshoot field problems, conduct forensics on mis-operations, and continuously monitor the performance, operation, cybersecurity, and health of a utility's Distribution Automation (DA) infrastructure.

SecureSmart has been successfully deployed to improve the reliability and troubleshooting of Advanced Distribution Management Systems (ADMS) with wireless distribution automation field components that include reclosers, capacitor banks, motor-operated switches, and voltage regulators. SecureSmart has also been used to conduct field analysis of synchronizing events such as power outages and the mass startup impact on DA Automatic Sectionalizing and Restoration (ASR) and teaming systems.

SECURESMART APPLICATIONS

SecureSmart is a sensor-based system that passively intercepts and analyzes DA, SCADA, and wireless FAN network traffic depending upon the location and type of sensors deployed. When deployed with a backend network sensor, SecureSmart can intercept unencrypted Distributed Network Protocol 3 (DNP3) traffic as well as the encrypted tunnel and supporting routing traffic across the entire DA infrastructure. When deployed with field sensors, SecureSmart can intercept wireless traffic in the FAN that contains over-the-air SCADA and management communications with energy controllers, peer-to-peer controller communications for teaming applications, and mesh network routing and network maintenance traffic.

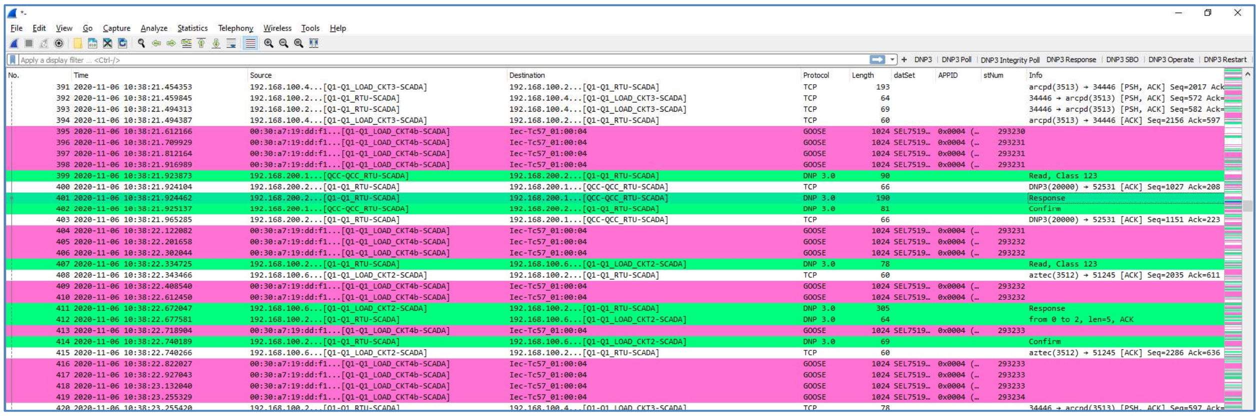
Both solutions are offered as a product and service solution with either on-premises or hosted application components to analyze intercepted traffic. For on-premises implementations, SecureSmart applications can be deployed as a Virtual Machine on an existing customer platform with a user desktop providing icon-based application access via remote desktop connection or a Web browser. In hosted application deployments, users access the SecureSmart applications via a service portal over a virtual private network connection.

SecureSmart applications consist of:

- ProbeLive FAN Packet Analyzer with live traffic feeds,
- TrafficProfiler Time Series Analyzer with Capture Repository,
- ProtocolPatroller Protocol and Communication Session Analyzer,
- MeshView Network Analytics,
- GridGuard Intrusion Detection System, and
- Jolt Telemetry Analyzer.

ProbeLive

The ProbeLive application provides real-time viewing and inspection of live traffic and historical traffic trace files. The underlying packet capture system continuously captures and stores full packets from each sensor. Each packet stream is sliced and stored in the convenient pcap file format in a directory structure. The duration of the packet capture files is configurable for each tap to create file sizes that are convenient to open and process in a packet analyzer application without scanning delays. Typical file durations that Peraton Labs used in DA monitoring applications are one to five minutes. Multiple files can be easily merged if a single large file is desired. The simplicity of the basic packet capture system translates into capture speed and reliability.


*-
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
+ DNP3 | DNP3 Poll | DNP3 Integrity Poll | DNP3 Response | DNP3 SBO | DNP3 Operate | DNP3 Restart

No.	Time	Source	Destination	Protocol	Length	datSet	APPID	stNum	Info
391	2020-11-06 10:38:21.454353	192.168.100.4...[Q1-Q1_LOAD_CKT3-SCADA]	192.168.100.2...[Q1-Q1_RTU-SCADA]	TCP	193				arcpd(3513) → 34446 [PSH, ACK] Seq=2017 Ack
392	2020-11-06 10:38:21.459845	192.168.100.2...[Q1-Q1_RTU-SCADA]	192.168.100.4...[Q1-Q1_LOAD_CKT3-SCADA]	TCP	64				34446 → arcpd(3513) [PSH, ACK] Seq=572 Ack=
393	2020-11-06 10:38:21.494313	192.168.100.2...[Q1-Q1_RTU-SCADA]	192.168.100.4...[Q1-Q1_LOAD_CKT3-SCADA]	TCP	69				34446 → arcpd(3513) [PSH, ACK] Seq=582 Ack=
394	2020-11-06 10:38:21.494387	192.168.100.4...[Q1-Q1_LOAD_CKT3-SCADA]	192.168.100.2...[Q1-Q1_RTU-SCADA]	TCP	60				arcpd(3513) → 34446 [ACK] Seq=2156 Ack=597
395	2020-11-06 10:38:21.612166	00:30:a7:19:dd:f1...[Q1-Q1_LOAD_CKT4b-SCADA]	Iec-Tc57_01:00:04	GOOSE	1024	SEL7519…	0x0004 (…	293230	
396	2020-11-06 10:38:21.709929	00:30:a7:19:dd:f1...[Q1-Q1_LOAD_CKT4b-SCADA]	Iec-Tc57_01:00:04	GOOSE	1024	SEL7519…	0x0004 (…	293231	
397	2020-11-06 10:38:21.812164	00:30:a7:19:dd:f1...[Q1-Q1_LOAD_CKT4b-SCADA]	Iec-Tc57_01:00:04	GOOSE	1024	SEL7519…	0x0004 (…	293231	
398	2020-11-06 10:38:21.916989	00:30:a7:19:dd:f1...[Q1-Q1_LOAD_CKT4b-SCADA]	Iec-Tc57_01:00:04	GOOSE	1024	SEL7519…	0x0004 (…	293231	
399	2020-11-06 10:38:21.923873	192.168.200.1...[QCC-QCC_RTU-SCADA]	192.168.200.2...[Q1-Q1_RTU-SCADA]	DNP 3.0	90				Read, Class 123
400	2020-11-06 10:38:21.924104	192.168.200.2...[Q1-Q1_RTU-SCADA]	192.168.200.1...[QCC-QCC_RTU-SCADA]	TCP	66				DNP3(20000) → 52531 [ACK] Seq=1027 Ack=208
401	2020-11-06 10:38:21.924462	192.168.200.2...[Q1-Q1_RTU-SCADA]	192.168.200.1...[QCC-QCC_RTU-SCADA]	DNP 3.0	190				Response
402	2020-11-06 10:38:21.925137	192.168.200.1...[QCC-QCC_RTU-SCADA]	192.168.200.2...[Q1-Q1_RTU-SCADA]	DNP 3.0	81				Confirm
403	2020-11-06 10:38:21.965285	192.168.200.2...[Q1-Q1_RTU-SCADA]	192.168.200.1...[QCC-QCC_RTU-SCADA]	TCP	66				DNP3(20000) → 52531 [ACK] Seq=1151 Ack=223
404	2020-11-06 10:38:22.122082	00:30:a7:19:dd:f1...[Q1-Q1_LOAD_CKT4b-SCADA]	Iec-Tc57_01:00:04	GOOSE	1024	SEL7519…	0x0004 (…	293231	
405	2020-11-06 10:38:22.201658	00:30:a7:19:dd:f1...[Q1-Q1_LOAD_CKT4b-SCADA]	Iec-Tc57_01:00:04	GOOSE	1024	SEL7519…	0x0004 (…	293232	
406	2020-11-06 10:38:22.302044	00:30:a7:19:dd:f1...[Q1-Q1_LOAD_CKT4b-SCADA]	Iec-Tc57_01:00:04	GOOSE	1024	SEL7519…	0x0004 (…	293232	
407	2020-11-06 10:38:22.334725	192.168.100.2...[Q1-Q1_RTU-SCADA]	192.168.100.6...[Q1-Q1_LOAD_CKT2-SCADA]	DNP 3.0	78				Read, Class 123
408	2020-11-06 10:38:22.343466	192.168.100.6...[Q1-Q1_LOAD_CKT2-SCADA]	192.168.100.2...[Q1-Q1_RTU-SCADA]	TCP	60				aztec(3512) → 51245 [ACK] Seq=2035 Ack=611
409	2020-11-06 10:38:22.408540	00:30:a7:19:dd:f1...[Q1-Q1_LOAD_CKT4b-SCADA]	Iec-Tc57_01:00:04	GOOSE	1024	SEL7519…	0x0004 (…	293232	
410	2020-11-06 10:38:22.612450	00:30:a7:19:dd:f1...[Q1-Q1_LOAD_CKT4b-SCADA]	Iec-Tc57_01:00:04	GOOSE	1024	SEL7519…	0x0004 (…	293232	
411	2020-11-06 10:38:22.672047	192.168.100.6...[Q1-Q1_LOAD_CKT2-SCADA]	192.168.100.2...[Q1-Q1_RTU-SCADA]	DNP 3.0	305				Response
412	2020-11-06 10:38:22.677581	192.168.100.2...[Q1-Q1_RTU-SCADA]	192.168.100.6...[Q1-Q1_LOAD_CKT2-SCADA]	DNP 3.0	64				from 0 to 2, len=5, ACK
413	2020-11-06 10:38:22.718904	00:30:a7:19:dd:f1...[Q1-Q1_LOAD_CKT4b-SCADA]	Iec-Tc57_01:00:04	GOOSE	1024	SEL7519…	0x0004 (…	293233	
414	2020-11-06 10:38:22.740189	192.168.100.2...[Q1-Q1_RTU-SCADA]	192.168.100.6...[Q1-Q1_LOAD_CKT2-SCADA]	DNP 3.0	69				Confirm
415	2020-11-06 10:38:22.740266	192.168.100.6...[Q1-Q1_LOAD_CKT2-SCADA]	192.168.100.2...[Q1-Q1_RTU-SCADA]	TCP	60				aztec(3512) → 51245 [ACK] Seq=2286 Ack=636
416	2020-11-06 10:38:22.822027	00:30:a7:19:dd:f1...[Q1-Q1_LOAD_CKT4b-SCADA]	Iec-Tc57_01:00:04	GOOSE	1024	SEL7519…	0x0004 (…	293233	
417	2020-11-06 10:38:22.927043	00:30:a7:19:dd:f1...[Q1-Q1_LOAD_CKT4b-SCADA]	Iec-Tc57_01:00:04	GOOSE	1024	SEL7519…	0x0004 (…	293233	
418	2020-11-06 10:38:23.132040	00:30:a7:19:dd:f1...[Q1-Q1_LOAD_CKT4b-SCADA]	Iec-Tc57_01:00:04	GOOSE	1024	SEL7519…	0x0004 (…	293233	
419	2020-11-06 10:38:23.255329	00:30:a7:19:dd:f1...[Q1-Q1_LOAD_CKT4b-SCADA]	Iec-Tc57_01:00:04	GOOSE	1024	SEL7519…	0x0004 (…	293234	
420	2020-11-06 10:38:23.255420	192.168.100.2...[Q1-Q1_RTU-SCADA]	192.168.100.4...[Q1-Q1_LOAD_CKT3-SCADA]	TCP	78				34446 → arcpd(3513) [PSH, ACK] Seq=597 Ack=

ProbeLive example traffic captures

ProbeLive uses the familiar open-source Wireshark packet analyzer with a custom Peraton Labs SecureSmart profile to view and dissect packets with advanced filtering, TCP stream analysis, and packet statistics. Users launch ProbeLive using icons on the SecureSmart Desktop to view live traffic from selected taps or open packet capture files. Decryption of IPsec traffic is possible if encryption keys are provided. Multiple live views provide the ability to monitor different taps simultaneously. Live packet capture viewing is useful for real-time troubleshooting of connection and session problems to immediately observe the effect of system changes or to monitor the behavior or reaction of devices to a live event. Historical pcap files are retrieved using the TrafficProfiler application.

SecureSmart ProbeLive provides custom Wireshark features to assist in the troubleshooting of DA applications. SecureSmart uses its profile, which defines a specific screen layout with chosen column parameters and set of predefined packet filters, for quick DA protocol analysis. Device names can be appended to source and destination IP addresses for more convenient device identification. SecureSmart further provides a custom capability to dissect the vendor proprietary mesh packet flows between head-end DA systems and mesh endpoints for proprietary protocols. This unique capability helps utilities monitor actual traffic exchanges in the wireless mesh that are not visible from monitoring systems positioned north of the take-out points and collectors.

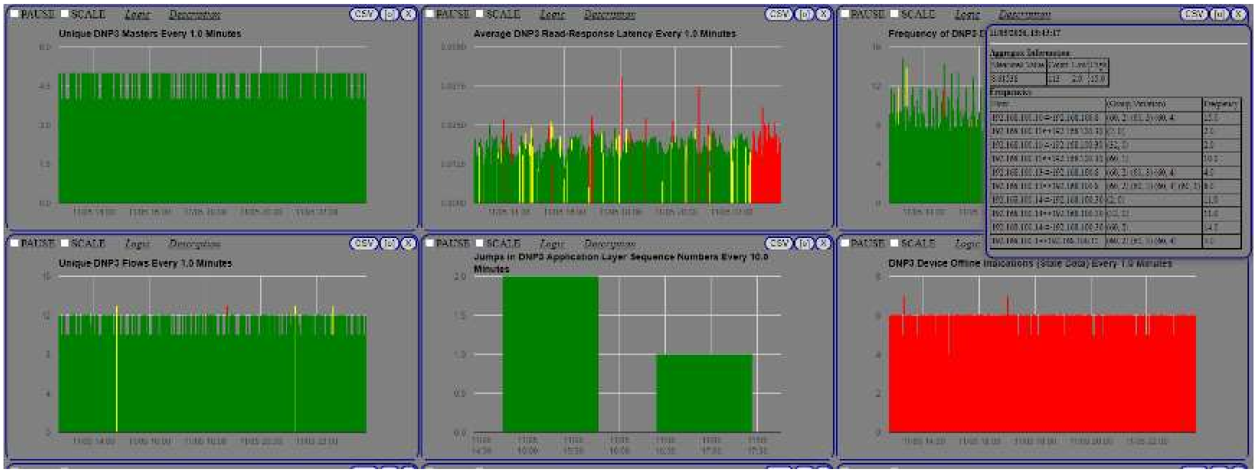
TrafficProfiler

To facilitate faster time to resolution and proactively monitor for signs of network problems before the occurrence of a mis-operation, Peraton Labs' SecureSmart provides its TrafficProfiler time series analyzer. TrafficProfiler is a real-time traffic monitoring tool that analyzes one or more live traffic streams to create a Web-based, multi-level dashboard of health, performance, service assurance, cybersecurity, and anomaly indicators. Complex time series measurements are made using predefined functions populated with regular expressions containing information elements extracted from packets as operands. The time series results are displayed as bar and pie charts. TrafficProfiler indicators can monitor any portion of the protocol stack, even non-IP and proprietary protocols, as long as the underlying protocol analysis function can dissect the traffic. Intelligent selection of TrafficProfiler indicators that have orthogonal range space facilitates root-cause analysis by simply glancing over a few indicators. TrafficProfiler comes preconfigured with a set of indicators that Peraton Labs has found useful to monitor and troubleshoot device and communications problems and to continuously assess the state of system cybersecurity. Indicators and troubleshooting to resolve problems include:

- Identify service-level traffic flow,
- Traffic breakdown by operation,
- Collector/Access Point utilization,

- Job duration traffic,
- Unencrypted traffic,
- TCP resets,
- Device management traffic,
- Troubleshooting FAN congestion after circuit failure,
- Discovering DA cross-utility traffic,
- Identifying field network RF interference,
- Communications round-trip latency,
- DNP3 unusual indications,
- Monitoring storm impacts,
- Identifying excessive FAN device communication hops,
- Visualizing unusually high alerts and/or traps within clustered geographic areas,
- Identifying meters with continual excessive reboots,
- Identifying causes of packet Luck and Time To Live (TTL) expiration,
- Tracing Read Not Received conditions,
- Identifying “Hot Potato” conditions where a packet is exchanged back and forth between devices,
- Identify Collector/Access Point/meter ID mismatches,
- Snap read and read job congestion impacting DA communications,
- Devices holding on to packets – not routing forward,
- Mesh routing mechanism peculiarities,
- Ping job usefulness against a specified set of meters, and much more.

A powerful “hover-over” feature identifies the top devices and values for the time window without need to open the packet capture file.


□ PAUSE
□ SCALE
Logic
Description
CSV
X
Unique DNP3 Masters Every 1.0 Minutes
Average DNP3 Read-Response Latency Every 1.0 Minutes
Frequency of DNP3
Aggregate Information
Frequencies
Unique DNP3 Flows Every 1.0 Minutes
Jumps in DNP3 Application Layer Sequence Numbers Every 10.0 Minutes
DNP3 Device Offline Indications (Stale Data) Every 1.0 Minutes

TrafficProfiler example indicator charts with hover-over details

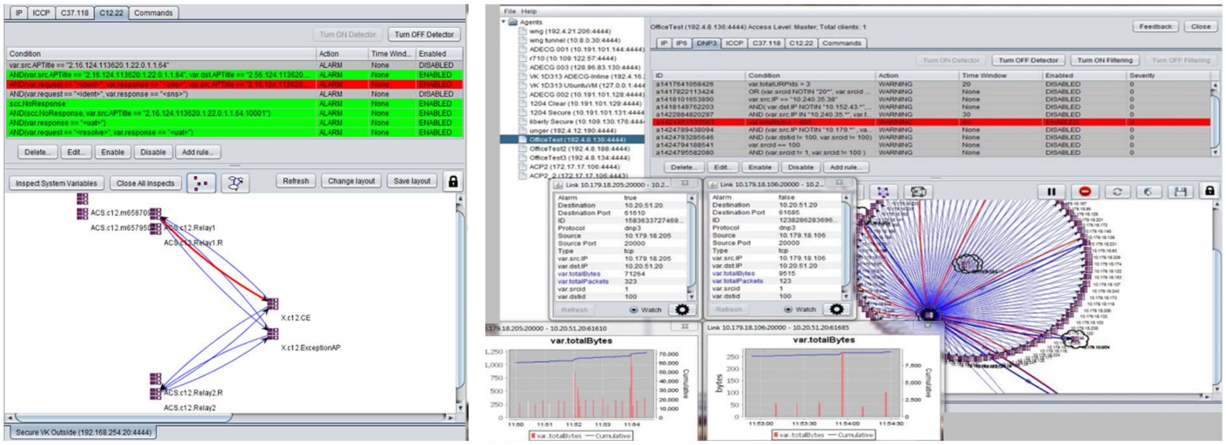
Indicators can be configured to monitor on a system, sensor, group, or individual device basis. Indicators are organized into affinity groups, such as network performance, service assurance, and cybersecurity to support different job functions. For a multiple service network, affinity groups are created to monitor service level performance of each service, such as electric metering, gas metering, water metering, intelligent streetlights, automatic service restoration, reclosers, and capacitor banks. Indicators can be revised or added to enable targeted analysis. A historical indicator database enables quick recall of past indicators. Individual indicator controls enable users to change the time aperture of each indicator chart and scale. Each indicator operates on a separate time base to facilitate measurements on different timescales. The indicator analysis window is configurable and typically set to one minute for DA applications. Multiple users can select and save dashboard layouts with different combinations of indicators for their personal dashboard views. The dashboard will auto-update for continuous Network Operations Center (NOC) / Security Operations Center (SOC) monitoring or to present a static time snapshot.

More than a troubleshooting aid, TrafficProfiler enables utilities to establish and monitor key performance indicators for DA network operation and support minimum service level performance for distribution operations. TrafficProfiler “learns” and establishes baselines for each indicator, or uses predefined thresholds, to alert upon deviation from the established “norm.” Visual alerts are provided using a color-coded sequence. TrafficProfiler can electronically feed alerts to integrate with other systems, such as SIEM, ServiceNow, and email alert systems.

ProtocolPatroller

The Peraton Labs’ SecureSmart ProtocolPatroller real-time protocol and communication session analyzer reduces time to resolution by mapping communication flows and detecting session problems and irregularities. ProtocolPatroller graphically maps communication flows between each endpoint pair and allows inspection at multiple layers within the protocol stack. In the case of DA sessions, each node is labeled by IP address, device name, its DNP3 role, and DNP3 ID. Drilldown capabilities provide detailed information for each session. Unrecognized devices detected in the environment and session links with anomalies are highlighted. Sessions are tracked at layers of the IP stack to discern logical channels using the same IP address pair. For example, ProtocolPatroller will map the TCP communications between an RTU and energy system at the IP level and map the DNP3 master-outstation flows between each DNP3 ID pair. ProtocolPatroller supports energy protocol suites, including DNP3, 61850 GOOSE, Inter-Control Center Protocol (ICCP), C37.118 Synchrophasor, L+G 8065, SEL Fast Message, C12.22, IP, Telnet, and HTTP.

ProtocolPatroller performs deep packet inspection to analyze sessions between each endpoint pair using stateful models and user-defined rules to detect anomalies. When session conditions satisfy the user-defined rules, prescribed actions are taken. In Monitor mode, ProtocolPatroller passively analyzes, detects and alerts on behavior anomalies using a user-defined set of protocol-specific rules and environment parameters. In the optional Protection Mode, ProtocolPatroller actively intervenes according to prescribed actions to mitigate malicious behavior and terminate sessions.



Condition	Action	Time Wind...	Enabled
var.src.APTitle == "2.16.124.113620.1.22.0.1.1.64"	ALARM	None	DISABLED
AND(var.src.APTitle == "2.16.124.113620.1.22.0.1.1.64", var.dst.APTitle == "2.56.124.113620...	ALARM	None	ENABLED
AND(var.request == "<ident>", var.response == "<sns>", var.src.APTitle == "2.16.124.113620...	ALARM	None	ENABLED
AND(var.request == "<ident>", var.response == "<sns>")	ALARM	None	DISABLED
scc.NoResponse	ALARM	None	ENABLED
AND(scc.NoResponse, var.src.APTitle == "2.16.124.113620.1.22.0.1.1.64.10001")	ALARM	None	ENABLED
AND(var.response == "<uat>")	ALARM	None	ENABLED
AND(var.request == "<resolve>", var.response == "<uat>")	ALARM	None	ENABLED

Agents
- wng (192.4.21.206:4444)
- wng tunnel (10.8.0.30:4444)
- ADECG 001 (10.191.101.144:4444)
- r710 (10.109.122.57:4444)
- ADECG 003 (128.96.83.130:4444)
- VK 1D313 ADECG-Inline (192.4.16.
- VK 1D313 UbuntuVM (127.0.0.1:444
- ADECG 002 (10.191.101.128:4444)
- 1204 Clear (10.191.101.129:4444)
- 1204 Secure (10.191.101.131:4444
- liberty Secure (10.109.130.176:444
- unger (192.4.12.190:4444)
- OfficeTest (192.4.8.136:4444)
- OfficeTest2 (192.4.8.188:4444)
- OfficeTest3 (192.4.8.134:4444)
- ACP2 (172.17.17.106:4444)
- ACP2_2 (172.17.17.106:4443)

OfficeTest (192.4.8.136:4444) Access Level: Master; Total clients: 1

ID	Condition	Action	Time Window	Enabled	Severity
a1417641058426	var.totalURPkts > 3	WARNING	20	DISABLED	0
a1417822113424	OR (var.srcid NOTIN "20*", var.srcid ...	WARNING	None	DISABLED	0
a1418101653890	var.src.IP == "10.240.35.38"	WARNING	None	DISABLED	0
a1418149762203	AND(var.dst.IP NOTIN "10.152.43.*",...	WARNING	None	DISABLED	0
a1422884820297	AND (var.src.IP IN "10.240.35.*", var.t...	WARNING	30	DISABLED	0
[illegible]	var.totalBytes > 400	WARNING	[illegible]	ENABLED	0
a1424789438094	AND (var.src.IP NOTIN "10.179.*" , va...	WARNING	None	DISABLED	0
a1424793285646	AND (var.dstid != 100, var.srcid != 100)	WARNING	None	DISABLED	0
a1424794188541	var.srcid == 100	WARNING	None	DISABLED	0
a1424795582080	AND (var.srcid != 1, var.srcid != 100)	WARNING	None	DISABLED	0

Link 10.179.18.205:20000 - 10.2...

Alarm	true
Destination	10.20.51.20
Destination Port	61610
ID	1583633727469...
Protocol	dnp3
Source	10.179.18.205
Source Port	20000
Type	tcp
var.src.IP	10.179.18.205
var.dst.IP	10.20.51.20
var.totalBytes	71264
var.totalPackets	323
var.srcid	1
var.dstid	100

Link 10.179.18.106:20000 - 10.2...

Alarm	false
Destination	10.20.51.20
Destination Port	61685
ID	1238286283696...
Protocol	dnp3
Source	10.179.18.106
Source Port	20000
Type	tcp
var.src.IP	10.179.18.106
var.dst.IP	10.20.51.20
var.totalBytes	9515
var.totalPackets	123
var.srcid	1
var.dstid	100

ProtocolPatroller example session displays

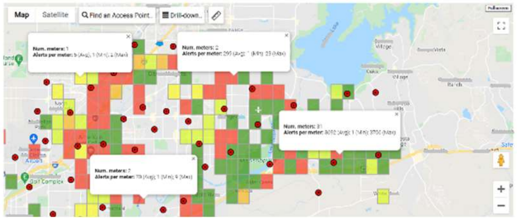
MeshView Network Analytics

SecureSmart MeshView Network Analytics is a packet database-driven, mesh network analysis tool that abstracts information from low-level packet detail to visualize node behavior and field network operation.

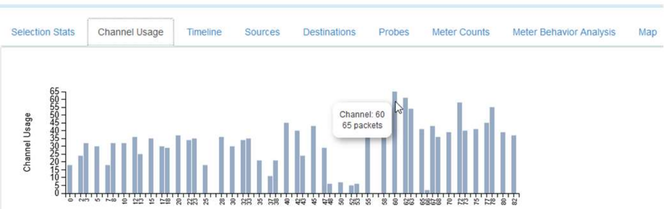
MeshView users create complex queries based on node information, traffic types, location, time, and more to visualize and answer FAN operations performance questions such as:

- How do endpoints route within the FAN?
- Where are the areas of poor connectivity?
- How does actual Access Point/Collector coverage compare to RF terrain models?
- Are certain field nodes over-utilized?
- Are security events clustering geographically?
- Are any nodes having difficulty communicating with back-end systems?

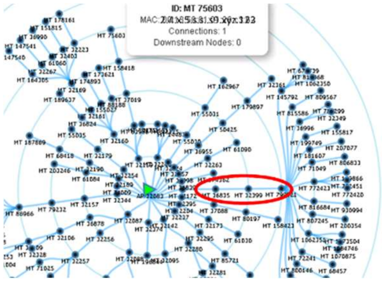
SecureSmart MeshView visualizes key reporting metrics across service area geography via tile maps, renders logical and geographic routing maps with time lapse imagery, and visualizes path loss/coverage modeling for network tuning. MeshView provides reports, statistics, and RF channel usage summaries.



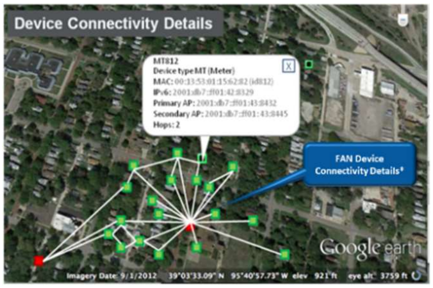
Example MeshView alerts per meter heat map



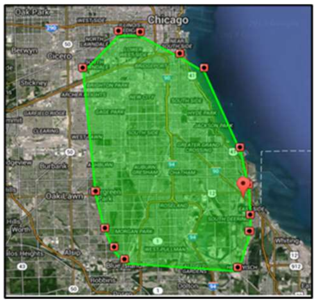
Example MeshView channel usage table



Example MeshView logical routing map playback identifying misrouting



Example MeshView FAN connectivity details

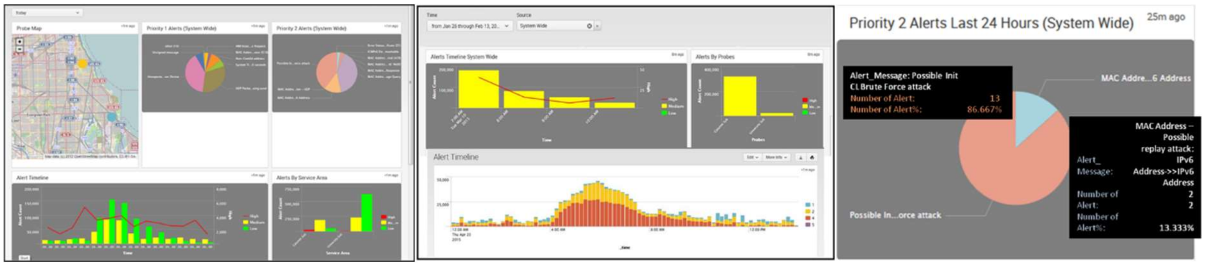


Example MeshView sensor coverage map

GridGuard IDS

Peraton Labs’ SecureSmart GridGuard is a customized, deep packet inspection Intrusion Detection System based on SNORT with custom extensions for DA systems. It is an industry-first DA FAN *Wireless* IDS. GridGuard employs experience and knowledge-driven rules and heuristics built upon vulnerabilities discovered in Peraton Labs’ extensive and ongoing 4-Quadrant Security Assessments[1] of field network and DA systems. GridGuard IDS provides traffic flow analysis, statistical traffic modeling, behavior and rate analysis, and node, protocol, and port whitelisting. GridGuard identifies node attribute changes and employs signature-based methods. GridGuard detects anomalies and monitors for exploitation of known system deficiencies as a residual risk solution. Real-time alerts are traceable to offending timestamped packets. GridGuard integrates with Splunk or other preferred SIEM systems to create custom dashboards for alert monitoring and reporting.

[1] Visit Vulnerability and risk analysis - Peraton Labs for more information about the Peraton Labs’ 4-Quadrant Assessment Methodology.


Probe Map
Priority 1 Alerts (System Wide)
Priority 2 Alerts (System Wide)
Alert Timeline
Alerts By Service Area
Alerts Timeline System Wide
Alerts By Probes
Alert Timeline
Priority 2 Alerts Last 24 Hours (System Wide)
25m ago
Alert_Message: Possible Init CL Brute Force attack
Number of Alert: 13
Number of Alert%: 86.667%
MAC Addre...6 Address
MAC Address – Possible replay attack: IPv6 Address->>IPv6 Address
Alert_ Message:
Number of Alert: 2
Number of Alert%: 13.333%
Possible In...orce attack

Example GridGuard dashboards

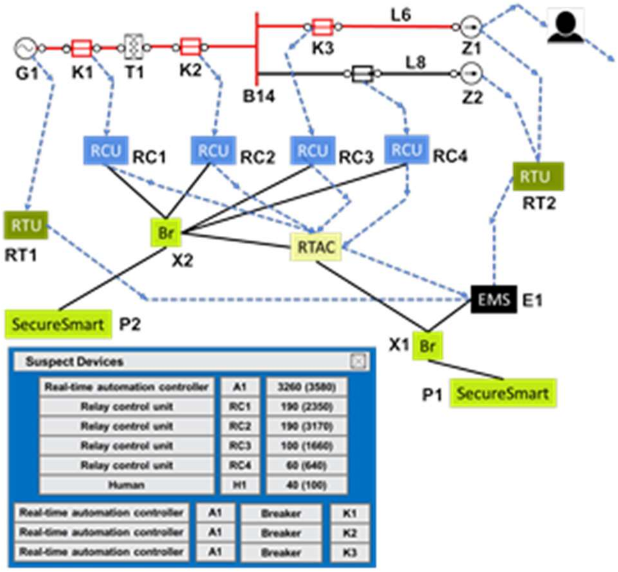
Peraton Labs' SecureSmart GridGuard has demonstrated it can detect and analyze wireless and wired DA and SCADA network anomalies and display network problems previously unseen. Examples of such network security anomalies include the following.

- Rogue devices and network IDs
- Cross traffic between bordering utilities and different environments
- Unexpected protocols and port usage
- Unexpected DNS Domain
- Insecure commands and legacy port operation
- Illegal intra-FAN traffic flows
- Backend IP and port scans
- Unrecognized FSU and field tool activity
- Mesh Packet Replay Attempts
- Misconfigured nodes (e.g., trap servers and DL CA)
- Lack of Link Layer Integrity HMAC
- Excessive node discovery/chattiness and rapidly cycling devices
- SCADA traffic in the "clear"
- Bad Signatures
- Mesh Reconfiguration / Instability
- Malformed Messages
- Layer 2 Synchronization and MITM Attacks
- Routing Attacks (e.g., blackholes, redirection)
- Null Role Secure Port Activity with No Security
- Last Gasp Forgery
- Unauthorized Meter Movement

Jolt Telemetry Analysis

The Peraton Labs' SecureSmart Jolt application performs advanced analyses of energy controller telemetry to assess the integrity and consistency of reported energy data and device state. By applying circuit laws, corroborating multiple sources of telemetry, reasoning deductively, and inferencing within the context of a one-line diagram, Jolt detects inconsistencies and point mapping problems and creates a ranked list of misbehaving devices. For DA systems, Jolt can examine conditions before and after an event to determine if prior conditions warranted the actions that were taken, and whether those actions were successful. For example, Jolt can compare the power factor before an automated capacitor bank engaged to see if the triggering conditions were met, and examine the power factor after the event to see if conditions improved. When used with a one-line diagram, Jolt can infer conditions from multiple nearby and distant reporting devices to detect inconsistencies in voltages, currents, phase angles, and other parameters to identify a device whose reporting is questionable. Jolt can determine if the data reported by an automated capacitor bank is consistent with values reported by other upstream and downstream devices.[2]

[2] For more information about Jolt and other EnergyDefender energy integrity applications visit ICS and IoT security - Peraton Labs.



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

Example SecureSmart Jolt network and inconsistency dashboard

SECURESMART SOLUTION ARCHITECTURE

The Peraton Labs SecureSmart solution accommodates several deployment models to satisfy customer requirements. It can be delivered as a turn-key service hosted in the Peraton Labs infrastructure, where the utility is only responsible for installing field sensors on utility assets and Peraton Labs maintains and operates the system and performs daily monitoring. It can be delivered as a turn-key service with backend systems installed in the utility's data center, where Peraton Labs remotes into the utility infrastructure to perform daily monitoring. It can be delivered as a product solution, where the utility purchases the hardware, licenses the software, and performs daily monitoring and Peraton Labs provides maintenance and support services.

Visit Energy - Peraton Labs for more information.

Peraton | LABS

LEARN MORE AT

PERATONLABS.COM

150 Mount Airy Road
Basking Ridge, NJ 07920