As increasingly sophisticated cyberattacks on Industrial Control Systems (ICS) in general, and supervisory control and data acquisition (SCADA) systems in particular, are becoming an industry norm, North American utilities are experiencing thousands of attacks each month.

Perspecta Labs’ ProtocolPatroller part of its SecureSmart™ critical infrastructure solution line, is providing utilities continuous cyber monitoring and anomaly detection and protection. The award winning SecureSmart ProtocolPatroller delivers extensive protocol-specific security capabilities for smart grid and other ICS and SCADA applications.

**Detect and stop cyberattacks in real time**

ProtocolPatroller provides cybersecurity protection across a wide range of threats and SCADA protocols, including:

- Inter-Control Center Communications Protocol (ICCP)
- Synchrophasor Protocol C37.118
- Advanced Metering Infrastructure (AMI) Data Transport Protocol C12.22
- Substation Automation 61850-Generic Object Oriented Substation Events (GOOSE)
- SCADA Distributed Network Protocol (DNP3)
- Schweitzer Engineering Laboratories (SEL) Fast Message protocol at the SCADA application layer
- Address Resolution Protocol (ARP), Hypertext Transfer Protocol (HTTP) and Telnet at the IP layer

More broadly, the software’s modular design allows it be easily extendable to protect other ICS SCADA protocols. For each such protocol, ProtocolPatroller employs a collection of behavior model checkers that have been verified with formal methods to detect communication anomalies. Using these robust checkers, the ProtocolPatroller detects ongoing attacks, including zero-day attacks, and alerts operators through a user-friendly dashboard. When used in the in-line protection mode, ProtocolPatroller can perform predetermined actions to help stop the ongoing attacks.

ProtocolPatroller software can be co-hosted as well as reside in a customer’s existing IT hardware or software platforms. Co-hosting can occur at gateways (e.g., in data centers or control centers), customers and servers (e.g., ICCP nodes, smart meter data collection engines), Intelligent Electronic Devices (IED), or even in a service cloud. Hosting is available as a dedicated platform.
Two modes of deployment

ProtocolPatroller deployment is available in two modes:

- **Sniff mode**: where attacks can be detected and alerted
- **In-line protection mode**: where attacks being detected can be terminated using predetermined attack vector rules and responses for different protocol attacks

The monitoring and filtering of potential vulnerabilities are available through the built-in and user-defined rules in ProtocolPatroller offerings. Moreover, the dashboard provides operators with great flexibility in terms of choosing which protocol they would like to monitor and protect, which set of communication sessions and endpoints they would like to pay attention to and which rules they would like to apply. ProtocolPatroller provides the ability to display only sub-nets for large networks.

Comparing ProtocolPatroller to other tools

Almost all cybersecurity tools employed in ICS and power system applications take the form of a gateway, with traditional capabilities including firewall, VPN, port scanning features or custom IDS for enterprise applications. ProtocolPatroller is an industry leading protocol-specific capability based on stateful model-checkers to patrol SCADA protocol communication contexts and behaviors, while applying deep-packet inspection to track event sequences and perform cross session comparisons. ProtocolPatroller has been installed and is currently operating in selected utility operating centers for monitoring ICCP and C12.22 traffic.

Why SecureSmart ProtocolPatroller?

- Industry-proven, high-value SCADA protocol protection capability
- Deep packet inspection
- Protocol-specific stateful model-checkers
- Extendable to common SCADA protocols
- Field proven in the smart grid utility industry