Solution Paper

SecFlow Security Appliance Review

NERC CIP version 5 Compliance Enabler

July 2014

Your Network's Edge

Abstract

The alarming increase in cyber attacks on critical infrastructure poses new risk management challenges for utilities. RAD's SecFlow provides resilient cybersecurity controls for remote substations.

This paper reviews SecFlow's compliance with NERC CIP 005 and 007 requirements for Electronic Security Perimeter and Systems Security Management.

Contents

1 The SecFlow Answer to Remote Substation Security, Compliance & Resilience

Remote Substation - Use Case For SecFlow

The Department of Homeland Security reports that of the growing number of cyber-attacks on critical infrastructure in 2012, more than 40 percent were made on energy-sector targets. This alarming increase of attacks poses new risk-management challenges for utilities, and energy sector owners and operators of critical infrastructure. Among their most challenging responsibilities is the need to improve security in remote substations.

The physical attacks on remote substations in Arkansas in the fall of 2013, which brought down transmission lines, sabotaged power poles and led to a fire in a substation control house, highlight the inherent vulnerability of remote sites.

A cyber attack on these sites is especially worrisome because of the inability of qualified cybersecurity and SCADA network experts to respond in time.

Fines from NERC CIP noncompliance add a further risk. The NERC May 2012 ERO Compliance Analysis Report shows that Electronic Security Perimeter ranks second in potential noncompliance under NERC CIP. The top violation area is under Systems Security Management. Managing compliance to remote sites is particularly burdensome. 2013 enforcement data from NERC shows that fines exceeding $100,000 are regularly imposed for these violations.

RAD's SecFlow helps solve the management challenge of providing resilient cybersecurity controls for remote substations. Its service-aware features enable SCADA managers to securely monitor and control devices within the remote perimeter.

The ease of compliance with CIP 005 and 007 is afforded from the coupling of the service-aware SecFlow secure communications appliance and the SecFlow Network Manager software. As a package, their features assure security managers of NERC CIP compliance for remote substations, especially for the two most problematic areas: Electronic Security Perimeter and Systems Security Management.

2 Remote Substation Secure Communications

The SecFlow is a multi-function hardware and security appliance with extensive capabilities and network applications that warrant a broader device characterization – closer to a full-feature appliance-type device – than the conservative "ruggedized switch" description that is commonly used. SecFlow is actually an all-in-one SCADA

security multiplier that offers the power industry many security and efficiency advantages, while also enabling NERC CIP version 5 compliance.

SecFlow offers a suite of mix-and-match security configurations, so that security managers can remotely tailor device-specific security controls. Options such as device-specific protocol white-listing, tailored access control configurations (for both physical and virtual ports) and a variety of other security features maximize its security coverage.

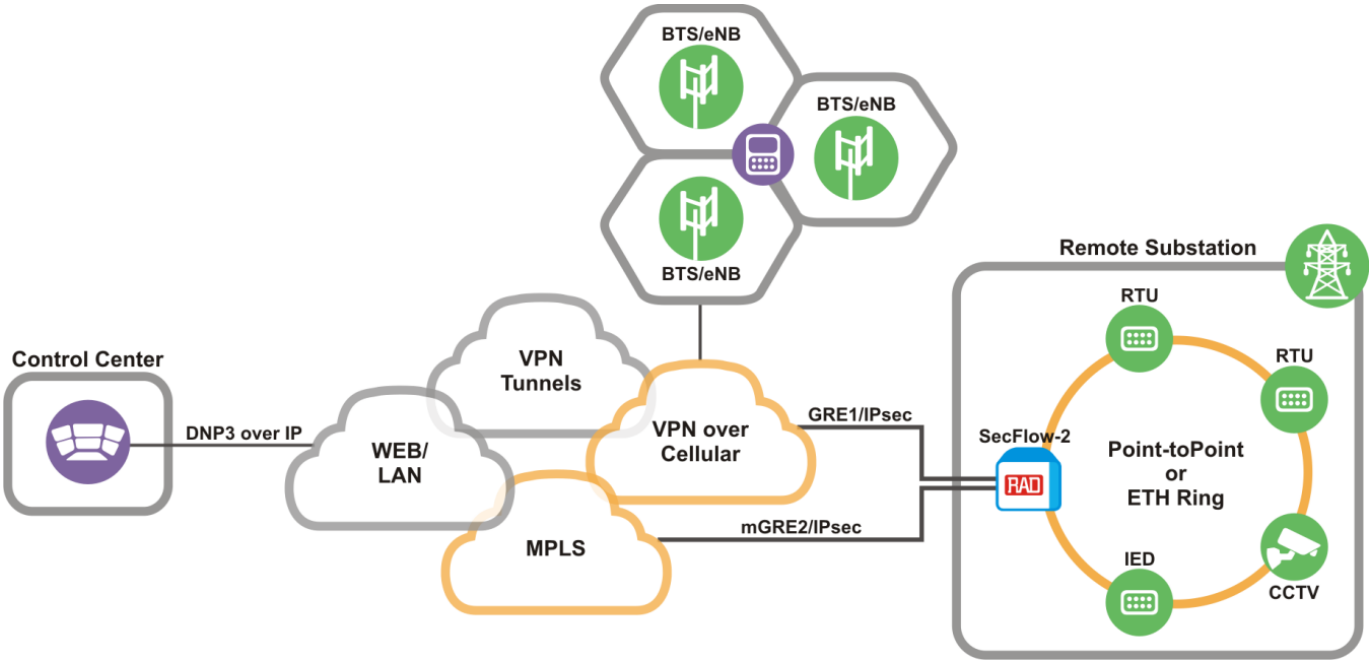

Figure 1: Secure communications for remote substations

What if each SCADA device within a remote substation could be distinctly and remotely configured for security, with separate access controls, white listing, and a suite of other specific security features? This is possible with the coupling of SecFlow Network Manager and SecFlow. These tailored security controls make SecFlow highly suitable for remote sites.

This analysis of SecFlow, conducted by independent cybersecurity subject matter experts, focuses on a power sector Use Case, particularly remote substation applications, analyzing how SecFlow can render a NERC CIP Responsible Entity compliance-ready.

3 SecFlow Product Review

Distributed Service-Aware Features in the SecFlow

Figure 2: RAD's SecFlow ruggedized SCADA-aware switch/routers

- Ruggedized switches with an integrated SCADA-aware firewall
- Enables dynamic configuration to detect and deeply analyze various SCADA protocols
- White-listing configuration options (command types, MAC addresses, ports, protocol)
- Configurable to drop and alert, alert, or simply drop traffic
- Configurable with sensors to detect SCADA traffic anomalies
- Anomaly detection and heuristics: can detect traffic spikes
- Enable automatic detection of "normalcy" baseline
- Failover communication redundancy through Ethernet and cellular
- IPSec VPN tunnels with X.509 certificates
- Remote collection of logs for activity monitoring
- Save on space requirements by combining multiple functions in a single device

4 SecFlow Network Manager

Advantages of Coupling SecFlow with SecFlow Network Manager

Full functionality of the SecFlow, as well as robust management of the SCADA network, is enabled from the SecFlow Network Manager software. This coupling of capabilities offers a suite of NERC CIP compliance options, as well as greatly improved security.

From a management console, SecFlow Network Manager affords configuration and security options, such as:

- Segmentation of SCADA device control by port, MAC ID, protocol, white-listing, port disabling, command type, and user access
- Multi-dimension access control functionality that complicates device access to any would-be attacker
- Global and per-application configuration management segmentation, so that user access controls may be configured to limit access

The suite of security controls offers substantial benefits to remote substations, and other critical installations that require both continuous remote security monitoring and management controls.

5 NERC CIP Compliance (version 5)

Preparing for NERC CIP Version 5 Compliance

The FERC has indicated that NERC CIP version 4 will be skipped in favor of version 5. Presidential Policy Directive – PPD-21 is also causing increased focus on cybersecurity. In addition, there is a general consensus among cybersecurity professionals – which will undoubtedly influence Public Utility Commissions (PUC) – that a dynamic cyber risk management approach will become the standard and norm. Such an approach, which adds a premium on the capability to adjust controls to new threats, requires security managers to invest in highly adaptable security solutions.

NERC CIP 5 similarly aligns with such an approach. Planning for improved cybersecurity, and for alignment with NERC CIP 5, should therefore involve assessment of the capabilities that can be adapted to heightened security requirements.

Moreover, increasing security to remote locations can strain an already over-taxed IT staff. In an increasingly hostile cyber landscape, both efficiency and resiliency is required. Security managers require solutions configured with a hardened security baseline for resilience, as well as ease of configuration modification and change management to increase efficiencies.

The all-in-one SecFlow, together with the SecFlow Network Manager software, meets these needs.

6 Mapping NERC CIP (version 5) Requirements

CIP003-5 Security Management Controls

The purpose of CIP003-5 (cybersecurity policy controls) is to provide a management and governance foundation for all requirements that apply to personnel who have authorized electronic access and/or authorized unescorted physical access to BES Cyber Systems. CIP003-5 periodic review and approval of the cybersecurity policy ensures that the policy is kept up-to-date and periodically reaffirms management's commitment to the protection of its BES Cyber Systems. The approach of CIP003-5 incorporates an objective of empowering and enabling the industry to identify, assess, and correct deficiencies in the implementation of CIP003-5 requirements. Methods and evidence for ensuring compliance include policy documents, revision history, records of review, and workflow evidence from a document management system assuring review of each policy at least once every 15 calendar months.

SecFlow, together with the SecFlow Network Manager software, either provides features that directly comply with certain CIP003-5 requirements, or provide the data or capability that enables the Responsible Entity to demonstrate through processes and record-keeping its compliance with a particular requirement.

CIP003-5 R1	Part 1.7: configuration change managemt and V.A enabled by Remote Access Agent.
CIP003-5 R1	Parts 1.2, 1.4, 1.5, 1.6: SecFlow Network Manager with SecFlow support and enable security management plans and processes for BES Cyber Systems, including system and asset identification, event logging, access control, configuration change management, recovery plans, and network management.

Table 1: RAD's SecFlow compliance with CIP003-5 security management controls

CIP005-5 Electronic Security Perimeter

The purpose of CIP005-5 (electronic security perimeter) is to manage electronic access to BES Cyber Systems by specifying a controlled Electronic Security Perimeter in support of protecting BES Cyber Systems against compromise that could lead to mis-operation or instability in the BES. Methods and evidence for ensuring compliance include the documented processes and direct system or capability measures that address the requirement.

SecFlow, through its SCADA-aware firewall, offers a suite of configurable controls to address access control, authentication, remote access controls, configuration change management, event and audit logging, and other features.

CIP005-5 R1	Part 1.3: inbound/outbound routable traffic at EAP access control by VLAN, SCADA firewall per port, enable/disable port, port access filter per MAC/IP, DoS protection. Part 1.4: dial-up authentication and documented processes by dual configuration systems, both with local or remote authentication, plus audit trail. Part 1.5: malicious traffic detection a EAP by service aware firewall acting as IPS/IDS, by validating protocol structure and session flow, checking code function against operator-provided list for validity, abnormality detection of traffic bursts or abnormal command patterns, operator alerts on detection, as well as optional abnormal packet drop.
CIP005-5 R2	Part 2.1: interactive remote access boundaries enabled by management interfaces physically separated from other interfaces, and logically via VLAN, and with ingress and egress filtering to ensure traffic does not cross interfaces, SSH and IPSEC tunneling (VPN). Physical host authentication in the internal network (MAC/IP address or IEEE802.1x) and validation of performed operations by that host. Logical authentication for access over insecure interfaces including IPSEC encryption keys and remote user credentials. Part 2.2: interactive remote access encryption performed by SSH, and system integration provided via IPSEC tunnels. Part 2.3: Authentication: reverse SSH sessions to defined remote console, with x.509 certificates as a transition pathway.

Table 2: RAD's SecFlow compliance with CIP003-5 electronic security perimeter

CIP007-5 Systems Security Management

The focus of CIP007-5 (systems security management) is on port control and access, patch management, malicious code detection and prevention, incident log capabilities, and access controls.

SecFlow, when together with the SecFlow Network Manager software, either provides features that directly comply with certain CIP007-5 requirements, or together provide the data or capability that enables the Responsible Entity to demonstrate through processes and record-keeping its compliance with a particular requirement.

CIP007-5 R1	Part 1.1: logical port disabling provided by full firewall capability, to include SCADA protocol awareness and port shutdown / MAC / IP restrictions, alerting VLAN capabilities, port shutdown and ACL capabilities. Part 1.2: Physical port shutdown capability and MAC/IP restrictions to ports.
CIP007-5 R2	Parts 2.1, 2.2, 2.3: SecFlow Network Manager software facilitates patch management through a variety of features, such as device identification, topology characterization and system categorization, device query, and inventory listing.
CIP007-5 R3	Parts 3.1, 3.2, 3.3, 3.4, 3.5: SecFlow Network Manager and SecFlow together or individually provide malware detection and prevention capabilities through packet inspection (includes SCADA awareness with anomaly detection and alerting, operator control over allowed/disallowed commands with alerting and dropping capabilities), and audit logs at both the SecFlow and SecFlow Network Manager.
CIP007-5 R4	Part 4.1: incident logging provided by SCADA-aware firewall and interfacing with SecFlow Network Manager; allows for detection and reaction to potential malicious activity, audit trail logging provides for failed access and logins. Parts 4.1, 4.2, 4.4, 4.5: SCADA-aware firewall is fully configurable to alert on anomalies; System is syslog- and SNMP-capable, and can send logs to SecFlow Network Manager for retention.
CIP007-5 R5	Part 5.1, 5.2: access control, user authentication and privilege-level associations via SSH for remote access, local/TACACS /Radius-capable; procedural system supports user-level access controls.

Table 3: RAD's SecFlow compliance with CIP007-5 systems security management

CIP009-5 Recovery Plans For BES Cyber Systems

Redundancy and recovery are enabled by multiple failover features:

CIP009-5 R1	Part 1.5: SecFlow supports multiple command interfaces to include cellular with support for two sim cards, allowing for N+2 failover of communications channels (RIP, VRRP).

Table 4: RAD's SecFlow compliance with CIP009-5 recovery plans for BES cyber systems

CIP010-1 Configuration Management and Vulnerability Assessments

SecFlow, together with SecFlow Network Manager software, either provides features that directly comply with certain CIP010-1 requirements, or together provide the data or capability that enables the Responsible Entity to demonstrate through processes and record-keeping its compliance with a particular requirement.

CIP010-1 R1	Parts 1.1, 1.2, 1.3: baseline configuration is enabled by the SCADA-aware firewall, configuration options of SecFlow, and the SecFlow Network Manager. SecFlow provides anomaly detection of SCADA traffic with alerting capability.
CIP010-1 R2	Part 2.1: SecFlow enables internal baselining and anomaly detection of SCADA traffic with alerting capability, including bad/anomalous traffic and detection of configuration change, or failure of devices, and theSecFlow Network management of SecFlow.

Table 5: RAD's SecFlow compliance with CIP010-1 configuration management and vulnerability assessments

CIP011-1 Information Protection

SecFlow Network Manager software provides features that enable the Responsible Entity to demonstrate through processes and record-keeping its compliance with a particular requirement of CIP011-1.

CIP011-1 R1	SecFlow Network Manager supports and enables information protection related to BES cyber systems, including system and asset identification, logging, change management, and network topology.

Table 6: RAD's SecFlow compliance with CIP011-1 information protection

NERC CIP version 5 Mapping Summary

CIP003-5 Security Management Controls

- R1 Cybersecurity Policy Controls
  - Part 1.2 Electronic Security Perimeter
  - Part 1.4 System Security Management
  - Part 1.8 Information Protection
- R2 Cybersecurity Policy Controls
  - Part 2.3 External Routable Protocol Connections
  - Part 2.4 Cyber Incident Response

Compliance: dynamic configuration meets a 15-month review cycle; extensive control options exceed requirements; remote access controls in the device as a perimeter gateway. SecFlow Network Manager provides the dynamic control and GUI, management, and response to incidents. It integrates with the embedded firewall to enable home-station management of SecFlow, as well as continuous monitoring.

CIP005-5 Electronic Security Perimeter

- R1 Comprehensive Process Controls
  - Part 1.1 Defined ESP for Cyber Assets

  - Part 1.2 Defined Electronic Access Point
  - Part 1.3 Access Control
  - Part 1.5 Malicious Traffic Detection
- R2 Interactive Remote Access
  - Part 2.1 Remote Access Barrier Control
  - Part 2.2 Remote Access Encryption
  - Part 2.3 Multi-factor Authentication

Compliance: comprehensive and synergistic compliance and security multiplier for CIP005-5 Tables R1 and R2 requirements: access control to device-level via white listing, protocol-aware access, MAC ID-aware access, and layered authentication and SSH; two-way traffic control, detection, and alerting. SecFlow Network Manager provides management of the SecFlow to enable compliance with Electronic Security Perimeter requirements. The robust features of the SecFlow, especially at remote locations, are readily accessible and managed via the SecFlow Network Manager.

CIP007-5 Systems Security Management

- R1 Ports and Services
  - Part 1.1 Logical Port Enabling & Control
  - Part 1.2 Physical Port Control
- R2 Security Patch Management
  - Part 2.1 Configuration Support for Patch Management
  - Part 2.2 Timely Inspection (35 days)
- R3 Malicious Code Prevention
  - Part 3.1 Detect, Deter, Prevent Method
  - Part 3.2 Mitigation of Malicious Code
  - Part 3.3 Process to Meet Part 3.1

Compliance: an integrated firewall within SecFlow ensures full compliance and exceeds all requirements: configurable, detect and prevent malicious code at the gateway; port control-enabled. Blocking malware attacks with application-(SCADA) aware firewall. The SecFlow Network Manager enables shutdown of physical and virtual ports, or permits device interface with the SecFlow only via specified ports. Patch management and continuous monitoring for malicious code are also enabled. Packet inspection includes SCADA awareness with anomaly detection and alerting, operator control over allowed/disallowed commands with alerting and dropping capabilities.

CIP009-5 Recovery Plan for BES Cyber Systems

- R1 Recover Specifications
  - Part 1.5 Failover Data Preservation

Compliance: redundant failover communication pathways to ensure constant interface with management software and data retention: cellular with support for two SIM cards, RIP, VRRP. The SecFlow Network Manager provides network topology and management; database backup for network administration; and multiple communication channels to SecFlow for redundancy. Emergency restoration via USB.

CIP010-1 Configuration Change Management

- R1 Change Management Process
  - Part 1.1 Baseline Configuration
  - Part 1.3 BES Cyber Asset Identification
  - Part 1.4 Change Controls and Documentation
  - Part 1.5 Change Testing and Documentation
- R2 Unauthorized Change Detection
  - Part 2.1 Detect Unauthorized Changes

Compliance: Device detection facilitates baseline configuration, change management, and device management. SCADA-aware firewall enables baselining and anomaly detection of SCADA traffic with alerting capability; integrates with management software to enable unauthorized change detection and continuous monitoring. The SecFlow Network Manager provides activity logs, alarm logs, visibility into configuration changes, management, and unauthorized change logs.

7 Conclusion

NERC CIP compliance becomes more critical than ever for power utilities, to properly thwart new cyber security threats. RAD's SecFlow multi-function hardware and security appliance offers the power industry many security and efficiency advantages while also enabling NERC CIP version 5 compliance.

www.rad.com

International Headquarters
RAD Data Communications Ltd.
24 Raoul Wallenberg St.
Tel Aviv 6971923 Israel
Tel: 972-3-6458181
Fax: 972-3-6498250
E-mail: market@rad.com
http://www.rad.com

North America Headquarters
RAD Data Communications Inc.
900 Corporate Drive
Mahwah, NJ 07430 USA
Tel: (201) 529-1100
Toll free: 1-800-444-7234
Fax: (201) 529-5777
E-mail: market@radusa.com
www.radusa.com

Your Network's Edge