

Solution Paper

> Securing Power Distribution Systems



Table of Contents

Introduction	3
Electric Power System Overview	3
Power Transmission	4
Typical Security and Compliance Issues.....	5
Remote Access	6
Security & Compliance Management.....	7
Perimeter and Network Segmentation	8
Control Room Protection	10
Field Device Protection	12

Introduction

This solution paper provides an introductory overview of the electric power supply chain including generation, transmission and distribution and then discusses typical security and compliance issues facing Electric Power Transmission Systems. Several common architectures are depicted, along with an overlay of solutions specifically designed to meet the NERC CIP Cyber Security requirements for securing these systems, while enhancing the performance of the Energy Management Systems (EMS) that control the efficient operation of power transmission.

Electric Power System Overview

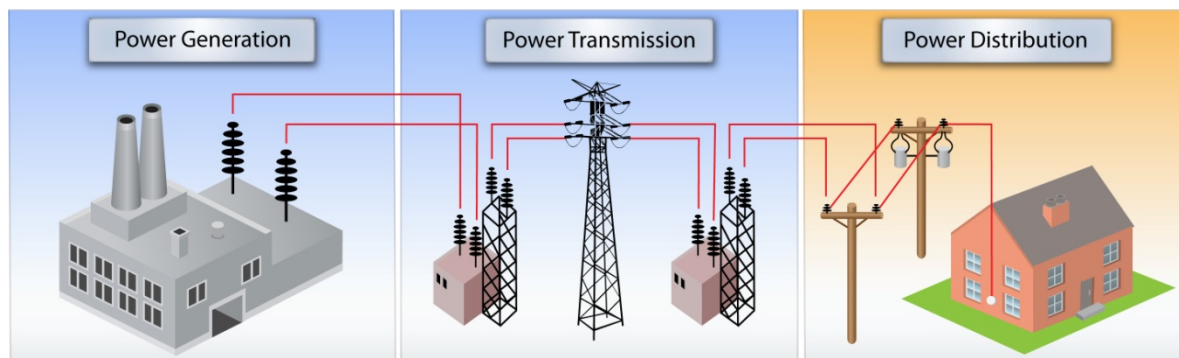
Electric Power Systems transform other types of energy into electrical energy and transmit this energy to a consumer. Unlike other utility commodities like water or natural gas, electricity cannot easily be stored. Energy can also neither be created nor destroyed, only transformed into different types of energy. Electric Power Systems are typically grouped into three functional areas:

Power Generation: Is the process of transforming various types of energy into electricity.

Transmission: Steps up the electricity to a higher voltage and then transports and routes the electricity over long distances for delivery to local markets.

Distribution: Handles the process of stepping down electricity to proper delivery levels and distributing it to the final consumers of the power.

The diagram below is a good example depicting these three functional areas.



Power Distribution

Electric power distribution is the final stage to deliver electricity to end users. A distribution system network carries electricity from the transmission system and delivers it to residential and commercial consumers. A typical power distribution network may include medium voltage power lines (less than 50 kV), electric substations and transformers which can be pole mounted. The final point of electric power distribution will use low voltage wiring (less than 1000 V) and electricity metering devices. The power must be stepped down to low voltage before it can be consumed by a home or business. The place where the conversion from transmission to distribution occurs is in a power substation.

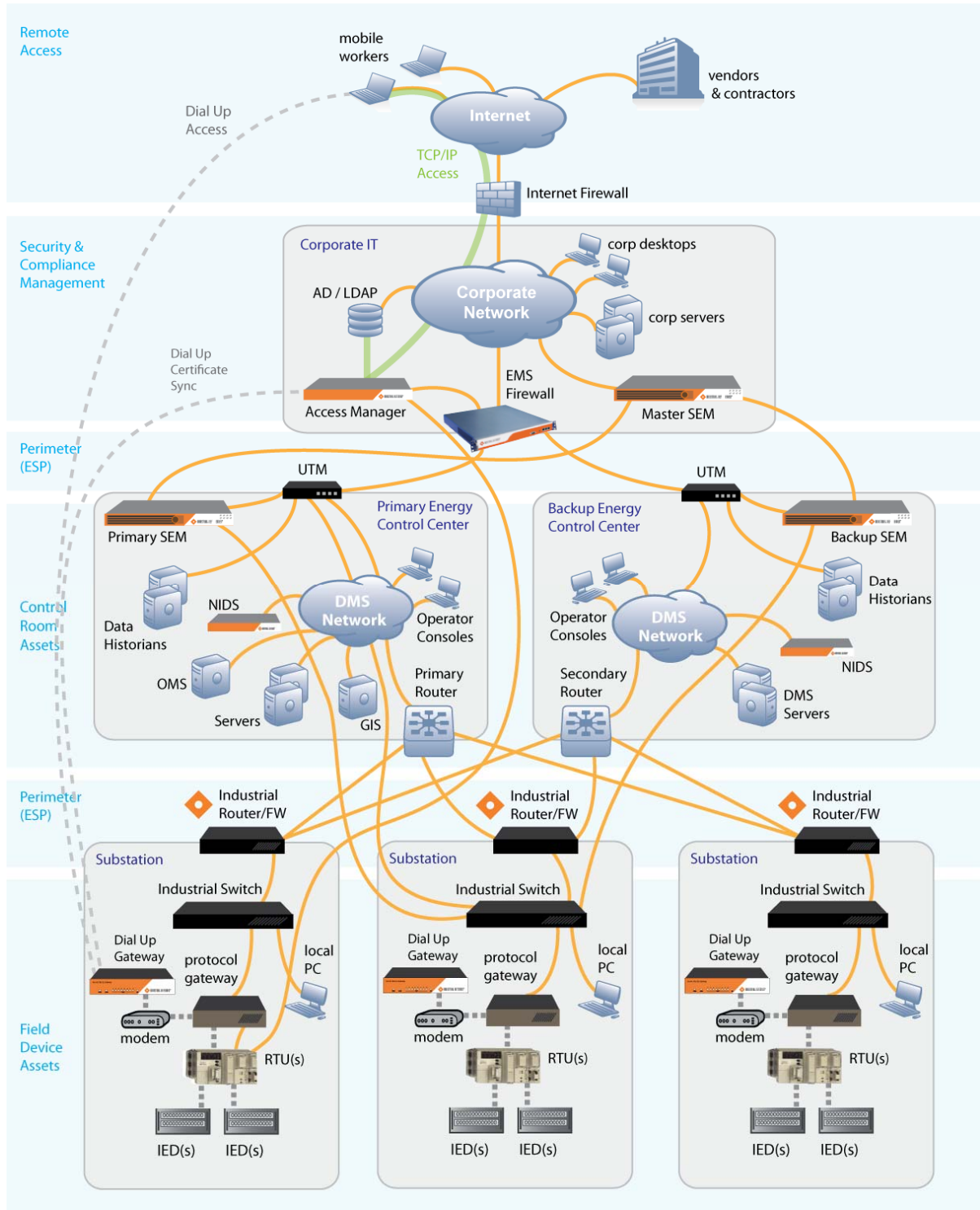
For power to be useful in a home or business it must be stepped down from the transmission system to the distribution system. This process may happen in several phases. The place where the conversion from “transmission” to “distribution” occurs is in the power substation.

A power substation can serve the following purpose:

- Transformers that step transmission voltages down to distribution voltages
- Has a “bus” that can split the distribution power off in multiple directions
- Contains circuit breakers and switches so that the substation can be disconnected from the transmission system or other separate distribution lines when necessary

This solution paper defines the common problem areas and individual pain points associated with securing the electric power distribution environment. This paper also contains detailed solution recommendations to solve each of these problem areas. The outline of the problem areas is contained below and includes a graphical depiction of where these issues are typically seen in a transmission system network diagram. These issues and problem areas are also mapped to the actual NERC CIP requirements and a solution matrix table.

Power Distribution Security & Compliance - Typical Architecture by Functional Area



Typical Security and Compliance Issues

REMOTE ACCESS

Key Challenge

A mobile workforce and 3rd party vendors have a growing need to establish remote connectivity to Critical Cyber Assets (CCAs) within the control center or substation environment for system access, troubleshooting, and restoration. The need for remote access connectivity can enhance productivity and provide cost savings to electric power asset owners and operators but it can also increase the cyber security risks and vulnerabilities if the proper security protection is not in place.

Security Challenges

Key Requirements

Remote Access to systems with Critical Cyber Assets (CCAs) must be secured, monitored and logged. This includes IP based Ethernet and Dial-up communications and managing multiple users and access privileges. Access to the distribution management system control center and substations must be adequately secured.

Authentication into an environment from a remote access connection should have the ability to support directory services infrastructure to securely manage all user activity.

Related NERC CIP Requirements

NERC-CIP 005 – Requires the identification and protection of Electronic Security Perimeter(s) inside which all Critical Cyber Assets reside as well as access points on the perimeter

CIP-005 R1.1. *Access points to the Electronic Security Perimeter(s) shall include any externally connected communication end point (for example dial-up modems) terminating at any device within the Electronic Security Perimeter*

NERC-CIP 007 – Requires Responsible Entities to define methods, processes, and procedures for securing those systems determined to be Critical Cyber Assets, as well as the non-critical Cyber Assets within the Electronic Security Perimeter(s).

CIP-007 R5. Account Management – *The responsible entity shall establish, implement, and document technical and procedural controls that enforce access authentication of, and accountability for, all user activity, and that minimize the risk of unauthorized system access*

Industrial Defender Solution

In power distribution environments, users have a need to remotely access critical cyber assets over both TCP/IP Ethernet networks and Dial-up based connections to access distribution management centers and substation environments. Industrial Defender provides a comprehensive solution for this environment with the **Industrial Defender Access Manager** solution. Access Manager detects and prevents unauthorized entry attempts while providing transparent, uninterrupted IP or dial-up substation access for authorized users. Access Manager's resilient, decentralized architecture provides continuous user access even under extreme conditions. Access Manager includes powerful management and audit reporting tools, comprehensive logging, and the fastest time to compliance of any solution.

SECURITY AND COMPLIANCE MANAGEMENT

Key Challenge

Managing the ongoing security and compliance of Critical Cyber Assets within a critical infrastructure environment should be a centralized activity. Security and compliance management solutions should be compatible with enterprise based systems and processes as required by bulk electricity owners and operators.

Security Challenges

Key Requirements	Related NERC CIP Requirements
<p>24 x 7 monitoring and logging of perimeter access activity including all Electronic Security Perimeter (ESP) access points</p> <p>24 x 7 monitoring of internal control room and field device Critical Cyber Assets (CCAs)</p> <p>Centralized repository of events, logs, and documentation management for audit traceability and audit verification</p>	<p>NERC CIP-005 – Requires the identification and protection of Electronic Security Perimeter(s) inside which all Critical Cyber Assets reside as well as access points on the perimeter</p> <p>CIP-005 R3. Monitoring Electronic Access – <i>The Responsible Entity shall implement and document an electronic or manual process(es) for monitoring and logging access at access points to the Electronic Security Perimeter(s) twenty-four hours a day, seven days a week</i></p> <p>NERC CIP-007 – Requires Responsible Entities to define methods, processes, and procedures for securing those systems determined to be Critical Cyber Assets, as well as the non-Critical Cyber Assets within the Electronic Security Perimeter(s).</p> <p>CIP-007 R6. Security Status Monitoring – <i>The Responsible Entity shall ensure that all Cyber Assets are within the Electronic Security Perimeter, as technically feasible, implement automated tools or organizational process controls to monitor system events that are related to cyber security.</i></p> <p>CIP-007 R9. Documentation Review and Maintenance – <i>The Responsible Entity shall review and update the documentation specified in Standard CIP-007 at least annually. Changes resulting from modifications to the systems or controls shall be documented within ninety calendar days of the change.</i></p>

Industrial Defender Solution

In power distribution environments, users have a need for a centralized event and log management solution for the Critical Cyber Assets (CCAs) that is capable of collecting events and logs over both TCP/IP Ethernet networks and Dial-up based connections. Industrial Defender provides a single solution for this environment with the Industrial Defender Security Event Management (SEM) solution.

- Industrial Defender SEM** is a purpose built event and log aggregator appliance that is designed to monitor all of the critical cyber assets found on typical power transmission energy management systems (EMS) and remote substation environments. The SEM supports scalable architectures for centralized and remote deployments. In addition, the SEM is control system agnostic, it is capable of collecting events and logs from any EMS system and the associated networking components. Preconfigured compliance reports are standard and an AutoAudit™ report also available.

- **Industrial Defender Managed Security Service (MSS)** 24x7 event monitoring and management service to monitor security of plant electronic security perimeter and critical cyber assets. This service is focused only on events generated within the DCS and all monitored IP devices and offer analysis, escalation and reporting to help meet compliance audit attestation.

PERIMETER AND NETWORK SEGMENTATION

Key Challenge

The perimeter between the Enterprise Corporate IT network and the environments where Critical Cyber Assets operate must be properly defined, secured and documented. Access Points (Firewalls, Routers, or UTM devices) must be implemented to restrict access to CCA devices. These access points must be enabled to monitor and log all legitimate, illegitimate or any attempts to access the environment.

Security Challenges

Key Requirements

Utilities must define the Electronic Security Perimeters (ESPs) around each Critical Cyber Asset, and any devices used as **Access Points (firewalls, routers, UTM devices) must be documented**

The **technical and procedural mechanisms** for providing the access control function must be documented, and this documentation should reside in a centralized document management system

All access, either authorized or attempted at the perimeter must be monitored, logged and have the ability to generate an incident notification communication for immediate action 24 x 7.

Documentation relating to the perimeter between the Critical Cyber Asset (CCA) networks and all other networks must be kept up to date and should be maintained in a **document management system**.

Related NERC CIP Requirements

NERC CIP-005 – Requires the identification and protection of Electronic Security Perimeter(s) inside which all Critical Cyber Assets reside as well as access points on the perimeter

CIP-005 R1. Electronic Security Perimeter – *The Responsible Entity shall ensure that every Critical Cyber Asset resides within an Electronic Security Perimeter. The Responsible Entity shall identify and document the Electronic Security Perimeter(s) and all access points to the perimeter(s).*

CIP-005 R2. Electronic Access Controls – *The Responsible Entity shall implement and document the organizational process and technical and procedural mechanisms for control of electronic access at all electronic access points to the Electronic Security Perimeter(s).*

CIP-005 R3. Monitoring Electronic Access – *The Responsible Entity shall implement and document an electronic or manual process(es) for monitoring and logging access at access points to the Electronic Security Perimeter(s) twenty-four hours a day, seven days a week*

CIP-005 R5. Documentation Review and Maintenance – *The Responsible Entity shall review, update, and maintain all documentation to support compliance with the requirements of Standard CIP-005*

Other Distribution System Network Challenges:

- Using dual or triple homed historians to interconnect with external systems can pose a significant security vulnerability
- Using outdated or end of life firewalls or routers at the plant perimeter can pose a significant cyber risk
- Operating distribution management system resources on a flat network can expose the network to cyber security risk

- Scanning of the network by the enterprise IT department can affect the availability and performance of the network environment
- Network and system resources within the perimeter that are managed and operated by multiple parties can present significant cyber risk to the environment.
- Lack of clear demarcation and ownership for the network and system administration of critical cyber assets, presents a significant cyber risk to the environment.

Industrial Defender Solution

Weak perimeter access controls and poor network segmentation practices are some of the most common findings in over 100 security assessments performed on critical infrastructure systems by Industrial Defender. Properly implementing and maintaining a solid perimeter can be effective in blocking external cyber threats before they have a chance to impact critical system components.

- **Industrial Defender Electronic Security Perimeter (ESP)** solution combines the Industrial Defender Security Event Manager (SEM) with Fortinet FortiGate Unified Threat Management (UTM) products. FortiGate UTMs include multiple security technologies in a single device (firewall, in-line intrusion prevention, antivirus, VPN and content filtering, as well as a high availability option). The integration of the SEM with the FortiGate UTMs provides the benefits of multiple defense layers in a single, easily configured solution.
- **Industrial Defender Access Manager** provides access control to communication endpoints within the security perimeter. Access Manager supports both centralized (tethered) and decentralized (untethered) access control for both dialup and IP based devices.
- **Industrial Defender Security Event Manager (SEM)** collects events and logs from firewalls, routers, servers, workstations, PLCs, controllers, and historians, and provides alerts on events of interest using both threshold and signature based methods. The SEM provides standard operational and compliance reports NERC audit attestation.
- **Industrial Defender Managed Security Service (MSS)** 24x7 event monitoring and management service to monitor security of plant electronic security perimeter and critical cyber assets. This service is focused only on events generated within the DCS and offer analysis, escalation and reporting to help meet compliance audit attestation.
- **Industrial Defender Professional Services** Network Architecture Review, Vulnerability Assessment and NERC Gap Analysis services. Regulations are not prescriptive and leave it up to the user to figure out how to establish security access controls. A firewall alone is not enough proof to demonstrate control of a perimeter, many sites still have “dual homed” historians acting as the firewall. Having professionals review the architecture, perform a vulnerability assessment or perform a compliance gap analysis is highly recommended.

SECURING CONTROL ROOM CRITICAL CYBER ASSETS (CCAs)

Key Challenge

Critical Cyber Assets (CCAs) that operate in the distribution management system control room have additional security requirements largely based on NERC-007 which can present electric power asset owners and operators a significant challenge given the large number of legacy systems in place. Securing the control room environment within the power transmission system is critical.

Security Challenges

Key Requirements

Control room operators should require system administrators to implement **test processes and procedures** and implement **change management** practices for CCA devices. This includes servers and workstations inside the Control Room that must operate 24 x 7. Detecting changes that have been made to these systems is vital in keeping the environment secure and also having the ability to support an audit.

For CCA devices in the Control Room and out in the field, system administrators must first know what minimum **ports and services** must be allowed to be operational for the function of operating the system, then they must report on any change of use in these ports and services.

Patch Management is a significant issue in SCADA, EMS, and Industrial Control Systems because of the high availability requirement and legacy system constraints. System administrators who need to comply with NERC CIP now only have 30 days from when a patch is ready to test the patch, then decide and document if they will use the new patch or leave the system un-patched. A process should be in place to implement an emergency patch when the risk is too high to wait for downtime.

The deployment of **Anti-virus** in the Control Room environment is a difficult problem to solve due to limited access to the internet for signature updates and the potential risk that new signature updates will disrupt or crash critical systems or applications that are vital to the operation of the plant environment. Many legacy systems will not perform efficiently with the added CPU and memory requirements that are consumed by the antivirus process. It's a well known fact that host based anti-virus solutions can impact the availability of operator workstations if not properly configured. As a result many control system have no host protection in place at all. Application white listing is another approach to malware prevention.

Account Management is a common security issue in

Related NERC CIP Requirements

NERC CIP-007 – Requires Responsible Entities to define methods, processes, and procedures for securing those systems determined to be Critical Cyber Assets, as well as the non-Critical Cyber Assets within the Electronic Security Perimeter(s).

CIP-007 R1. Test Procedures – *A testing process must ensure that new Cyber Assets and significant changes to existing Cyber Assets within the Electronic Security Perimeter do not adversely affect existing cyber security controls*

CIP-007 R2. Ports and Services – *The Responsible Entity shall establish and document a process to ensure that only those ports and services required for normal and emergency operations are enabled.*

CIP-007 R3. Security Patch Management – *The Responsible Entity shall establish and document a security patch management program for tracking, evaluating, testing, and installing applicable cyber security software patches for all Cyber Assets within the Electronic Security Perimeter(s)*

CIP-007 R3. Malicious Software Prevention – *The Responsible Entity shall use anti-virus software and other malicious software (“malware”) prevention tools, where technically feasible, to detect, prevent, deter, and mitigate the introduction, exposure, and propagation of malware on all Cyber Assets within the Electronic Security Perimeter(s) (ESPs).*

CIP-007 R5. Account Management – *The Responsible Entity shall establish, implement, and document technical and procedural controls that enforce access, authentication of, and*

the control room environment when operators share accounts and passwords, and when these systems often operate in isolated workgroups and not under a single set of group domain policies. Enforcement of secure account management practices and procedures is critical to demonstrating audit compliance.

Critical Cyber Asset (CCA) devices must be able to generate **security events or alerts** produced at the host operating system level or by the application layer, and make that data available to a centralized monitoring system.

accountability for, all user activity, and that minimize the risk of unauthorized system access.

CIP-007 R6. Security Status Monitoring – *The Responsible Entity shall ensure that all Cyber Assets within the Electronic Security Perimeter, as technically feasible, implement automated tools or organizational process controls to monitor cyber security system events.*

Other Control Room Challenges:

- **System Performance** issues are common with legacy Industrial Control and SCADA systems. Many of these systems do not have adequate system resources like additional CPU and memory allocation to run additional security programs like Antivirus software and host monitoring.
- Almost all SCADA and Industrial Control Systems use **Clear Text Protocols**, which are highly vulnerable to data manipulation and commands can be routed.

Industrial Defender Solution

Many of the challenges in securing the critical cyber assets inside the control room include monitoring and detecting cyber security intrusion without impacting system availability, reliability or performance. Our approach in dealing with these challenges is to leverage purpose built solutions that are passive and have been tested to ensure network, and CPU bandwidth are not consumed even on older systems. Our **Defense-in-Depth** solutions include a defense perimeter to establish an **electronic security perimeter** and **demilitarized zone** for the system.

The next component of a defense-in-depth security approach is to monitor and detect for operational anomalies. Control systems tend to be static and can easily be baselined. Once a baseline set of thresholds are in place it should be easy to detect the change and raise an alert if the system begins to behave in an abnormal way if a comprehensive monitoring solution is in place. There are many reasons that could cause a stable system to become unstable. For example the system could be impacted if a change is made to the system or a patch is applied. It is possible that a compromise of the system has occurred because the system becomes increasingly vulnerable to attack over time through reluctance to patch the core system resources. A **Network Intrusion Detection System (NIDS)**, **Host Intrusion Detection Systems (HIDS)** and a **Security Event Management (SEM)** device are an effective way to monitor and manage the network, host and application health of the control room environment without compromising the operational performance of the network. "You cannot control what you do not measure."

The NERC CIP drafting team recognized this and dedicated much of the CIP-007 standard to Patch, Change, and Account management. While meeting these requirements may be much easier to manage in an Enterprise IT environment, the challenges of an always-on operational environment made up of many legacy systems poses unique issues.

SECURING FIELD DEVICE CRITICAL CYBER ASSETS (CCAs)

Key Challenge

The Critical Cyber Assets (CCAs) that operate in the field in substation environments such as DCS controllers, PLCs, RTUs, IEDs, and embedded devices used for CEMS must be effectively monitored and secured and are also subject to parts of NERC CIP-007.

Security Challenges

Key Requirements

Since most of the CCAs that operate in the field are embedded systems, many do not have the capability to meet the Account Management, Antivirus, and most other requirements in CIP-007. They do have ports and services that must comply, so utilities must know and monitor the use of ports and services on field devices.

The same holds true for monitoring the security status of field devices. If a CCA field device generates security event logs, then these should be monitored by a central system.

Almost all SCADA and Control System protocols are based on clear text, which means that the data and passwords can be viewed by everyone. How are these legacy protocols secured within your plant environment? Damaging commands can be sent into the control system network without your control or knowledge. It is now public knowledge that the capability exists to send corrupted packets that could crash PLCs, RTUs, IEDs, and many field devices.

Related NERC CIP Requirements

NERC CIP-007 – Requires Responsible Entities to define methods, processes, and procedures for securing those systems determined to be Critical Cyber Assets, as well as the non-Critical Cyber Assets within the Electronic Security Perimeter(s).

CIP-007 R2. Ports and Services — *The Responsible Entity shall establish and document a process to ensure that only those ports and services required for normal and emergency operations are enabled.*

CIP-007 R6. Security Status Monitoring — *The Responsible Entity shall ensure that all Cyber Assets within the Electronic Security Perimeter, as technically feasible, implement automated tools or organizational process controls to monitor system events that are related to cyber security.*

Industrial Defender Solution

Industrial Defender cyber security solutions can address the security and compliance requirements for CCA's that are not typical computing devices which operate in clean control room environments.

- **Industrial Defender Access Manager** provides access control to communication endpoints within the security perimeter. Access Manager enables selectable port security assignments and provides comprehensive auditing and reporting functionality.
- A **Network Intrusion Detection System (NIDS)**, **Host Intrusion Detection Systems (HIDS)** and a **Security Event Management (SEM)** device are an effective way to monitor and manage the critical cyber assets in the field, without compromising the operational performance of the network.

Industrial Defender Professional Services Network Architecture Review, Vulnerability Assessment and NERC Gap Analysis services. Minimizing the ESP can have a significant cost benefit if properly designed. Regulations are not prescriptive and leave it up to the user to figure out how to establish.



Conclusion

In order to effectively maintain the reliability and availability of the bulk electric system power distribution systems must be adequately secured against cyber security risks and vulnerabilities. With over 17 years of industrial control and SCADA expertise, Industrial Defender can assist bulk electricity asset owners and operators with securing their power transmission systems while also supporting compliance mandates like the North American Electricity Reliability Corporation Critical Infrastructure Standards (NERC CIP). For more information on our industry leading cyber security solutions please visit us at <http://www.industrialdefender.com> or contact us at Tel-508-718-6700.