



# New Perspectives on NERC CIP Access Management

By John Shaw, Executive VP  
GarrettCom, Inc.

A major objective of NERC CIP cyber security standards is to ensure that only specifically authorized people are able to electronically access control systems and Intelligent Electronic Devices (IEDs) that can affect critical power grid operations. To demonstrate NERC compliance, utilities must be able to prove that related protections are in place and vigilantly observed.

As utilities move from learning about CIP standards and related technologies, to the planning and now the implementation phase for CIP processes, CIP teams are gaining additional perspectives into the scope, interrelationships and evolving requirements of secure access management. These perspectives may be grouped into three areas:

## Real world implementation

NERC CIP standards are intentionally unspecific in many areas, allowing some interpretation and customization to the current environments of each utility. While there are many important mandates, each utility has the flexibility to adapt implementation specifics to take into account local variations such as existing IT infrastructure, substation communications, control system capabilities, and operating procedures.

## Preparation for “Life under NERC CIP”

NERC CIP compliance is not a static achievement. Becoming compliant is not just getting to “done”, but rather getting into position to execute ongoing procedures. Successful compliance includes looking ahead and implementing tools and processes that are the least burdensome to sustain over time.

## Anticipation of ongoing change

Cyber security is a dynamic landscape, continually altered by new threats, developing technology and inevitable changes to NERC CIP requirements as they undergo refinements of technology and of the definition of critical assets. Current implementations must remain flexible enough to accommodate a changing technological and regulatory environment.

Successful management of each of these perspectives affects system architecture, network architecture and operations processes.

## Implementation in the Real World

The basic elements of access management for CIP include:

- Identifying Critical Cyber Assets (CCAs) -- applicable to all of NERC CIP,
- Establishing an Electronic Security Perimeter around CCAs,
- Identifying and screening key personnel,
- Defining user profiles for each person, i.e., limit what they are allowed to access,
- Establishing a 2-factor authentication mechanism for users,
- Authorizing each permitted access event against individual user profiles,
- Logging all accesses and provide related reports and audits,
- Identifying, logging and alerting on all exception events,
- Supporting ongoing changes to users, CCAs, the network and device passwords, and
- Providing back-up and recovery tools for access management systems and processes.

These specific requirements can be met in a variety of ways, but an overall goal is to tailor the implementation to limit the disruption to the current operating environment and to simplify the overall project.

Many utilities already have a user authentication infrastructure within their Enterprise IT environment. Common technologies include Microsoft Active Directory, used for coordinating user authentication over multiple systems, and RSA SecurID servers, used to provide two-factor authentication, i.e., a password (something you know) and an RSA token (something you have). Most current IEDs or older control systems do not support these services directly.

## Access Management Systems Can Integrate IT and Substation Networking

A new CIP Access Management System (AMS) can bridge the substation world with current IT tools both by functioning as the secure gateway for legacy devices and by interoperating with existing Enterprise authentication services.

One possible system architecture for initial implementations is shown in **Figure 1**. The basic steps for user access to IEDs in this architecture would be:

- The end user activates a secure access client software application on their PC.
- The end user is transparently connected to the AMS server, which obtains credentials from the end user and interrogates Active Directory and/or RSA SecurID servers as well as its internal security profile data base to authenticate the user and validate authorized target devices.

- The end user clicks on a desktop directory icon for the authorized target IED.
- In active coordination with the router/firewall/gateway at the substation, the AMS establishes a secure connection to the target IED and connects the end user to the IED, as if to the IED's front panel port.
- AMS client software on the end user PC selects and initiates the appropriate vendor-specific application program on the PC for use with this IED, if applicable.
- The AMS server logs every access event and, optionally, all activity during the user session.
- The AMS retrieves additional event logs periodically from the substation router/firewall/gateway and receives any exception alerts for additional security monitoring and audits.

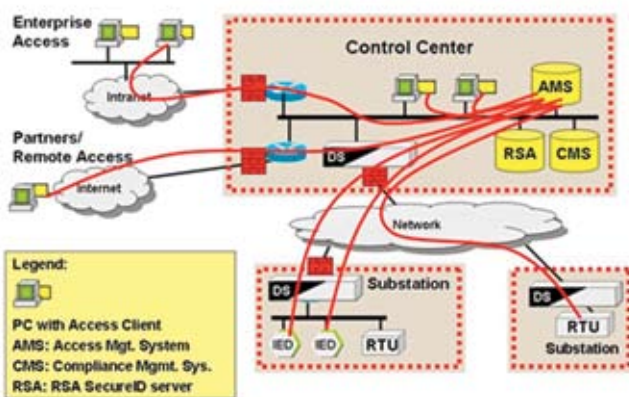


Figure 1: Access Management Architecture

Some utility cyber security implementations have additional active mechanisms in place to detect and alert on forms of attack that are more complex than a direct login attempt. An example is an Intrusion Detection System (IDS) that looks for patterns of attack such as aggressive transmissions to exposed protocol ports or other vulnerabilities in host operating systems. IP Firewalls at the control center and at substations may also detect basic network attacks (or simply misguided packets) that also constitute security events.

To manage these diverse sources it is desirable to link firewall events, AMS events and IDS events to a common Security Event Management console, as shown in **Figure 1**.

Access Management must also integrate with the substation network itself. For ease of initial implementation, an AMS may interoperate with a wide variety of substation gateway devices on a secure basis. Possible substation gateways may include existing serial communications processors (e.g., SEL 2020/2030), WAN router/firewalls, some serial-IP terminal servers, telephone-line-sharing switches, and other vendor-specific devices.

While there may be many devices that interoperate with an AMS for interfacing to serial IEDs, some may fail to provide either a complete Electronic Security Perimeter function for the substation (e.g., firewall non-AMS-related SCADA connections) or the required level of event logging. A comprehensive substation access gateway would incorporate:

- WAN connectivity,
- IP routing,
- Stateful (“TCP connection-aware”) IP firewall,
- IPsec VPN,
- Direct connectivity for serial devices, Ethernet devices and Ethernet LAN, and
- Secure connection management with the AMS for both serial and IP sessions including logging of sessions and alerting of any exceptions.

Many utilities will end up with more than one configuration type for substation communications, accommodating different situations. Variations include use of an integrated router/firewall/gateway, use of a secure telephone-line-sharing switch for dial-up substations, and the use of multiple devices in series, such as a router/firewall with a serial communications processor. (**Figure 1** shows how an AMS architecture can work with this variability.)

### Living in a NERC CIP World

Utilities may complete implementation of a CIP-compliant framework by the appointed ready date, July 1, 2009, but compliance will never be truly completed. Compliance requires keeping security technologies current and diligence at administrative tasks of record keeping, change management and periodic audits. It is critical that tools be put in place to minimize this administrative overhead.

One such tool is an Access Management System that also supports additional compliance management tasks beyond pure access control. An AMS can be used to automate the maintenance of records in ways that promote flexibility and reconfiguration. For example:

- The AMS holds an inventory of all the IEDS and systems that users may have access to. By flagging those devices designated as Critical Cyber Assets (CCAs), the AMS becomes a repository of the current CCA inventory information and can be used to produce audit reports and to manage changes to the official CCA list.
- An authorized user list may be used as a control point for physical access control systems and other personnel-related CIP functions.
- An AMS can provide scheduled updates of individual or related groups of IEDs – or of specific IEDs when special concerns arise, in compliance with the CIP requirement that all IED and system passwords be periodically changed.
- An AMS can pull log files from remote gateways and archive these automatically on a regular basis for audit purposes, without operator intervention.
- An AMS can manage other file types, such as configuration files and IED logs, and assist with administering and updating software for selected substation devices.

Secure access procedures designed to keep intruders out can also make access difficult for authorized users. A well-implemented AMS architecture can reverse this effect and make remote access even easier than before CIP.

By using an AMS, such as the Crossbow™ Secure Access Manager, which is purpose-built for the substation environment rather than using generic IT access tools that do not understand the protocols, devices and software applications common to utilities, it is possible to enhance end user productivity in ways such as:

- Organizing the IEDs that are relevant to that particular user -- essentially only those that the user is allowed to access -- into graphic-assisted directories, grouped into various combinations of region, substation or device type.
- -Supporting PC software that provides click-through access to the target IEDs, making the network connection and session logging functions transparent to the user.
- Associating the appropriate vendor-specific software application on the user's PC, such as AcSElerator, WinECP or Enervista, with each target IED, enabling AMS client software to automatically launch this application, further simplifying on-demand IED access.

## Anticipation...

NERC CIP standards have been criticized for not going far enough in securing the power grid from sophisticated attacks. Researchers have made considerable efforts to identify and demonstrate potential security breaches, revealing vulnerabilities that the minimum CIP standards may not remedy. Also, the current standards only apply to the relatively small percentage of overall utility assets considered "critical" under the definitions of the standard. While the primary transmission grid is addressed, billions of dollars of utility assets are left unprotected.

Regulators have signaled that the CIP standards will likely be expanded. This will include technical details from additional expert stakeholders to strengthen defenses and to react to the evolving nature of cyber threats. The standards will also likely spread

to more utilities and substations, if not by regulation, than at least by "best practices" as IT influences extend more into substations and as utilities become generally accustomed to cyber protections as the normal way of business.

Implementers are already taking steps to prepare for such change. At a detailed level, an AMS and remote gateways may be selected that have a wide variety of embedded security technologies. As standards evolve, there will be flexibility in implementing one or a combination of technologies, such as IPsec Virtual Private Networks (VPNs) with various strong encryption and key exchange algorithms, SSH port forwarding, Secure FTP, and SSL protocols applied to both serial and IP-based end devices. There is no need to rely on one specific technique becoming the preferred standard, since highly flexible devices are available.

Similarly, the server technology for centralized server elements of the AMS can be built on standard IT platforms so that they benefit from evolving major vendor tools and standard IT security practices.

Substation networking flexibility becomes even more important as more substations, including more distributed and smaller substations, fall within the utilities' cyber security plans. While some access management architectures feature a single vendor-specific substation gateway option, other AMS architectures utilize a wide variety of remote gateway types. Options may include multiple gateway form factors, support for different WAN network services, preferred partner products for complementary requirements, and a generally open secure network architecture to integrate additional products as required over time.

Additionally, more enhanced cyber security functionality will be required locally within major substations over time. This may include local IDS systems or user authentication services within the substation, with databases and administration tied into central AMS servers and processes. Deployment should include a roadmap supporting a substation-based IDS/authentication server.

## Choose Adaptive Technologies and Keep Moving Forward

The clock is ticking. Utilities are only several months from the mandatory NERC CIP compliance date. Implementation is accelerating, even while the learning curve continues for many. Fortunately, utilities have many potential technologies and partners to work with, including access management solutions created specifically for the world of substation operations.

Project teams can find flexible, proven access management technologies that can adapt to particular utility environments to make implementation simpler, less disruptive, less risky and less costly. Ongoing processes can be highly automated to reduce administrative overhead and system interfaces can be designed for ease-of-use to increase end-user productivity accessing remote substations.

And, while it is hard to anticipate all the new cyber security threats and regulations that may emerge, it is possible to implement open-ended solutions that cover many extra bases and leave future options open. The common theme for overall success is to pick a substation-centered security solution that is highly adaptive, simplifying the initial project and facilitating long-term operations. ■

## About the Author

**John M. Shaw** is Executive Vice President of GarrettCom, Inc., a leading supplier of substation-hardened networking products. Shaw leads GarrettCom's planning for NERC CIP cyber security compliance solutions and is an active speaker and writer on network security. He has more than 25 years experience in planning utility- and carrier-grade data networks, telecommunications technical marketing and executive management, including positions at Tellabs, Newbridge Networks (now Alcatel-Lucent) and NYNEX (now Verizon).

Contact him at [jshaw@garrettcom.com](mailto:jshaw@garrettcom.com)