

# MEETING NERC 1300 SECURITY OBJECTIVES FOR REMOTE IED ACCESS USING TWO-FACTOR AUTHENTICATION

**Deryk Yuill, Bow Networks**

## **Introduction**

Remote IED maintenance has proven a real value to utilities, and has saved countless hours in travel time to substations. Modern networking technology has allowed this function to be implemented inexpensively, in many cases sharing a communications channel with other functions. With this ease of access comes increasing concerns over security. Given the rather crude login control mechanisms in most IEDs (single user name & password), IT security groups have become increasingly resistant to providing this access capability. Furthermore, new requirements brought on by NERC 1300 will require utilities to bolster the security for remote access.

This paper will examine the requirements of NERC 1300, and explore an advanced authentication mechanism designed to address these requirements, which provides the following benefits:

- centralized user administration
- individual user accounts
- audit log
- secure, two-factor authentication
- encryption

Lessons learned during field deployment of such a system shall be discussed.

## **NERC 1300 Overview**

NERC Standard 1300 – Cyber Security, is being developed as a permanent replacement for NERC 1200, the urgent action standard for cyber security, which will expire in August, 2005. Note that as of this writing, NERC 1300 is still under development, and subject to change. The reader is encouraged to read both the standard itself, and the companion Frequently Asked Question (FAQ) document. These, and other supporting documents, are available at:

<http://www.nerc.com/~filez/standards/Cyber-Security-Permanent.html>

NERC 1300 consists of the following sections:

- 1301 – Security Management Controls
- 1302 – Critical Cyber Assets
- 1303 – Personnel and Training
- 1304 – Electronic Security
- 1305 – Physical Security

- 1306 – Systems Security Management
- 1307 – Incident Response Planning
- 1308 – Recovery Plans

Much of NERC 1300 deals with broad organizational issues, control center cyber security, and other issues beyond the scope of this paper. NERC 1300 (unlike NERC 1200) does include certain substation assets within its scope. The following section identifies those requirements within the various sections of NERC 1300 that impact substations in general, and remote IED access in particular.

## **NERC 1300 from the substation perspective**

### **1301 – Security Management Controls**

Much of this section deals with the formal processes required in a utility to manage cyber security. The key point that requires specific action with respect to IED access is Access Control:

- A list of personnel authorized to access critical cyber assets (defined in 1302) must be created and managed. Formal processes must be in place to create new user accounts, periodically review account privileges, and terminate user privileges when no longer required. It is important to note that this is to be done on a per-system, per-application basis.
- A responsible entity must be designated to administer access privileges. Typically, this would be a manager with responsibility for the IEDs in question.
- In addition, a separate entity should periodically review access privileges. Typically, this would be a separate security or audit department.

### **1302 – Critical Cyber Assets**

This section deals with defining which devices and systems (“Cyber Assets”) are to be considered critical, and consequently under the jurisdiction of NERC 1300. There is essentially a two-part test for this:

1. Does the cyber asset support a critical bulk electric system asset?
2. Is the cyber asset accessible using a routable protocol, or dial-up connection?

Critical Bulk Electric System Assets are defined to include telemetry, monitoring and control, and transmission substations. NERC standard 200 defines the bulk electric system as being above 35 kV, or as approved in a tariff filed with FERC. The determination of criticality is up to individual utilities. Note that there is currently much discussion surrounding these definitions and they may be clarified in future versions of 1300 or other referenced standards.

Consequently, RTUs, relays, and other IEDs in transmission substations, accessible by dial-up or IP network, are subject to the provisions of NERC 1300. Devices accessible via dedicated modem are excluded.

### **1303 – Personnel and Training**

Personnel having access to critical cyber assets are subject to a range of measures relating to training and background checks. It is expected that these measures will be implemented in a broad fashion across an organization.

### **1304 – Electronic Security**

The electronic security perimeter is defined as the logical border surrounding the critical cyber assets. It does not include the communications links connecting discrete electronic perimeters. For example, typical electronic security perimeters would exist at the control center, and at *each* substation containing critical cyber assets. The perimeter would include the modems or routers at each end, but not the telecommunications infrastructure in between.

Organizational, Technical, and Procedural controls must be implemented to control all electronic access points to the electronic security perimeter *and* the critical cyber assets within that perimeter.

Access must be monitored, 24 hours a day, 7 days a week, for:

- Authorized access
- Failed access attempts
- Intrusions

Strong authentication of accessing parties is required. Strong authentication is required to involve at least two of the following three factors:

- What a person knows (eg password or PIN)
- What a person has (eg token or smart card)
- What a person is (eg biometric characteristic)

### **1306 – Systems Security Management**

This section adds a number of significant requirements with respect to substation IED access management, including:

- Ability to audit user activity
- Individual user accounts (as opposed to group accounts)
- Access privileges must be reviewed at least semi-annually
- All information used to manage access to critical cyber-assets must be backed up on a regular basis.

### **Summary of requirements for a NERC 1300 compliant remote IED access mechanism**

From the perspective of providing secure remote access to substation IEDs that meets the requirements of NERC 1300, the following requirements must be met:

- Access rights must be granted on a per IED basis
- Each individual must have their own individual user account
- Audit logs must be created, documenting successful and failed accesses
- Strong (2-factor) authentication must be provided.

- Administration of user privileges may only be done by designated individual(s).
- Access privileges must be easily auditable.
- Authorized individuals are required to be trained in security procedures, and are subject to background checks.

## **Authentication**

Authentication is the process of verifying who, or what, a particular entity is. Entities that may be authenticated include people, devices (eg workstation, IED) and even individual applications running on a particular system.

Note that authentication does not in itself provide any indication as to what the entity is allowed to do. That is the function of *authorization*.

Authentication schemes vary greatly in complexity, and also in their security. In general, security is proportional to complexity.

Authentication schemes are generally classified based on the number of *factors* they use. Factors are “pieces of proof” that the user is who they say they are. Typical factors used for user authentication are:

- What a person knows (eg password or PIN)
- What a person has (eg token or smart card)
- What a person is (eg biometric characteristic)

The more factors used, the more difficult it is to fool, and consequently the more secure the system will be.

## **Password security**

Although widely used, passwords are the least secure of all authentication factors. The main difficulty is that users tend to set their passwords to something easy to remember, which also tends to make them easy to guess.

Standards do exist which define rules for creating strong passwords. An example of this is the US Department of Energy order DOE 205.3. This includes such requirements as:

- Minimum 8 characters
- Upper AND lower case letters AND numbers AND special characters (punctuation)
- Not include common words in any language

This results in passwords such as “aH6f&L8%”. The trouble with these sorts of passwords is that they are so difficult to remember, people write them down, which largely defeats the purpose.

## **Two Factor Authentication**

A common way to greatly enhance the security offered by passwords alone is to require a second factor. A second factor is usually something that the user must possess, such as an ID card, digital certificate, or some form of electronic token. A wide range of such devices exist on the market today.

### **Centralized Authentication**

Since there are many applications in an organization that require users to be authenticated, the preferred architecture is to implement a centralized authentication server that provides authentication services to individual applications. This greatly simplifies the maintenance of user identities within an organization.

It is important to recognize that there is an important procedural component to authentication, as well as the underlying support technology. Since every major application relies on the authentication server, it becomes one of the most important components in an organization's security infrastructure. Administration of this system may only be done by highly trusted individuals, and additions and deletions of users is done only with proper managerial sign-off.

### **Proposed secure access architecture**

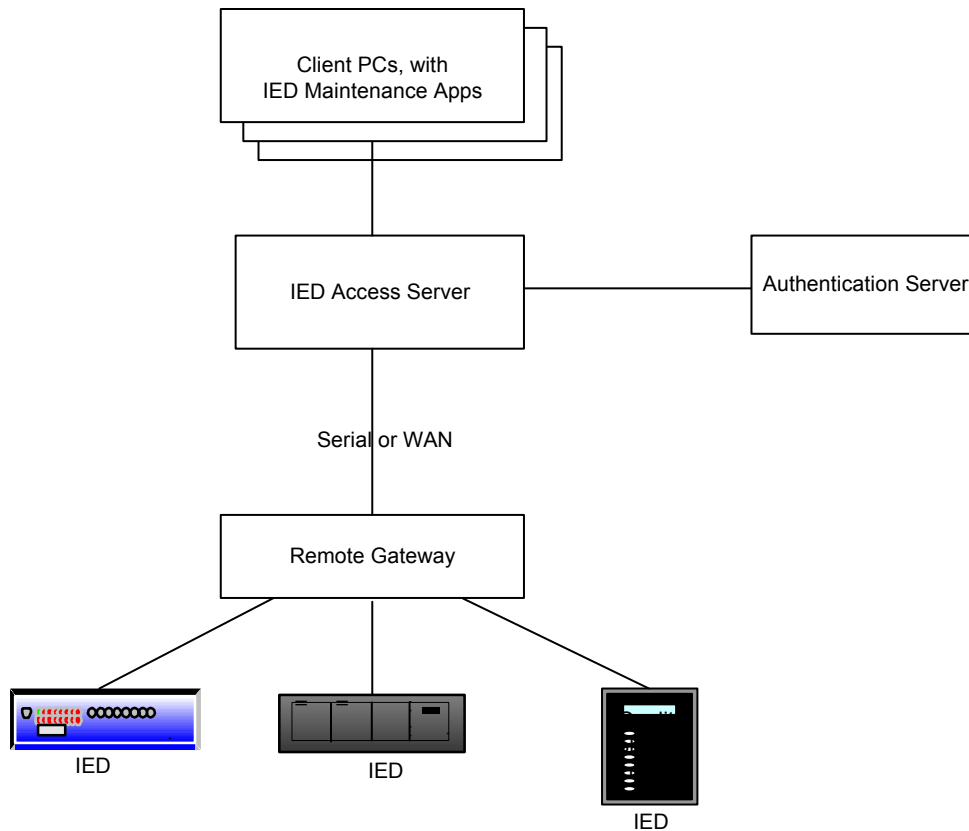
Today's substation IEDs provide only very basic access controls. Often only a single group account is provided, with 1-factor (password) authentication. Furthermore, management of these devices is done on a per-IED basis. Thus, eliminating privileges for a particular user would involve:

1. define a new password
2. change password in every IED
3. notify all authorized users of the new password.

Clearly, this is unrealistic.

An architecture is required that can work with the constraints of today's IEDs, and overlay their basic security features with a more sophisticated access management system.

In conjunction with several utilities concerned with meeting NERC 1300 requirements, the following architecture was developed and implemented.



The main components of the architecture are:

- Client PC, running the various IED applications
- IED Access server, which provides the access control mechanisms
- Remote gateway, which provides physical connectivity in the substation
- Authentication server

The key to the architecture is providing a controlled, secure connection to the substation gateway device. Depending on the substation, this may be best provided using a dial-up connection, or WAN. Encryption may be needed in certain cases.

It was the objective in all involved utilities to leverage their installed base of gateway devices wherever possible. This objective was achieved by implementing a secret, strong password between the gateway and the server. This password is only known to the IED access server. Thus, remote access is only possible via this server, even if the gateway is dialed directly.

This results in the IED access server being involved in every remote IED connection, which allows it to securely perform the following required functions:

- Control IED access on a per IED basis
- Maintain individual user accounts
- Creation of audit logs
- Perform user authentication. Interface to external authentication systems, such as commonly used for 2-factor authentication.

- Control administration of access privileges.
- Provide reports for auditing access privileges.

## **Lessons learned**

Field deployment of this architecture is only just beginning, at time of writing. However, there are a number of considerations that have already been identified:

- Achieve organizational buy-in. Deploying a secure IED access system requires involvement from more than just the protection department. The IT security folks will surely need to be involved, as well as the group that operates the communications infrastructure. It is critical to the success of the project to involve them early, and ensure an architecture is designed to satisfy all constituencies.
- Ensure the system works for both remote users, as well as users in the substation.
- Some 2-factor schemes can be reduced to 1-factor schemes, by poor user habits (eg writing the PIN number on the back of a security token).

As these projects proceed, there will be additional lessons learned. An updated version of this paper will be available at <http://www.bownetworks.com/downloads/distributech2005.pdf>