Secure Substation Automation for Operations & Maintenance

Byron Flynn
GE Energy

1. Abstract

Today's Cyber Security requirements have created a need to redesign the Station Automation Architectures to provide secure access for Operations and Maintenance Systems and Personnel. This paper will review several architectures being used and planned by utilities today.

Several real world architectures will be reviewed including

1. Serial SCADA & Dial-up Maintenance,

2. Serial SCADA & LAN based Maintenance,

3. Combined LAN for SCADA and Maintenance and;

4. Separate SCADA WAN/LAN and Maintenance WAN/LAN.

Each architecture will include various methods of User authentication and secure access to various station IEDs including relays, meters, RTUs, PLCs and station servers. This will include configuration access, maintenance access, and manual and automatic data retrieval of fault data.

2. Background

In August of 2003, NERC issued the Urgent Action Cyber Security Standard 1200. This standard was set to expire in August of 2005 but was given a 1 year extension. A new standard originally called Standard 1300 and now named the NERC Critical Infrastructure Protection (CIP) Cyber Security Standard.

As of January 16, 2006, the current version of the document is Draft 4 [1]. The section headings are:

CIP-002 Critical Cyber Asset Identification

CIP-003 Security Management Controls

CIP-004 Personnel and Training

CIP-005 Electronic Security Perimeter(s)

CIP-006 Physical Security

CIP-007 Systems Security Management

CIP-008 Incident Reporting and Response Planning

CIP-009 Recovery Plans for Critical Cyber Assets

According to NERC:

Bulk Electric Systems are "defined by the Regional Reliability Organization, the electrical generation resources, transmission lines, interconnections with neighboring systems, and associated equipment, generally operated at voltages of 100 kV or higher. Radial transmission facilities serving only load with one transmission source are generally not included in this definition." [2]

Critical Assets are those "facilities, systems, and equipment which, if destroyed, degraded, or otherwise rendered unavailable, would affect the reliability or operability of the Bulk Electric System." [3]

Critical Cyber Assets are "Programmable electronic devices and communication networks including hardware, software, and data." [4] "Critical Cyber Assets are further qualified to be those having at least one of the following characteristics:

R3.1. The Cyber Asset uses a routable protocol to communicate outside the Electronic Security Perimeter; or,

R3.2. The Cyber Asset uses a routable protocol within a Control Center; or,

R3.3. The Cyber Asset is dial-up accessible." [5]

3. Definitions [6]

3.1 Certificate Authority

A certificate authority or certification authority (CA) is an entity which issues digital certificates. In cryptography, a public key certificate (or identity certificate) is a certificate which uses a digital signature to bind together a public key with an identity – information such as the name of a person or an organization, their address, and so forth. The certificate can be used to verify that a public key belongs to an individual.

CHAP
Challenge Handshake Authentication Protocol is an access control protocol for dialing into a network that provides a moderate degree of security. CHAP uses encryption of random values with the client's password for authentication.

HTTPS
Hyper Text Transport Protocol Secure is a secure version of HTTP, the communication protocol of the World Wide Web, invented by Netscape Communications Corporation to provide authentication and encrypted communication. Instead of using plain text socket communication, HTTPS encrypts the session data using either a version of the SSL (Secure Socket Layer) protocol or the TLS (Transport Layer Security) protocol, thus ensuring reasonable protection from eavesdroppers, and man in the middle attacks.

3.2 Identification Factors

There are generally four Identification Factors that are used for authentication. None of them are entirely foolproof, but in order of least to most secure, they are:

1. What You Know – passwords are widely used to identify a User, but only verify that somebody knows the password.
2. What You Have – digital certificates in the User's computer add more security than a password, and smart cards verify that Users have a physical token in their possession, but either can be stolen.
3. What You Are – biometrics such as fingerprints and iris recognition are more difficult but not impossible to forge.
4. What You Do – dynamic biometrics such as hand writing a signature and voice recognition are the most secure; however, replay attacks can fool the system.

PKI
Public Key Infrastructure is an arrangement that provides for third party vetting of, and vouching for, User identities. It also allows binding of public keys to Users. Public Keys are typically in certificates.

PPP
Point-to-Point Protocol is the most popular method for transporting IP packets over a serial link between the User and the ISP. Developed in 1994 by the IETF, PPP establishes the session between the User's computer and the ISP using its own Link Control Protocol (LCP). PPP supports CHAP authentication.

SSL
Secure Sockets Layer is the primary security protocol used on the Internet. Originally developed by Netscape, it validates the identity of a website and provides an encrypted connection for transactions. SSL uses HTTPS protocol. Use of SSL requires a certificate from a Certificate Authority.

Secure Connection Relay
In Secure Connection Relay, a client outside the security perimeter establishes an SSL connection with a gateway, which then makes an unencrypted TCP connection to another TCP address on the substation LAN and relays traffic between the SSL connection and the TCP connection.

Secure Terminal Server
In Secure Terminal Server, a client outside the security perimeter establishes an SSL connection with a gateway, which then opens a serial port and relays traffic between the SSL connection and the serial port.

Secure Data Concentrator
This capability provides secure SSL encapsulation for any networked SCADA protocol on the concentrator.

TLS
Transport Layer Security and it predecessor are cryptographic protocols which provide secure communications on the Internet. There are slight differences between SSL 3.0 and TLS 1.0, but the protocol remains substantially the same.

T-F A
Two Factor Authentication requires two authentication factors before accessing a system and is considered strong authentication.

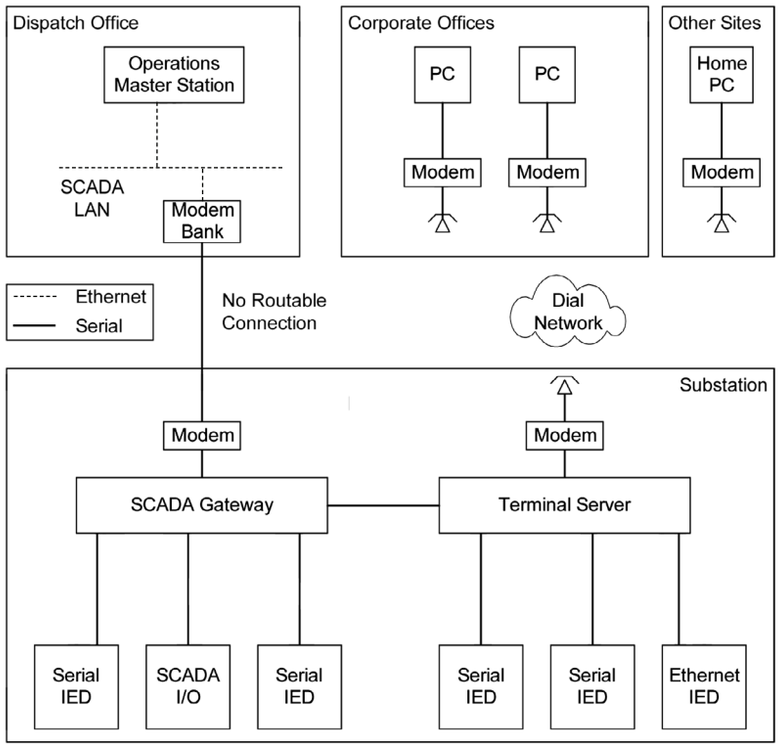

Fig 1.
Existing Architecture.

4. System Architectures

4.1 Introduction

Applying the appropriate level of security to a complex system is one of the biggest challenges utilities are facing today. These challenges are amplified because for security reasons, it is very difficult for utilities to share security best practices outside of the personnel directly responsible with that security. While this paper does not reveal specific architectures being used by any utility, it attempts to outline several typical architectures with various levels of security.

By its nature, security will always be a "cat and mouse" game where new threats require new security methods. Establishing a security strategy also requires a balancing act where any method of restricting access must be balanced with the critical nature of the asset and the limitations placed on employees with substation cyber access rights. It is important and useful to review the various threats to a security system. They are [7]

- the Hacker. The proverbial teenager just looking to break into things. May not even want to do any damage. They often have a lot of computing power and expertise in corporate networking, but typically will not know anything about power systems or utility protocols.
- the Vandal. Indistinguishable from the Hacker except for motive. Wants to break things, and doesn't really care what. Less common than the Hacker, but more dangerous.
- the Terrorist. This is the attacker people are most afraid of, but is actually less likely to occur than many others. Wants to do specific damage and will probably research the target's network and operations. Would need to know something about power systems and utility protocols. To get this information, could enlist the help of...
- the Disgruntled Employee. This is one of the most dangerous of potential attackers, because they already know the utility's security systems, procedures and weaknesses.
- the Competitor. Utilities are required to communicate with, and therefore share networks with, their competitors. The competitor is probably an uncommon but extremely dangerous threats to the utility network because:
  a) utilities cannot simply prohibit all access, but must limit what data competitors can see.
  b) competitors already know about power systems and probably quite a bit about their target's network.
  c) their attack, if it occurs, will likely be subtle, i.e. eavesdropping rather than denial of service, and therefore harder to detect.
- the Customer. Unfortunately, utilities' customers may also be a threat. They are an especially dangerous threat because they often want to commit fraud rather than to simply damage the electrical network. As noted with competitors, the customer's attack may be hard to detect because all they want to do is modify a few key values.

The following portion of this paper reviews several methods of establishing a secure connection to block unauthorized access and allow appropriate access to the two most common types of data in the substation, often referred to as – SCADA or Operational Data and Maintenance or Non-Operational Data. These architectures are representative of systems in-use or being planned by Utilities today.

4.2 Common System

The Figure 1 contains the most common architecture today for access of substation data for Operations and Maintenance personnel.

The Dispatch office connects to the station over a dedicated communications line using a SCADA protocol. The Maintenance Users connect from any computer with a modem to the IEDs through an unsecured port switch. The Unsecured Port Switch can send data to the SCADA Gateway via a standard SCADA Protocol. The connection is made using a SCADA protocol supported by both boxes, commonly DNP. The SCADA Gateway is typically the master and Port Switch is the slave. This connection is limiting and it can be difficult to share data from the SCADA IEDs with the Port Switch. It is also impossible for User's connecting to the Port Switch to access the SCADA IEDs through that connection. Each device must be connected directly to the Port Switch for the remote PCs to access the IEDs.

The need for a Station LAN increases as additional IEDs support Ethernet communications, such as protective relays, RTUs, PLCs, meters, and DFRs. As Ethernet-based IEDs are added to the substation, the common architecture is changed as shown below to support remote connection to the Station LAN.

4.3 Current Station LAN Architectures

Many IEDs contain the ability to communicate via a LAN port. The Figure 2 contains an initial architecture for access of substation data for Operations and Maintenance personnel.

The Port Switch has been replaced by a Terminal Server, which can provide the ability to connect from a remote PC to serial, or Ethernet devices. This capability is provided using PPP. PPP provides the ability to connect to the Terminal Server with Telnet and then tunnel through to the serial IEDs. The Terminal Server would also allow the remote PC to connect directly to the Station LAN. Many Ethernet IEDs and Terminal Servers can also provide web pages to be viewed by browsers connected locally to the Station LAN or remotely via dial-up.

The SCADA Gateway has also been upgraded to include an Ethernet connection to the Station LAN. This provides the ability to remotely access data from the Ethernet IEDs through the Dial-up Port.

4.4 Security

The Port Switch is typically secured with a password only; the Terminal Server can be secured with login IDs and support CHAP. CHAP provides an increased level of security however, it provides only single factor authentication, anyone who has

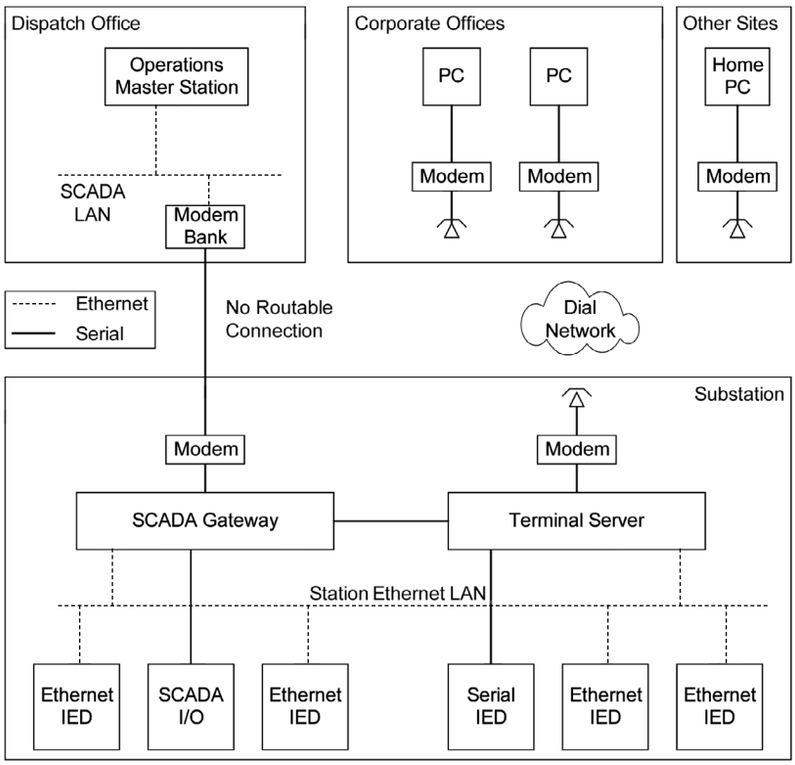

Fig 2.
Existing Architecture with a Station LAN.

the password could log into the Station from any modem. Furthermore, the Ethernet devices would not be secured unless routing was disabled in the Terminal Server between the remote connections and the Ethernet IEDs. Then Ethernet access would not be possible remotely.

5. Secure Architecture #1 – Dial-Up

The gateway meets the NERC security criteria, provides protocol conversion and data concentration for both the Serial and Ethernet IEDs. The gateway also polls those IEDs and concentrates the data in an internal database. Then web pages are generated to display the non-SCADA data providing a convenient tool for viewing fault data from the Stations IED relays together on one web page. Other IEDs can also be displayed including transformer or breaker monitoring and diagnostics, metering, and all the various station analogs including MW loading, voltages, PF, etc.

In order to meet the NERC CIP, two additional capabilities need to be added: the addition of a second authentication factor and the ability to audit successful or unsuccessful login attempts. The architecture shown in Figure 3 illustrates system with the additional NERC CIP functionality.

The system in Figure 3 uses PPP and CHAP providing one authentication factor. SSL and PKI provide a second authentication factor through the use of digital certificates on each PC. Each PC must have SSL and utilize either an additional hardware or software based authorization key before attempting to access the Maintenance Gateway. The Maintenance Gateway will also need to be configured for that User's access and authorization rights. The authorization rights would include rights on the gateway such as View, Control, Configuration or Security Administration and the specific serial or Ethernet IEDs the User is permitted to directly access.

Strong authentication is achieved through the use of the two factors, the User's ID and password (under CHAP) "Something They Know" and either a hardware or software key/certificate "Something They Have".

The gateway also must record and report successful or unsuccessful login attempts. This supports the NERC CIP requirements of "Where technically feasible, the security monitoring process(es) shall detect and alert for attempts at or actual unauthorized accesses. These alerts shall provide for appropriate notification to designated response personnel. Where alerting is not technically feasible, the Responsible Entity shall review or otherwise assess access logs for attempts at or actual unauthorized accesses at least every ninety calendar days." [8].

A useful tool to enable security administration for this architecture and the subsequent architectures is a Certificate Authority. A Certificate Authority provides a convenient method to manage Certificates for the Gateways, Master Stations or PC Users. Some Gateways come with an initial Certificate valid for a specific period of time after which a new certificate would need to be issued. As new Users request access to the stations a new certificate would be generated for that user. This tool could also generate a revocation list when a user's access rights are removed.

5.1 Remote access to IEDs

Once the User has been authenticated by the Gateway, the Station IEDs can be accessed remotely. Serial IEDs are accessed through serial tunneling software on the Gateway.

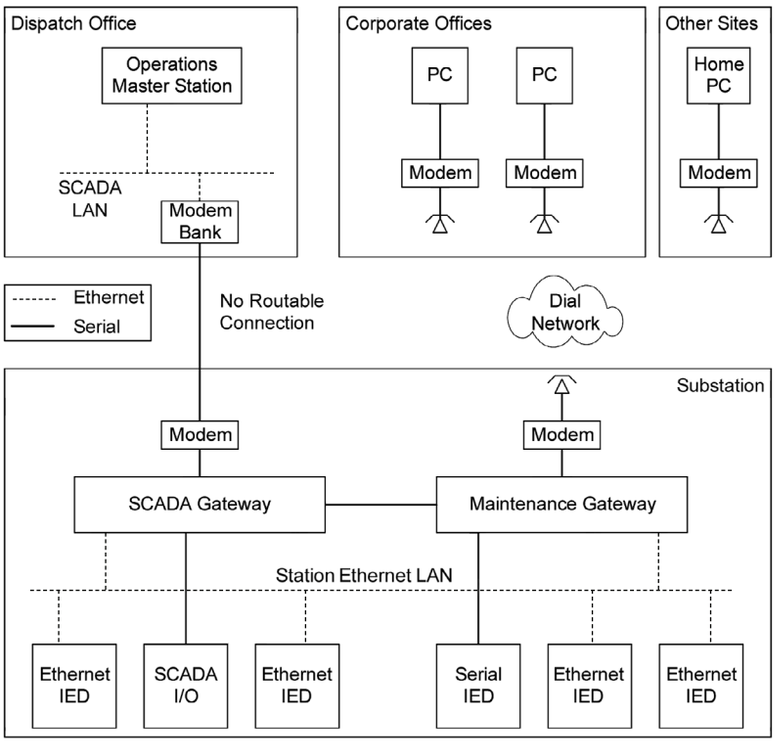

Fig 3.
Secure Dial-Up System.

If the IED software supports Ethernet access, then the serial IEDs are accessed through a serial tunnel established by the Gateway. The User can then access the IED using the IED's native software. The User can connect directly to the IED if that software supports connecting using an Ethernet connection. Otherwise, the User would need to run a virtual serial port software program. That software creates a virtual serial port that the IED software access which redirects the channel to the Gateway and the IED.

The Gateway does control the particular serial and Ethernet IEDs the remote User can access based on their Username and certificate. The serial IEDs are accessed using Secure Terminal Server for the IEDs that the User has authorization to connect. The Gateway also allows an Ethernet connection only to authorized Ethernet IEDs using Secure Connection Relay. These methods restrict remote User access to only the IEDs that the User is authorized to access.

5.2 System Advantages

This system offers security and flexibility. It is the most similar to the dial-up techniques being used today by many Utilities to remotely access the station's non-operational data and IEDs. This architecture provides capabilities of secure access by authorized Users from virtually any dial line.

5.3 System Disadvantages

This system, however, has some significant limitations. Access speeds can be one of the biggest challenges. Also, this technique requires the use of either hard token for each authorized User or a soft token/certificate installed on each User's PC.

Administration of the system is also very demanding. Each Gateway must contain a listing of authorized Users and their IED access rights. This makes the NERC requirement of removing remote access within 24 hours of termination of authorized employees difficult and time consuming.

6. Secure Architecture #2 – Dial-Up Maintenance Server

A similar architecture that allows for centralized password administration of dial circuits is shown in Figure 4. This architecture includes a Secure Dial-Up Maintenance Server installed behind a firewall and connected to a modem bank. This system provides the ability to connect to the Maintenance Gateway and the Station IEDs using a similar technique as the previous Architecture but includes the convenience of LAN connection by the PCs.

Users connect through the Corporate LAN through a firewall to a Maintenance Server. This server provides two-factor authentication with User ID with Password and SSL with PKI including hard token or soft token/certificate. Additionally, each User must have access to the server through the firewall on the network.

The Maintenance Server can be tied to a central Authentication Server which can support Single Sign On (SSO). SSO allows users to only remember one user-ID and password for the Corporate System and for the Maintenance Server/Gateway. It also allows users to authenticate once to gain access to Corporate resources and the Maintenance Server/Gateway. The Authentication Server also can optionally support one time password package (e.g. RSA SecureID).

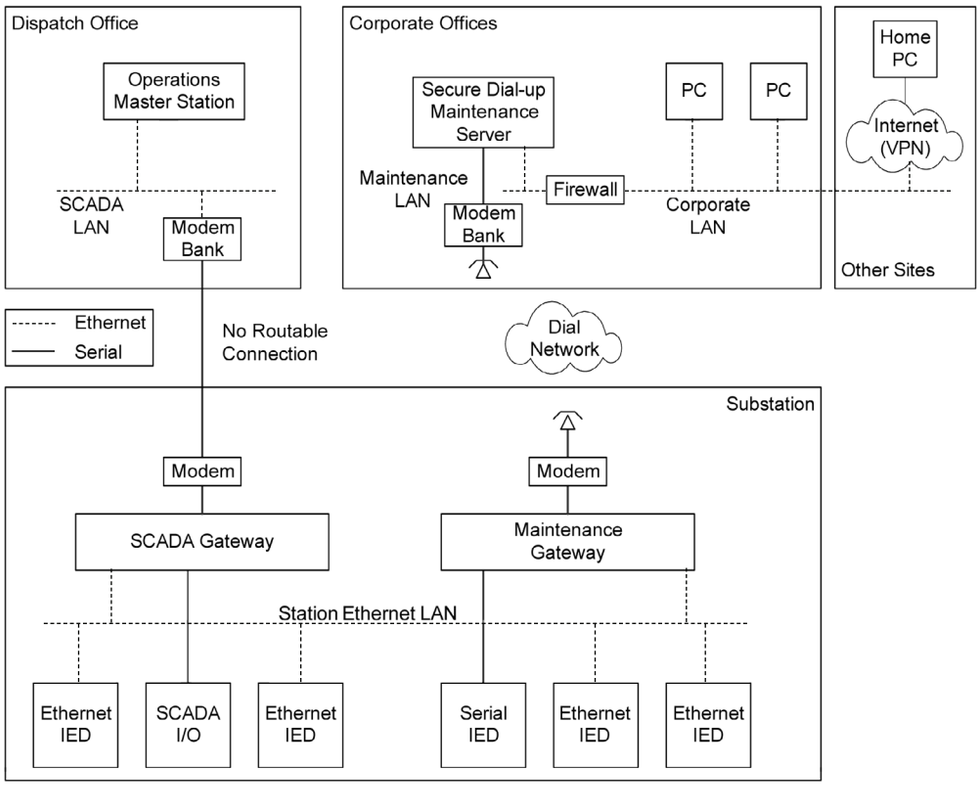

Fig 4.
Serial Maintenance Server.

While the Authentication Server becomes a centralized authority, the Maintenance Server still manages the User's access rights in each Gateway. When a User wants to log-in to a Gateway over the WAN, the User is authenticated by the Maintenance Server then the access rights are set up with the Gateway. The Gateway tracks successful or unsuccessful login attempts. .

Performing authentication on a central server makes it much easier to meet the following CIP requirement: "The Responsible Entity shall revoke such access to Critical Cyber Assets within 24 hours for personnel terminated for cause and within seven calendar days for personnel who no longer require such access to Critical Cyber Assets." [9].

Once a User is authenticated, the server then presents a pick list of substations and IEDs. The User then selects one of the choices and the Maintenance Server then dials one of the modems to the appropriate Maintenance Gateway in the Station using PPP. The Server maintains a randomly generated Maintenance Gateway Password and the appropriate SSL and PKI soft token/ certificate for access to the Gateway. The Maintenance Server sends the authenticated User's ID to the Maintenance Gateway for audit trail and sends that User's specific access rights to the Gateway. This allows specific access control for the Gateway's Web Pages, the serial IEDs and the Ethernet IEDs.

The Maintenance Server contains the necessary scripts to establish Gateway pass-through connection to the appropriate IED. Users connecting to the system from a home PC will use their approved method of connecting, usually VPN, to the Corporate LAN and then access the Maintenance Server over that LAN.

As in the previous architecture, the Gateway must maintain a log of success or unsuccessful login attempts for retrieval by the System Administrator.

This method of accessing the system provides some convenience to the Users, as they don't have to remember the phone number for the stations. They also don't need to remember the script necessary to access a particular IED, as the scripts are stored in the Dial-Up Maintenance Server. The Dial-Up Server also randomly establishes and routinely changes the passwords on each Station Gateway. Security is improved since the Gateway's uses a strong password that is kept private.

6.1 Remote access to IEDs

Once the User has been authenticated by the Maintenance Server and the Server connects to the Gateway, the Station IEDs can be accessed remotely by running the appropriate script on the Server. The Server establishes the access control in the Gateway and enables/disables access as appropriate with these scripts. As with the previous architecture, the serial IEDs are accessed through serial tunneling software on the Server and Gateway and Ethernet IEDs are accessed using Secure Connection Relay. These methods restrict remote User access to only the IEDs that the User is authorized to access.

6.2 System Advantages

This system is also secure and flexible and it provides secure access without the requirement of specific Username and Password and maintenance rights at each Gateway because the Maintenance Server provides centralized administration. Whenever the access rights of a User change, the Administrator only changes the Maintenance Server. Significantly reducing the effort required by the Administrator over a system without

a Maintenance Server. Users also don't need to learn different access address or IED scripts to connect to remote devices.

6.3 System Disadvantages

This system requires users to have LAN access to the Maintenance Server before they can access the Gateways in the Station. This will require User's to change the method of accessing the system. Two-factor authentication is still required at the Maintenance Server because it has become another secure access boundary to the Stations. This system also has the speed limitations inherent of dial-up access.

If dial-up access is still necessary from multiple sites to the Gateway then both methods need to be administrated on the Gateway and Maintenance Server making the system more complicated. Administrators may desire to provide only a few authorized dial-up users to operate only as a backup to the server.

7. Secure Architecture #3 – O&M Shared High Speed Connection

The architecture shown in Figure 5 adds a WAN connection to the substation shared between the Operations and Maintenance areas. In addition, the dial-up access exists as a backup to the WAN based stations or as an example of a mixture of WAN and dial-up stations.

The O&M WAN connection changes method of access for both Operations (SCADA) and Maintenance access. Both are accessing the station using routable protocols and therefore both access methods fall in the NERC security requirement.

7.1 SCADA Access

SCADA access to the station would utilize a routable SCADA protocol such as DNP3, Modbus IP or IEC 61850. Cyber security for the SCADA system includes SSL using Secure Data Concentrator mode. The Secure Data Concentrator mode allows for SSL security to be applied to any routable SCADA protocols.

Obviously, this requires the security capabilities match for both the SCADA Master Station and the Gateway. Additionally both systems must recognize the other's certificate and SSL/TLS encryption.

7.2 Maintenance Access

The maintenance access is similar to the connection in the previous examples, User-ID with a strong password authentication and SSL with PKI. But now WAN based Gateways are accessed over the WAN eliminating the need for serial PPP. Serial PPP would only be used for substation without WAN connection or as a backup. The speed of the connection will be much faster and more reliable than dial-up.

Also, because both SCADA and Maintenance share the same WAN it would be useful if the WAN is designed to support prioritizing SCADA packet over Maintenance packets so that there is no impact on SCADA whenever large files are being copied to the Maintenance Server.

7.3 Remote access to IEDs

This system is similar to the previous option but provides a LAN connection to the Gateway. Utilizing Secure Connection Relay,

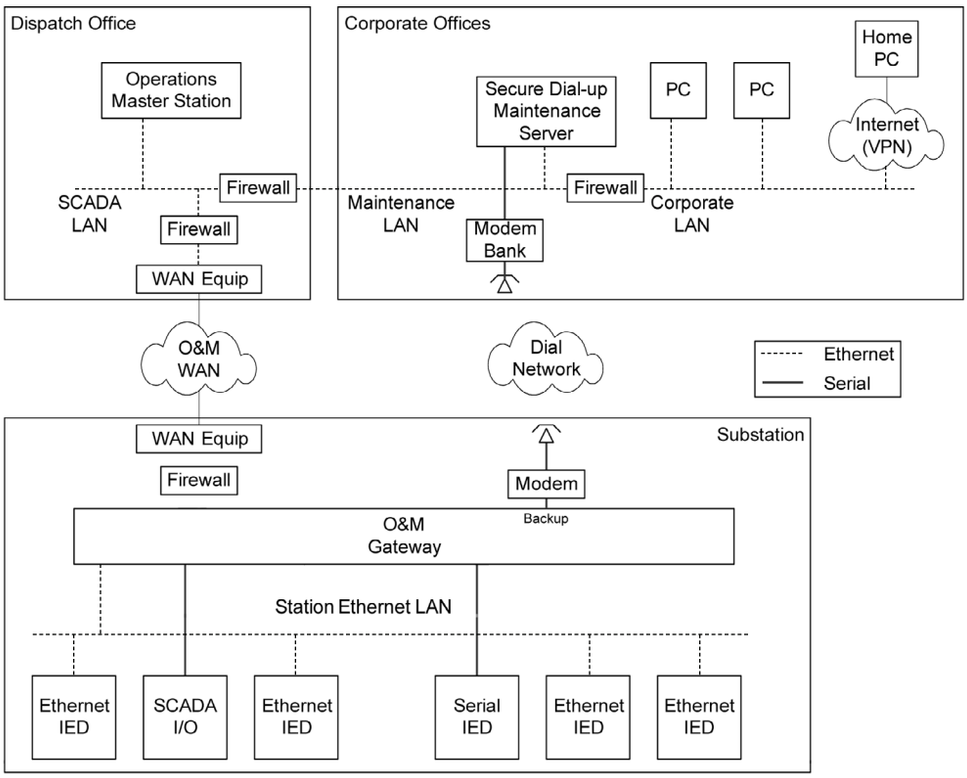

Fig 5.
Shared O&M WAN.

the Server establishes the access control in the Gateway and enables/disables access as appropriate with these scripts. As with the previous architecture, the serial IEDs are accessed through serial tunneling software on the Server and Gateway and Ethernet IEDs. These methods restrict remote User access to only the IEDs that the User is authorized to access.

7.4 System Advantages

This architecture has similar advantages to the previous system and operates at LAN speeds. This provides a significant performance boost for User access.

By sharing the communications channel between the Operations and Non-Operations access, the costs providing two connections is reduced and the two connections can share the bandwidth and performance improvements of the higher speed line. It may be necessary to add the ability to prioritize the Operational traffic over the Non-Operational traffic in the LAN equipment connected to the communications channel.

This system has the advantages of supporting SSO and centralized access right control. Allowing user accounts to be administered in a single location.

7.5 System Disadvantages

Sharing the LAN connection to the Gateway by both Operations and Maintenance can increase the security risks. It is necessary to prevent unauthorized users from gaining access anything on the Dispatch Center. Often this system provides a Maintenance LAN connection that is physically restricted and not connected to the Corporate LAN, increasing security and reducing flexibility for various users.

This system also requires users to have LAN access to the Maintenance Server before they can access the Gateways in the Station. Two-factor authentication is still required at the Maintenance Server.

If dial-up access is still necessary from multiple sites to the Gateway then both methods need to be administrated on the Gateway and Maintenance Server making the system more complicated. Administrators may desire to provide only a few authorized dial-up users to operate only as a backup to the server.

8. Secure Architecture #4 – Separate O&M High Speed Connection

This architecture is more popular than the previous architecture where the SCADA and Maintenance WANs are separated into two networks. This could be a completely separate communication channel or a part of a Virtual LAN or VLAN. A VLAN provides the capability for the WAN/LANs to coexist on the same physical network or network equipment. Otherwise, this system is identical to the functionality of the previous system.

8.1 Remote access to IEDs

This system is similar to the previous options but separates the two LAN connections to the Station. Often this connection is operated over the same physical connection using two Virtual LANs, or V-LANs. Equipment connected to each end of the communications channel separate the two V-LANs into two separate physical LANs at each end. Often, this equipment also allows the ability to dynamically assign channel bandwidth between the two V-LANs as necessary.

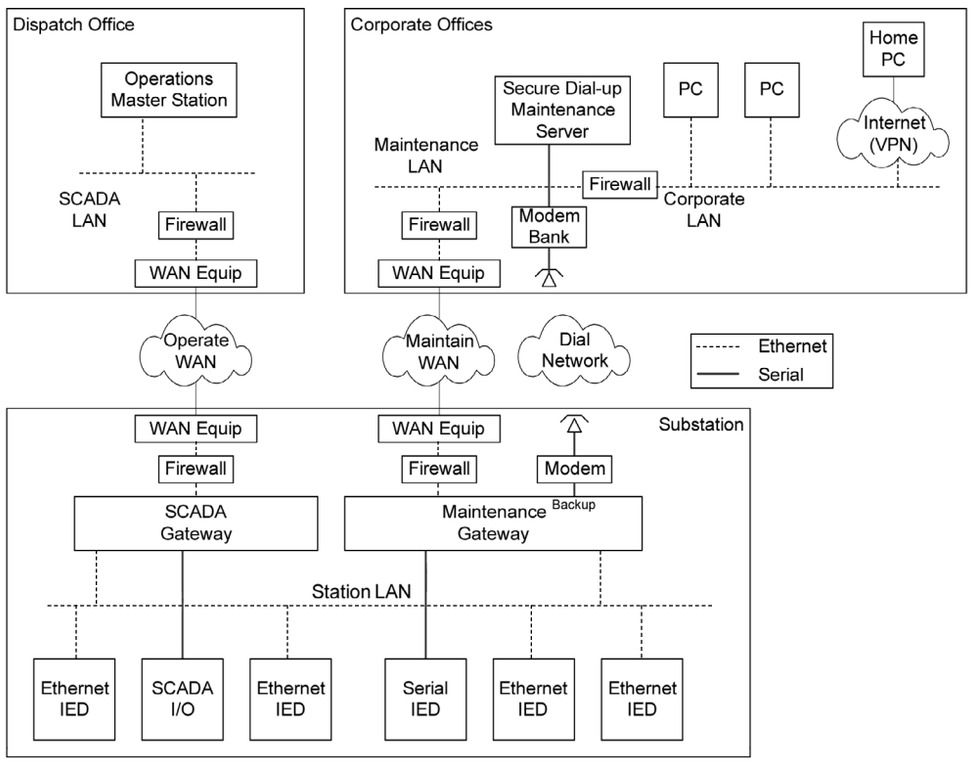

Fig 6.
Separate O&M WAN.

8.2 System Advantages

This architecture has similar advantages to the previous system and operates at LAN speeds with improved security because there is no connection to the Operations LAN from the Maintenance LAN.

By sharing the communications channel using V-LANs between the Operations and Non-Operations access, the costs can be reduced and the bandwidth can be shared while reducing the security risks.

This system has the advantages of supporting SSO and centralized access right control. Allowing user accounts to be administered in a single location.

8.3 System Disadvantages

This system also requires users to have LAN access to the Maintenance Server before they can access the Gateways in the Station. Two-factor authentication is still required at the Maintenance Server.

If dial-up access is still necessary from multiple sites to the Gateway then both methods need to be administrated on the Gateway and Maintenance Server making the system more complicated. Administrators may desire to provide only a few authorized dial-up users to operate only as a backup to the server.

9. Secure Architecture #5 – Separate Station and Corporate LANs

This architecture breaks the routable connections between the Maintenance LAN and the Corporate LAN or the Station LAN. This architecture is functionally identical to the system previously described however it provides an improved level of security and isolation of the various functions.

IEDs that need to share data with both the SCADA and the Maintenance Gateway must do so over a non-routable connection. Those IEDs must communicate over two communication channels or the two Gateways to share IED data serially between the Operations and the Maintenance Gateways. This breaks the routing connection between the two LANs in the substation completely.

The Corporate LAN is also disconnected from the Maintenance LAN. A new Maintenance Database Server is added to the system with two NIC cards. The Maintenance Server is designed not to create a routable connection between the two LANs. The Maintenance Gateway in the station will automatically send data and oscillography files to the Maintenance Database Server. Users on the Corporate LAN can access the substation data on the Maintenance Database Server without having a direct connection to the station. The Maintenance Server must be secured to prevent a Corporate LAN User from gaining access through to the Maintenance LAN.

Devices connected to the Dispatch Office side of the Maintenance LAN can access the Maintenance Gateway and with SSL and PKI can access the serial and Ethernet IEDs directly. Of the security architectures discussed here, this architecture is the most secure but can be the most complicated.

9.1 Remote access to IEDs

This system is similar to the previous options but separates the Maintenance LAN from the Corporate LAN. It also separates

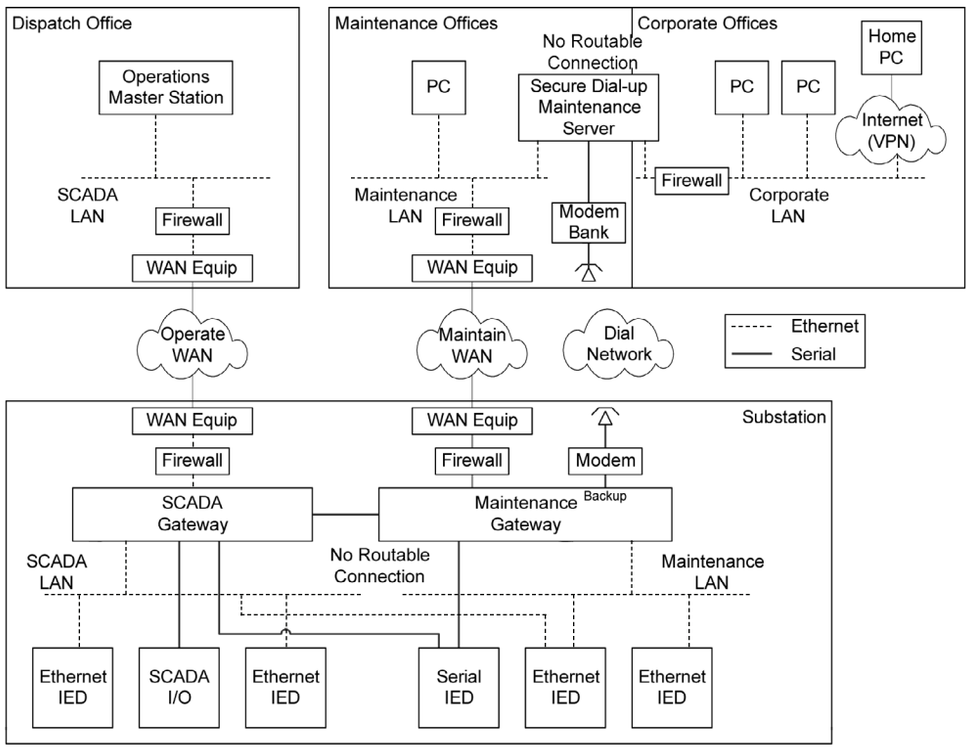

Fig 7.
Separate O&M Station LAN.

the Station Operations and Maintenance LANs. Access to the IEDs is only provided by users connected directly to the Maintenance LAN. Users on the Corporate LAN can access a new Maintenance Database Server which provides data from the Station IEDs and the Gateway without providing remote access from users outside the Maintenance LAN.

9.2 System Advantages

This system provides the greatest level of security between the Corporate LAN and the Maintenance LAN because there is no routable connection between the two LANs. User's can access data from the Stations on the Maintenance Server and can access the IEDs directly from the Maintenance LAN which is often only available in a physically secure location. Two-factor authentication is no longer required by the Corporate LAN Users because they cannot gain access to the Gateways directly from the Corporate LAN.

This system has the advantages of supporting SSO and centralized access right control. Allowing user accounts to be administered in a single location.

9.3 System Disadvantages

This system is more complicated and restricts remote access only to users who have LAN access to the Maintenance LAN before they can access the Gateways in the Station. Two-factor authentication is still required at the Maintenance Server for these users. This system also is more expensive and requires dual serial communications to the IEDs and/or a serial data connection between the SCADA and Maintenance Gateways.

If dial-up access is still necessary from multiple sites to the Gateway then both methods need to be administrated on the Gateway and Maintenance Server making the system more complicated. Administrators may desire to provide only a few authorized dial-up users to operate only as a backup to the server.

10. Summary

As utilities seek to balance the critical nature of the asset and the cyber threat with the access requirements of authorized Users, the search for solutions will continue to be an ongoing challenge for both Utilities and Security Solution Suppliers. Most Utilities are implementing a mix of the architectures outlined in this paper depending on the critical nature of the asset and the communications available to the site.

Answers to the following questions will help determine the architecture that fits best:

- what Users need access to the data from the IEDs and who needs direct access to the IEDs?
- what type of communications exists or is economically available?
- what type of substation architectures are implemented or planned? Do they include Ethernet?
- will the Maintenance LAN and Operations LAN be connected? At the Substation, share a communications line, or at the dispatch office?
- how will the Corporate LAN be connected to the system if at all?
- will authorized Users be able to access the data or the IEDs from remote locations?

11. References

[1] http://www.nerc.com/~filez/standards/Cyber-Security-Permanent.html

[2] ftp://www.nerc.com/pub/sys/all_updl/standards/sar/Glossary_Clean_1-07-05.pdf "Glossary of Terms Used in Reliability Standards", Page 2, Adopted by NERC Board of Trustees: February 8, 2005, Effective Date: April 1, 2005

[3] ftp://www.nerc.com/pub/sys/all_updl/standards/sar/Cyber_Security_Standards_Board_Approval_02May06.pdf Standard CIP–002–1 — Cyber Security — Critical Cyber Asset Identification Page 2

[4] ftp://www.nerc.com/pub/sys/all_updl/standards/sar/Cyber_Security_Standards_Board_Approval_02May06.pdf Standard CIP–002–1 — Cyber Security — Critical Cyber Asset Identification Page 2

[5] ftp://www.nerc.com/pub/sys/all_updl/standards/sar/Cyber_Security_Standards_Board_Approval_02May06.pdf Standard CIP–002–1 — Cyber Security — Critical Cyber Asset Identification, Part B – R3, Page 4

[6] http://computing-dictionary.thefreedictionary.com/ Definitions used from this web site

http://encyclopedia.thefreedictionary.com/Two+Factor+Authentication

http://encyclopedia.thefreedictionary.com/SSL

http://encyclopedia.thefreedictionary.com/HTTPS

http://encyclopedia.thefreedictionary.com/Transport+Layer+Security

http://encyclopedia.thefreedictionary.com/CHAP

http://encyclopedia.thefreedictionary.com/PPP

http://encyclopedia.thefreedictionary.com/PKI

http://encyclopedia.thefreedictionary.com/Certificate+authority

[7] Network Security Basics, Product Information, PRPI-039-001-1, GE Energy 01/08/2002

[8] ftp://www.nerc.com/pub/sys/all_updl/standards/sar/Cyber_Security_Standards_Board_Approval_02May06.pdf Standard CIP-005-1Cyber Security – Electronic Security R3.2, Page 5

[9] ftp://www.nerc.com/pub/sys/all_updl/standards/sar/Cyber_Security_Standards_Board_Approval_02May06.pdf Standard CIP-004-1Cyber Security – Electronic Security R4.2, Page 4