

Securing Distribution Automation

Jacques Benoit
Senior Analyst Information Security
Cooper Power Systems

Serge Gagnon
IT Project Leader
Hydro-Québec

Luc Tétreault
Automation Engineer
Hydro-Québec

Abstract

The security requirements of distribution automation are quite different than those at the transmission and generation levels of the power network. To automate the distribution network, a utility has to deploy a large number of geographically dispersed simple devices that use a variety of communication technologies including wireless and dialup. Typical field devices have limited computational capacity, and communications are often established on demand, using low bandwidth connections. Maintenance is provided by a large number of field technicians for which access and permissions must be managed.

In this paper, we will discuss how a major utility is handling the security requirements of its distribution automation system. We will discuss some of the strategies and solutions that are being considered in order to ensure the secure operation of the distribution automation system. The use of DNP3 Secure Authentication will be presented as a means to ensure the security of control operations, while supporting the continued use of legacy devices. We will also discuss solutions to manage device passwords, and the use of Public Key Infrastructure (PKI) and X.509 certificates as a means of authenticating users and assigning permissions.

Background

In 2001, Hydro-Québec started work on a strategy to automate its distribution network. The short term goal was to improve the reliability of the distribution network by reducing the duration of outages. The long term goal was to build an “interactive network”.

After a pilot project demonstrated the benefits of the proposed strategy, Hydro-Québec started to deploy in 2006 a large-scale distribution automation system that will ultimately provide the capability of remotely managing 3750 switches and breakers on 1100 feeders. The key components of the system are cabinets that contain a motorized switch, a small RTU and a communications gateway. Some cabinets also contain a protective relay. The

gateway device is used to manage communications, but also to add local processing capability to the solution. Hydro- Québec has generalized this practice in many of its projects to protect against obsolescence by providing the capability to add new functionalities as requirements evolve. In this project, the gateway device is also used to establish an electronic perimeter protecting the other IEDs in the cabinet.

As part of the interactive network vision, each cabinet produces a large number of data points including more than 100 binaries and 20 analogs used to monitor the power line and the cabinet status.

With such large number of devices and data points to support, Hydro- Québec chose to implement regional control centers. Each control center implements a Front End Processor (FEP) that manages communication with the cabinets and provides data to the Distribution Management System (DMS).

The FEP supports a variety of communication links including, but not limited to, dialup and direct serial connections. On a scheduled basis, the FEP connects to each cabinet and polls for data. The cabinet can also call in to report an event or change of status. The control center can also initiate communication with the cabinet on demand to control the switch or retrieve data. Engineering users can also initiate a connection to perform remote device maintenance.

Cyber Security Requirements

The goal of distribution automation is to improve network reliability. Obviously, introducing automation also introduces risk. Providing the capability to remotely operate switches and breakers introduces the risk of unplanned operations resulting from errors, or even malevolent parties.

To protect from unintended or malicious operations, the system must provide the following:

- Ensure that control operations originate from an authorized control center
- Ensure that remote maintenance access is only granted to authorized users
- Ensure that local maintenance access is only granted to authorized users
- Ensure that only authorized devices can connect to the communications network

From the initial design, Hydro-Québec specified that the cabinet has to provide both a physical and electronic perimeter. Any breach to the cabinet must be detected and immediately reported to the control center.

The electronic perimeter must provide:

- Authentication through individual user accounts
- The ability to assign functions and features based on the user account
- An audit trail that lists events in the order they occurred

- The ability to monitor security events and make the information available to control centers
- A mechanism through which a control center can grant or refuse access to a function or feature

Security requirements and applicable standards

Until recently, cyber security in the power industry has been left to the initiative of utilities and vendors. NERC CIP initiated a fundamental change by requiring that utilities implement a security plan to protect their critical assets. The Department of Energy has gone even further by announcing that Smart Grid projects funded under the Recovery Act must “*provide reasonable assurance that their cyber security will provide protection against broad based systemic failures in the electric grid in the event of a cyber security breach.*”

Under the Energy Independence and Security Act of 2007 (EISA), the National Institute of Standards and Technology (NIST) has been assigned the “*primary responsibility to coordinate development of a framework that includes protocols and model standards for information management to achieve interoperability of Smart Grid devices and systems...*”

The *NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 1.0* document, is the output of the first phase of the NIST three phase plan. This document identifies 75 existing standards that are applicable to the ongoing development of the Smart Grid.

For instance, the IEEE 1686-2007 standard establishes a baseline of security requirements and features that must be provided in IEDs to accommodate critical infrastructure programs. Some specific requirements are:

- Unique user ID and password combinations, generated by the user.
- The ability to assign IED functions and features according to the individual user-created ID/password combinations.
- The ability to record an audit trail listing events in the order in which they occur.
- The ability to monitor security-related activity and make the information available to a supervisory system through a real-time communication protocol.
- The ability for SCADA to grant permission prior to performing actions, locally or remotely.
- The ability to authenticate that the configuration software is a copy that has been authorized by the user.

The typical IED is very far from complying with IEEE 1686. However, Hydro-Québec’s experience is that these requirements can be met by using an appropriate data concentrator or communications processor to act as an electronic perimeter to the connected IEDs and RTUs.

The security of data exchanges and communications for control systems in the power industry is addressed by the IEC 62351 family of standards. The following two parts of the standard were identified as being directly applicable to the Hydro-Québec project:

- IEC 62351-3 specifies how to secure TCP/IP-based protocols through the use of Transport Layer Security (TLS).
- IEC 62351-5 specifies how to add user and device authentication, and data integrity protection to protocols derived from IEC 61870-5, such as DNP3.

A key requirement in any large scale project is upgradability through firmware updates. Two standards address this issue. IEEE 1686-2007 specifies that firmware should be managed according to C37.231 *IEEE Recommended Practice for Microprocessor-Based Protection Equipment Firmware Control*. The new *NEMA SG-AMI 1 Requirements for Smart Meter Upgradeability* standard results from a NIST Priority Action Plan to fill the gaps in existing standards. The standard recognizes that utilities are currently deploying large number of devices in AMI and DR projects that will most probably not comply with future requirements. These devices will need to be upgraded. The standard thus defines the upgradability requirements for smart meters used in AMI applications. Both of these standards define requirements that should be considered for all field devices, not just smart meters and protective relays.

Securing the communications link

Most of the cabinets used in the Hydro-Québec distribution automation project are connected using on-demand dialup connections. This solution was deemed the most cost-effective in urban areas since the cabinets are installed on utility poles that already carry telephone lines.

Traditionally, dialup connections have been secured through the use of Caller ID to filter incoming calls and callback to further ensure that only authorized devices are connected. However, the introduction of IP Telephony has resulted in a merging of technologies and telephony is now becoming vulnerable to traditional network attack techniques such as address spoofing. The telephone link can no longer be considered as secure and additional security measures need to be applied.

Once the dialup connection is established, the software generally sets up a TCP/IP link using the industry-standard PPP protocol with CHAP authentication. The authentication prevents an unauthorized party from gaining access to the network. The authentication requires that a secret or password be shared between both parties. The password is not transmitted on the link, but is used to generate challenge and response messages. When used with a complex password, this approach ensures the authenticity of the party initiating the call. As with any system based on the use of shared passwords, there should be a strategy to change the passwords on a regular basis. This is especially important for systems which are deployed for a very long time as it is the case in the power industry.

The issue of field device password management has been identified by the NIST CyberSecurity Coordination Task Group as one of the issues that needs to be addressed for Smart Grid security. While there exist many enterprise-level products for password management, to our knowledge there are none that have been designed to meet the requirements of distributed field devices. Typical enterprise password management systems are designed to support devices such as routers and switches on standard enterprise networks. They generally are not designed to manage devices connected through low speed dialup connections that may suffer from communication drop off or timeouts. The use of a custom solution or the use of an additional layer of protection may be required to mitigate this risk.

For instance, the data being exchanged on the link can also be protected. A common approach is to set up a VPN to ensure the authenticity of both networks endpoints and the confidentiality of the data. However, with a VPN the network itself remains exposed. If a system is compromised, the malicious code can propagate through the VPN.

The IEC 62351-3 standard provides a different strategy and recommends protecting the information flow through the use of Transport Layer Security (TLS, previously known as SSL) to authenticate both parties and encrypt the data. Since the TLS protocol is implemented at the application level it provides very good security between the control center and the field device. However, TLS must be supported at both ends and requires the use of a certificate to establish authenticity. In the same manner as a password, this certificate may need to be replaced during the lifetime of the device. Also, since TLS encrypts the exchanged data, it requires additional processing power that may not be available in less expensive field devices.

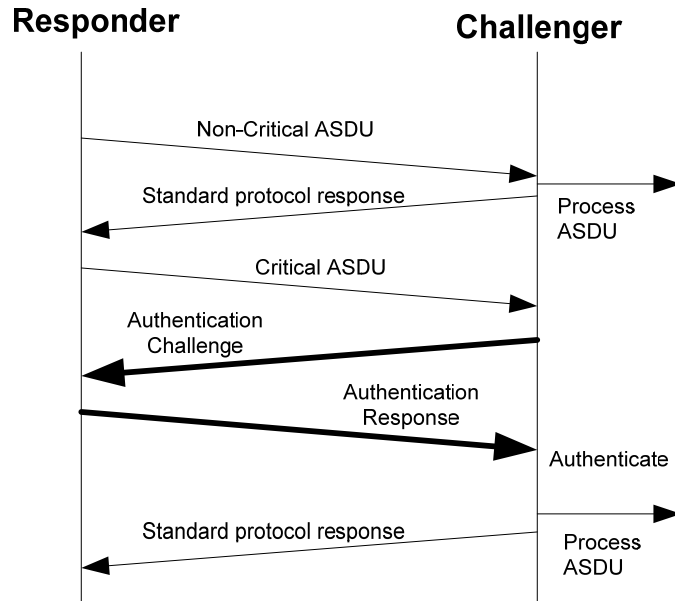
Securing control operations

The power industry has generalized the use of the DNP3 protocol for control center to field device communications. However, DNP3 was not designed with security in mind. The field device always assumes that a control request was issued by a legitimate control center. This deficiency makes the protocol vulnerable to spoofing, modification and replay attacks.

To address the security of protocols used in the power industry, the IEC TC57 Working Group 15 developed the IEC 62351-5 standard. This standard recommends a strategy to add authentication to the TC57 protocols and their derivatives, such as DNP3. Based on these recommendations, the DNP3 Users Group has proposed and adopted an extension to DNP3 called “Secure Authentication”.

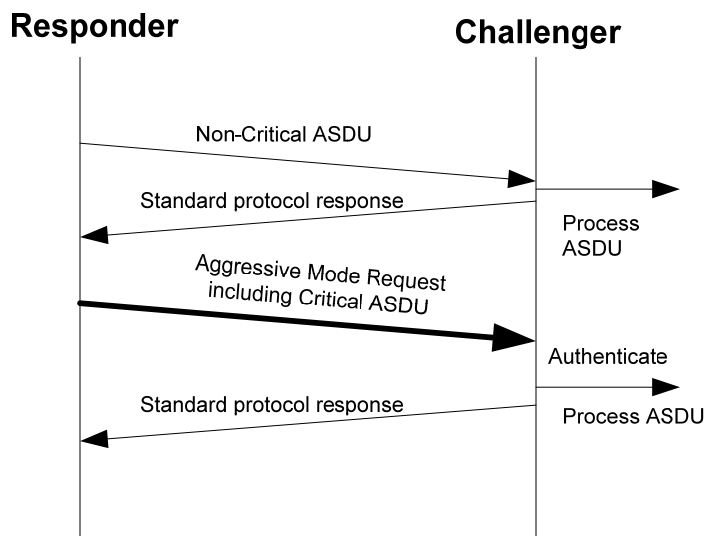
This addition to the DNP3 protocol provides authentication and protection against spoofing, modification and replay attacks. The basic concept is that both the receiver and sender can challenge the other party whenever they receive a critical protocol message (referred to as an Application Service Data Unit or ASDU). The challenge message contains pseudo-random data and a sequence number. The response contains a

cryptographic hash (HMAC) value calculated from the challenge, the sequence number and a shared secret key. Since both the sender and receiver share the secret key, they will both calculate the same hash value from the same inputs, thus authenticating the other party and the integrity of the message.



Challenge of a Critical ASDU ^[1]

The standard also defines an “aggressive mode” for situations where the challenge/response mechanism would introduce too much latency. In aggressive mode, the authentication information is added at the end of the critical ASDU.



Aggressive Mode Request ^[1]

DNP3 Secure Authentication provides a good solution for improving the security of applications such as distribution automation. By limiting the use of cryptography to the calculation of a hash function, it reduces bandwidth usage and computational requirements. In situations where confidentiality is required, TLS should be used as prescribed by IEC 62351-3.

Since security functions have been added as new message types to the existing protocol, it can interoperate with legacy devices if required. The designers of the protocol have also taken into account how it can be used with a communications gateway to provide secure communications to both compliant and legacy devices.

By adding the challenge/response mechanism as part of the protocol, the solution becomes independent of the communication medium and can be used to add security to TCP/IP or serial devices.

The current implementation of the protocol does not specify how to distribute the shared encryption key. As we mentioned previously, the NIST CyberSecurity Coordination Task Group has identified that the management of device passwords and encryption keys will need to be addressed to ensure the security of the Smart Grid.

Another issue raised by NIST when establishing the interoperability roadmap for the Smart Grid is that the DNP3 Users Group is not an official Standard Organization. This situation is changing with the announcement that IEEE will adopt DNP3 as a new standard designated IEEE P1815.

Authenticating users and systems

The vast majority of IEDs implement a security model based on permission levels protected by different passwords. To simplify commissioning and field maintenance, utilities often use the same password for all field devices. The problem with this approach is that it provides no accountability and permissions cannot be granted and revoked on an individual basis, thus making it impossible to meet the requirements of existing security standards. For instance, IEEE 1686-2007 states that there must be individual user accounts and passwords. NERC CIP-004-2 R4.2 states that access to critical assets must be revoked within 24 hours for personnel terminated for cause.

Many communications gateways and data concentrator vendors provide the capability to tie in to an existing enterprise security infrastructure such as Active Directory through the use of a RADIUS server to authenticate users. Enterprise-level authentication is a good solution for remote maintenance access. An enterprise-level remote access server authenticates the user before establishing a communications link to the field device for maintenance. However, in order to perform local maintenance, the field technician will need to be authenticated by the enterprise, which requires an active communications link.

The availability of an enterprise uplink can generally not be ensured at all times and a local authentication solution is still required.

To fulfill this requirement, some vendors provide an innovative mechanism where a remote access server grants the user a limited duration “security ticket” that can be used to access a field device. However, to manage revocation within 24 hours, the security ticket lifetime will need to be limited to 24 hours and the field technician will need to connect to the enterprise server every day to get a new security ticket.

A non-proprietary standards-based mechanism that can be used to manage authentication and assign permissions does exist. With the X.509 standard, the International Telecommunication Union (ITU) has defined standard formats to establish a Public Key Infrastructure (PKI) based on Certificate Authorities (CA), public key certificates, attribute certificates and certificate revocation lists.

The key concept behind a PKI is the use of asymmetric cryptography. In traditional symmetric cryptography, both parties share a secret key that they use to encrypt and decrypt messages. In asymmetric cryptography, keys come in pairs. A message encrypted with one key can only be decrypted using the other key. One key is known as the public key and can be widely shared. The other key, known as the private key, is kept in a secure location. Since public keys can be shared, the sender of a message can use the intended receiver’s public key to encrypt the message. Only the intended receiver with the appropriate private key will then be able to decrypt the message.

Asymmetric cryptography can also be used to authenticate the sender and to protect the contents of the message. Before sending the message, the sender calculates a hash, encrypts it with her own private key and adds it to the message. This portion of the message is called a digital signature. The receiver of the message calculates the message hash, extracts the signature and uses the sender’s public key to decrypt it. If the hash matches, the receiver can be certain of the sender identity and the integrity of the message contents.

In order to set up an authentication and authorization, an additional mechanism is required. In the above discussion, we assumed that both parties have access to their respective public keys and that they are confident that the key was in fact provided by the correct party. To ensure the authenticity of public keys, the standard defines a Certificate Authority (CA) that validates parties and issues public keys. To begin, a user generates a pair of keys and sends the public key to the CA. The CA confirms the identity of the user, creates an electronic document containing the user’s name and public key, and signs this document using its own private key. The signed document is called a public key certificate.

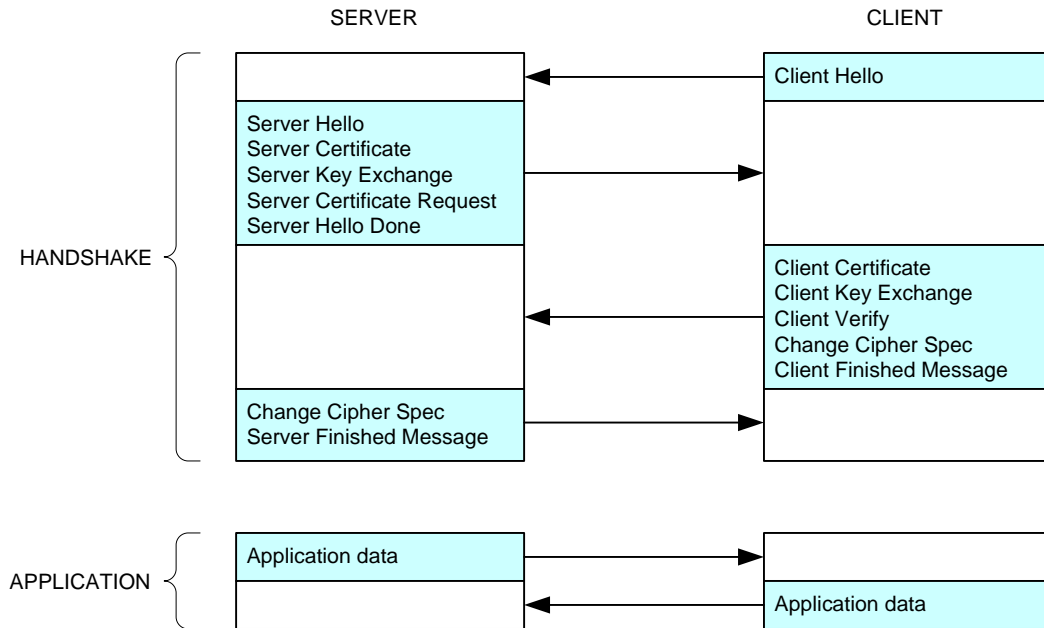
To set up a PKI, the CA’s public key certificate is distributed to all parties. This certificate is called a root certificate and is self-signed. Any party that trusts the CA can then use the CA’s public key to validate the authenticity of a public key certificate provided by an unknown user. If the signature on the certificate is valid and we trust the

CA, we can also trust the identity of the user bearing the certificate. Public key certificates are widely used to authenticate web sites and to set up encryption with the TLS protocol.

Many large organizations have already set up a PKI to authenticate users, sign documents, email and applications, encrypt data exchanges and file storage. The addition of X.509 certificates support to devices and communications gateways provides a secure mechanism to authenticate users and systems. Web browsers typically install more than a hundred root certificates for widely known commercial CAs such as VeriSign. In an automation application, IEDs and communications gateways would probably be limited to the utility's CA root certificate for authenticating users and the device vendor's CA for authenticating software releases.

While X.509 certificates are good for authenticating users, there still remains to define an authorization mechanism to specify what the user can do. The X.509 standard provides this capability in the form of "attribute certificates". Attribute certificates are similar to public key certificates but instead of being used to identify an individual or system, are used to store user-defined data fields, or attributes. An attribute certificate can thus be used to carry a user's specific access permissions or group memberships. It must be noted that while the standards define this capability, its use is not widespread, device permissions are generally vendor specific, and there will thus remain interoperability challenges.

Whenever a user requires access to a field device, both the user and the device can be authenticated through their certificates. This capability is a standard function of the TLS protocol that can be used by the maintenance tool. Once the user is authenticated, the maintenance tool then provides the user's attribute certificate which describes the user's permissions.



Using Certificates for Mutual Authentication with Transport Layer Security

The interest of the certificate mechanism is that it can be used even when no connection to a central authority is available. However, a means must be provided to invalidate a certificate and revoke access when it is no longer required. This can be achieved through the X.509 certificate expiry date. Typically, certificates used to identify systems will have a very long lifetime, those used to identify users will have a shorter lifetime, and those used to assign permissions will have an even shorter lifetime.

When access need to be removed before the expiry date, the CA can revoke the certificate. There are two standard methods to propagate certificate revocation information. The Online Certificate Status Protocol (OCSP) defines a means for the device to verify the validity of a certificate in real-time. However, as the name implies, this requires a live connection to an OCSP Responder. Another strategy is the use of a Certificate Revocation List (CRL) that contains the list of all certificates that have been revoked before their expiration. The infrastructure must then provide a means to distribute the CRL to all devices. This operation can be integrated as part of the regular data exchanges performed by the distribution automation system.

Conclusion

The deployment of a distribution automation system is a complex undertaking. As with all large scale projects, a simple error or omission can have a huge cost impact if it becomes necessary to modify or replace all installed systems. As the NIST Framework and Roadmap for Smart Grid Interoperability Standards states, *“In the absence of standards, there is a risk that the diverse Smart Grid technologies that are the objects of*

these mounting investments will become prematurely obsolete or, worse, be implemented without adequate security measures.”

In order to achieve its original “interactive network” vision, Hydro-Québec specified from the beginning that the automation components provide sufficient processing power, be remotely upgradable and comply with existing standards, including security. By “future-proofing” its solution, it has been able to evolve the functional and security requirements as new technologies and best practices are deployed. The IEC 62351 standards and DNP3 Secure Authentication are good examples of relatively lightweight solutions that are now coming into usage and that can significantly enhance the operational security of the distribution automation system.

References

1. DNP3 Users Group, DNP3 Specification, Supplement to Volume 2, Secure Authentication, Version 2.00, 31 July, 2008
2. DRAFT NISTIR 7628, Smart Grid Cyber Security Strategy and Requirements, February 2010
3. Grant Gilchrist, “DNP3 Revolution: Past, Present and Future, Security for DNP3”, presented at DistribuTECH 2006, downloaded from www.enernex.com/Reports/DNPSecurity-Gilchrist.pdf
4. Hervé Delmas, Patrick Cossette and Robert O’ Reilly, “A Case Study: How a Utility Automated and Integrated Data/Control for 4000 Pole-Top Switches and Protection Relays, and Reduced its SAIDI”, presented at Western Power Delivery and Automation Conference 2007
5. IEC 62351 1-8, Power System Control and Associated Communications - Data and Communication Security
6. IEEE 1686-2007, IEEE Standard for Substation Intelligent Electronic Devices (IEDs) Cyber Security Capabilities
7. IEEE C37.231 IEEE Recommended Practice for Microprocessor-Based Protection Equipment Firmware Control
8. NEMA SG-AMI 1 Requirements for Smart Meter Upgradeability
9. NIST Special Publication 1108, NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 1.0
10. RFC 2549 Internet X.509 Public key Infrastructure Certificate and CRL Profile, <http://www.ietf.org/rfc/rfc2459.txt>

11. RFC 3281 An Internet Attribute Certificate Profile for Authorization,
<http://www.ietf.org/rfc/rfc3281.txt>
12. SSL/TLS in Detail, Microsoft® Windows Server™ 2003 Operations guide,
downloaded from [http://technet.microsoft.com/en-us/library/cc785811\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/cc785811(WS.10).aspx)