

Securing Distribution Automation

Jacques Benoit, Cooper Power Systems

Serge Gagnon, Hydro-Québec

Luc Tétreault, Hydro-Québec

Western Power Delivery Automation Conference

Spokane, Washington

April 2010

Agenda

- > Hydro-Québec Distribution Automation project overview
- > Cyber security requirements
- > Security requirements and applicable standards
- > Securing the communications link
- > Securing control operations
- > Authenticating users and systems
- > Conclusion

Hydro-Québec Distribution Automation Project

- > Project started in 2001 with the following goals
 - Improve reliability and reduce outage duration
 - Move towards a modern “interactive network”
- > Deployment started in 2006
- > Project scope
 - 3750 switches
 - 1100 feeders

Key Components

- > Pole-top cabinets that contain:
 - Motorized switch
 - RTU
 - Communications gateway / Data concentrator
 - Protective relay (in some cabinets)
- > The communications gateway
 - Concentrates data from multiple devices
 - Provides local processing capability
 - Implements electronic perimeter
 - Helps protect against obsolescence

Distributed Architecture

- > Very high volume of data
 - Large number of data points per cabinet
 - > 100 binaries
 - > 20 analogs
 - Large number of cabinets
- > Load distributed through Regional Control Centers
 - Front End Processor (FEP)
 - Distribution Management System (DMS)

Front End Processors

- > Manage all communications
- > Feed data to DMS
- > Support various communication links
 - Direct TCP/IP
 - Dialup
 - Other
- > Perform scheduled data poll of cabinets
- > Cabinets can call in to report events and changes of status
- > On-demand communication to retrieve data, control switches, and perform remote maintenance

High Level Cyber Security Requirements

- > To protect from unintended or malicious operations, the system must ensure that:
 - Only authorized devices can connect to the communications network
 - Control operations originate from an authorized control center
 - Remote maintenance access is only granted to authorized users
 - Local maintenance access is only granted to authorized users

Security requirements and applicable standards

- > Until very recently, security was not a regulatory requirement
- > NERC CIP introduced a security framework that mostly applies to generation and transmission
- > NERC CIP definition of critical asset is evolving towards a risk and impact-based assessment
- > Projects funded under the Recovery Act require cyber security
- > *NIST Framework and Roadmap for Smart Grid Interoperability Standards* has identified 75 existing standards, including security, that are applicable to Smart Grid projects

Electronic Perimeter

IEEE 1686-2007

- > IEEE Standard for Substation Intelligent Electronic Devices (IEDs) Cyber Security Capabilities
 - Unique user ID and password combinations.
 - Ability to assign IED functions and features according to the individual user accounts.
 - Ability to record an audit trail listing events in the order in which they occur.
 - Ability to monitor security-related activity and make the information available to a supervisory system through a real-time communications protocol.
 - Ability for SCADA to grant permission prior to performing actions, locally or remotely.
 - Ability to authenticate that the configuration software is a copy that has been authorized by the user.

Communications Security

IEC 62351

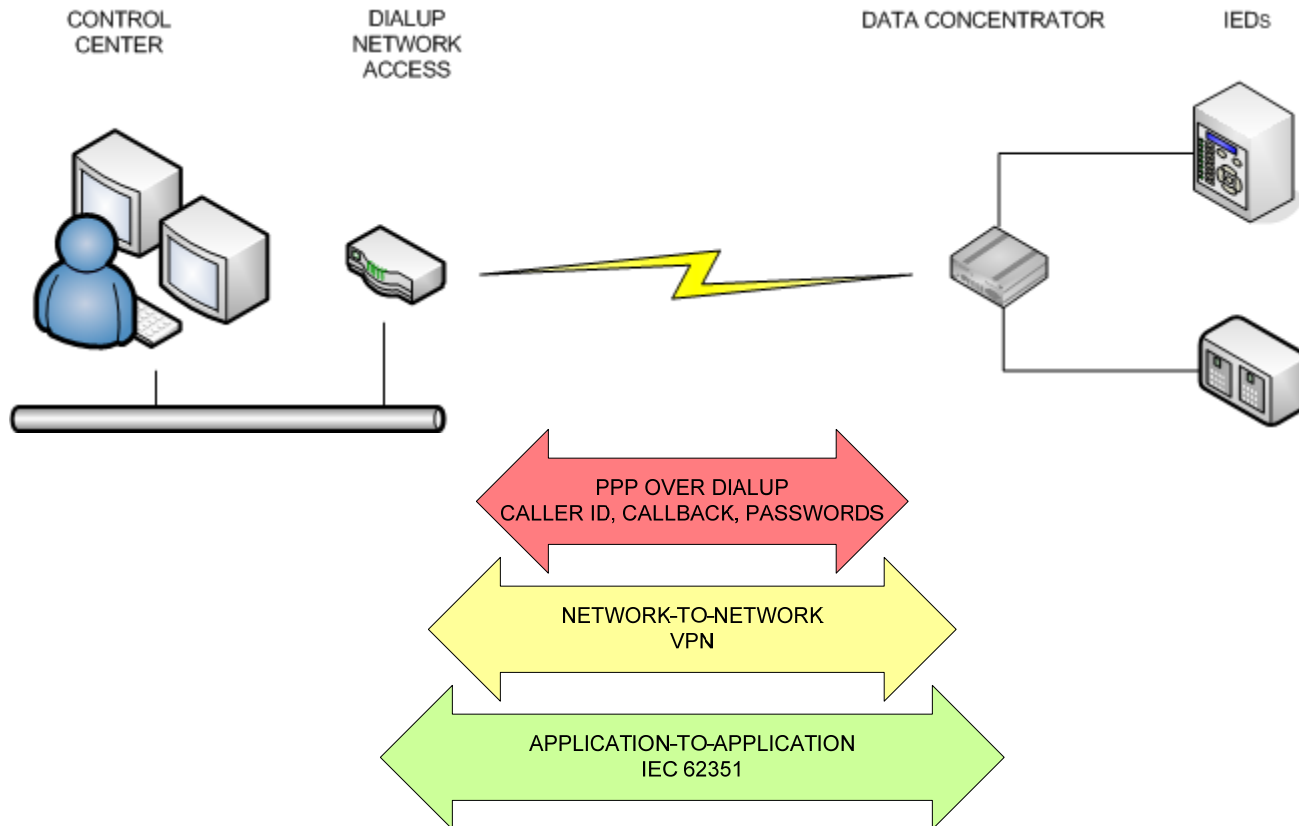
- > Standard developed for handling the security of TC-57 protocols including IEC 61850, IEC 60870-5 and its derivatives, such as DNP3
 - IEC 62351-3 specifies how to secure TCP/IP-based protocols through the use of Transport Layer Security (TLS).
 - IEC 62351-5 specifies how to add user and device authentication, and data integrity.

Firmware Updates

IEEE C37.231, NEMA SG-AMI 1

- > IEEE 1686-2007 specifies that firmware should be managed according to *C37.231 IEEE Recommended Practice for Microprocessor-Based Protection Equipment Firmware Control*.
- > NEMA SG-AMI 1 developed as Priority Action Plan, part of the *NIST Framework and Roadmap for Smart Grid Interoperability Standards*, addresses firmware updates for smart meters.
- > Many of these requirements apply to any type of device:
 - Recover to previous version if unable to complete upgrade.
 - Have no impact on device operational settings.
 - Validate that a firmware image passes integrity check.
 - Validate that the firmware image comes from a trusted source.

Securing the Communications Link



Dial-Up Security

- > Access can be protected by Caller ID, callback, and shared passwords.
- > Caller ID spoofing is much easier with IP telephony.
- > Enterprise password management solutions are available, but not designed to handle unreliable communications with field devices.
- > NIST CyberSecurity Coordination Task Group has identified device password management as one of the issues that needs to be addressed for Smart Grid security.

Network-to-Network Security

- > Typically implemented through a VPN
 - Authenticates both network endpoints.
 - Encrypts traffic exchanged between endpoints.
 - Acts as a “tunnel” to carry information between two networks
- > Does not address:
 - Authenticity of party issuing control requests.
 - Rogue application or malware at master station.
 - Rogue application or malware at outstation.

Securing TCP/IP-Based Protocols

IEC 62351-3

Securing TCP/IP-based protocols through the use of Transport Layer Security (TLS), was previously known as SSL:

- > Shall support at least AES-128 encryption.
- > Shall support multiple Certificate Authorities (CA).
- > Shall renegotiate symmetric keys based upon a time period and a maximum allowed number of packets/bytes sent.
- > Shall use bidirectional certificate exchange and validation.

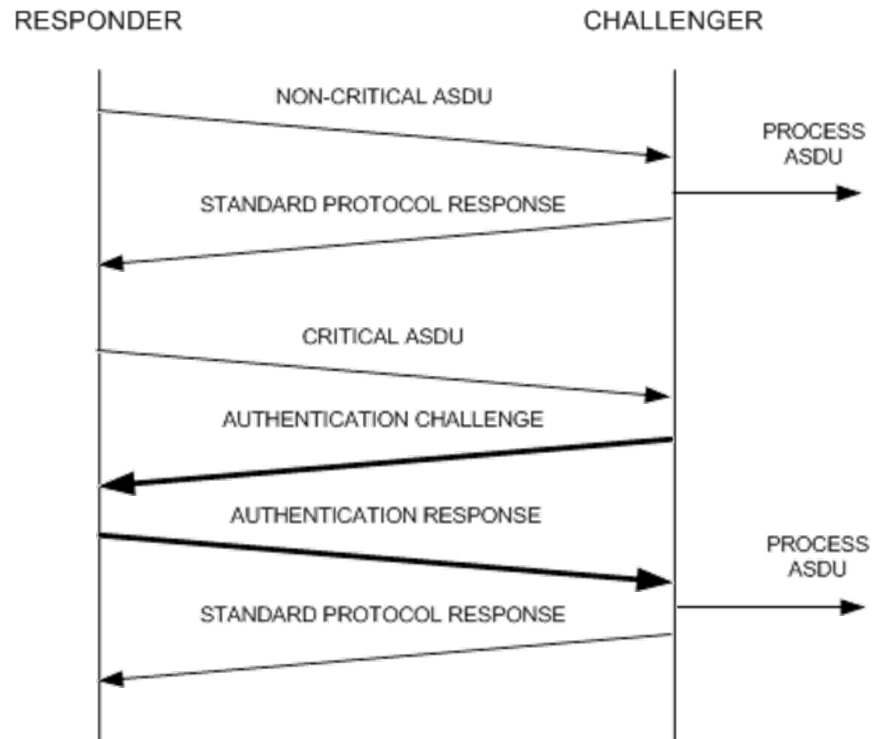
User Authentication and Data Integrity

IEC 62351-5

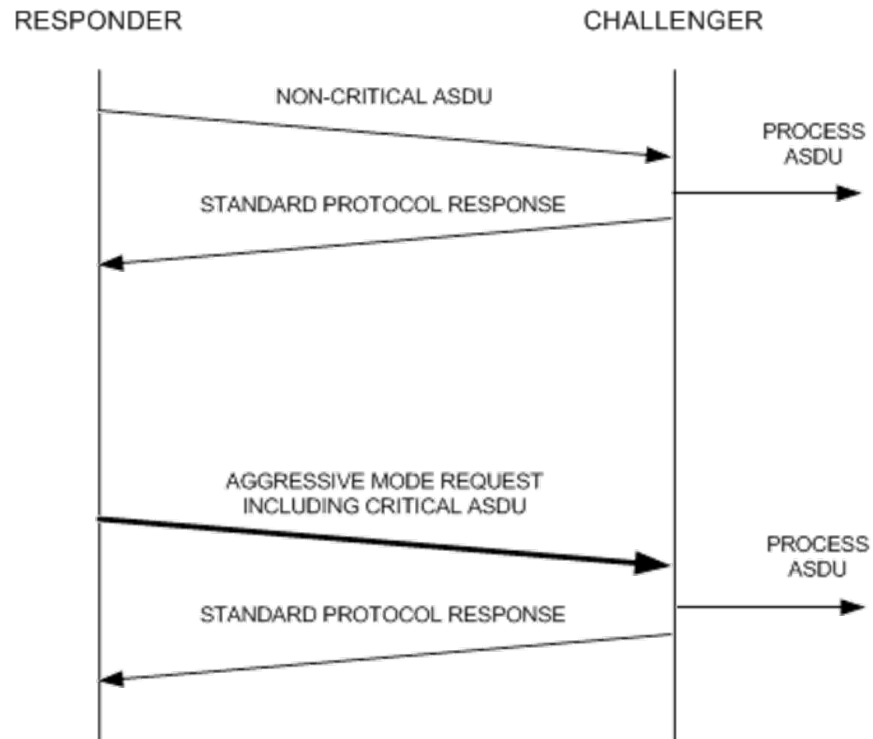
Securing IEC 60870-5 and derivatives, such as DNP3:

- > Defines a challenge-response mechanism that addresses the following threats:
 - Spoofing, Modification, Replay.
 - Eavesdropping - on exchanges of cryptographic keys only, not on other data.
 - Non-repudiation – to the extent of identifying individual users of the system.
- > Application layer only
 - Supports bridging across data concentrators and networks with different media types.
 - Protects against rogue applications.
 - Provides the capability of authenticating individual users.
- > Bidirectional

Securing Control Operations Through DNP3 Secure Authentication



DNP3 Secure Authentication Aggressive Mode



Authentication Challenge

- > Authentication challenge message (g120v1)
 - Sequence number
 - User number – identifies session keys to use
 - HMAC algorithm – SHA-1 (4 or 10 octets), SHA-256 (8 or 16 octets)
 - Reason for challenge – CRITICAL function. Previous ASDU must be included in calculation of HMAC.
 - Pseudo-random challenge data

Authentication Reply

- > Authentication reply message (g120v2)
 - Sequence number
 - User number
 - HMAC value

DNP3 Secure Authentication

Key Benefits and Issues

- > Relatively lightweight, uses cryptography but does not encrypt data.
- > Can be combined with TLS if confidentiality required.
- > Independent of transport, can be used with serial or network communications.
- > Added as new messages to protocol. Can interoperate with legacy devices.
- > Standard supports the use of data concentrators.
- > Management of encryption keys is not defined and remains to be addressed.
- > Now supported by IEEE as IEEE P1815.

Authenticating Users and Systems

> Requirements

- Only authorized devices can connect to the distribution automation system.
- Individual user accounts.
- Granular access permissions.
- Support remote maintenance access.
- Support local maintenance access.
- Manage access locally, even when no connection is available.

- > International Telecommunication Union (ITU) standard that defines a Public Key Infrastructure (PKI) based on:
 - Certificate Authorities (CA)
 - Public key certificates
 - Attribute certificates
 - Certificate revocation lists

Asymmetric Cryptography or Public Key Cryptography

- > The basics...
 - In **symmetric** cryptography both parties share a secret key used 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.
 - 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.

Digital Signatures

- > Asymmetric cryptography can be used to authenticate the sender and to protect the contents of a message:
 - Before sending a message, Alice calculates a hash of the message.
 - Alice encrypts the hash with her private key, adds it to the message as a **digital signature** and sends the message.
 - Bob calculates the hash of the received message.
 - He extracts the signature and uses Alice's public key to decrypt it.
 - If the hash matches, Bob can be certain it comes from Alice and was not tampered with.

Certificate Authority

- > A **Certificate Authority** (CA) acts a trusted third party that validates individuals and issues public keys.
 - Alice generates a key pair
 - She sends the public key to the CA
 - The CA confirms her identity
 - The CA generates an electronic document that contains the user's name and public key
 - The CA signs this document using its own private key
 - The signed document is called a **public key certificate**

Establishing Trust

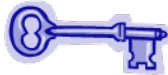
- > To set up a Public Key Infrastructure (PKI):
 - The CA's public key certificate is distributed to all parties.
 - A party that trusts the CA can then use the CA's public key to validate the authenticity of a public key certificate provided by an unknown user.
 - If the signature on the certificate 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.

Using Certificates

Certificate Authority



Alice sends her public key to be signed by the CA



Bob retrieves a copy of the CA public key certificate

The CA issues Alice a signed public key certificate

Bob trusts that the message is really from Alice since it is signed with a certificate issued by the trusted CA



Alice's Certificate



Alice



Alice sends a message to Bob signed with her certificate

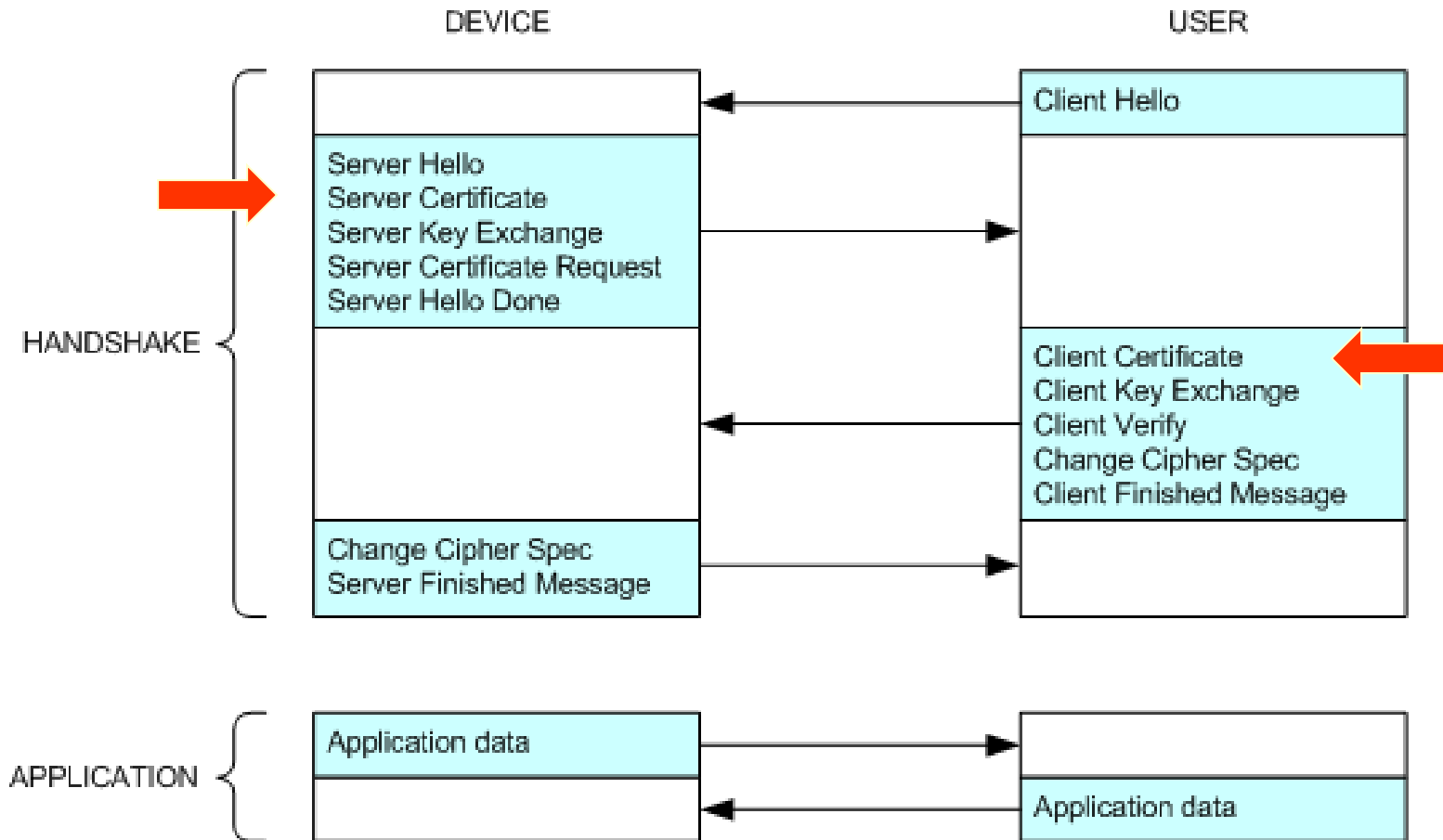


Bob



CA Certificate

Transport Layer Security



Authenticating and Assigning Permissions

- > Each user has a public key certificate used for identification purposes.
- > Each device has a public key certificate to identify it.
- > Each user has an **attribute certificate** used to assign permissions.
- > Attribute certificates are similar to public key certificates but are used to establish access permissions.
- > The X.509 standard defines attribute certificates, but there is currently no standard format to define device permissions.

Revoking Access

- > Certificates have a limited lifetime
 - Device certificates typically have a very long lifetime.
 - User certificates typically have a shorter lifetime.
 - Attribute certificates typically have an even shorter lifetime.
- > Certificates can be revoked before their expiration
 - The **Online Certificate Status Protocol (OCSP)** can be used to validate a certificate when a connection is available.
 - **Certificate Revocation Lists (CRL)** can be propagated on a periodic basis.

Conclusion

Many technologies and standards are already available to meet the security requirements of distribution automation.

However, there remain gaps and work is still in progress to establish the required standards and best practices.

To achieve its original “interactive network” vision, Hydro-Québec specified from the beginning that –

- Automation components provide sufficient processing power
- Be remotely upgradable
- Comply with existing standards, including security

By thus “future-proofing” its solution, Hydro-Québec has been able to evolve its solution as functional and security requirements evolve.

Contact Information

Jacques Benoit

Senior Analyst Information Security
Cooper Power Systems
Jacques.Benoit@CooperIndustries.com

Serge Gagnon

Chargé de projets informatiques
Hydro-Québec
gagnon.serge@hydro.qc.ca

Luc Tétrault

Ingénieur Automatismes
Hydro-Québec
Tetreault.Luc.2@hydro.qc.ca