Design and commissioning of a massive IEC61850 Multivendor Substation Automation Project: A twisted path

Case Study

Diego Quintero, P. Eng.,
Telecommunication Engineer
Kari Blyth, P. Eng,
Senior Engineer, P&C – Digital Power Systems

September 2020

BBA

Disclaimer

This document is provided for informational purposes only. Anyone who uses this document is responsible for determining whether or not it applies to his or her activities. At no time will BBA or the author be held liable for any error or omission that the document may contain or that may result from its use.

The information contained in this document is subject to change without notice.

Diego Quintero P. Eng
Kari Blyth, P. Eng.

Executive Summary

Technologies, such as IEC61850, introduce the need for a different engineering approach to electrical protection networks (EPN). Traditional telecommunication networks transporting information, require a new approach in design and architecture capable of responding to these emerging technologies.

These new protection networks have very precise requirements, such as GOOSE messages, in which a time greater than 3 ms is not allowed between the moment an event occurs and a protection signal is received.

This is why factors such as performance, reliability, redundancy, and cybersecurity are elements that become relevant when defining the network architecture and telecommunication protocols to use.

Table of Contents

EPN project scope

Introduction

The client is an Oil Sands site with an electrical transmission and distribution system to support the oil sand production. The electrical system is tied to the Alberta Interconnected Electric System (AIES) with two 260kV transmission lines. The 260kV is transformed to 144kV and is delivered through two 144kV ring bus substations. The 144kV is further transformed to 72kV, 34.5kV and 13.8kV before it reaches the process plant utilization voltages of 13.8kV, 4.16kV and 600V. 72kV is distributed throughout the mine, while 34.5kV and 13.8kV are distributed to the process areas for plant operation. As a result, there are 56 different electrical equipment buildings with the associated protection, control and visibility.

Protection and Control

The protection and control system of the electrical system is one of the largest in North America. It consists of more than 1100 IEDs (Intelligent Electrical Devices), from different vendors, distributed in 56 different buildings. The 144kV substations are equipped with two protection and control schemes. Scheme A and B, each implemented with a different vendor for all of the protection and control functions including bus protection, breaker failure and bay control units (BCUs). Scheme A utilizes a point-to point process bus technology, while Scheme B uses conventional copper wiring to instrument transformers. In the lower voltage levels, non-redundant relays with conventional copper design provide the protection and control.

IEC61850 is the main communication protocol for the station and bay level. MMS (Manufacturing Message Specification) provides vertical communication to exchange data between the IEDs and gateways, while GOOSE (Generic Object Oriented System Event) facilitates horizontal communication to exchange data between IEDs. All IEDs are connected to two redundant Ethernet networks, called A and B networks, using PRP (parallel redundancy protocol). IEDs with no PRP capability are connected via a RedBox (redundancy Box) to the PRP network.

The following GOOSE applications are deployed in the project:

- Breaker Failure Initiate: Breaker management relays are responsible for the breaker failure protection. Protection trips initiating a breaker failure send their initiate signal via GOOSE messages to the breaker management relay. There is no hard wire connection for the external breaker failure initiate signal.
- Breaker Failure Trip: The breaker management relays receive the initiate signals from the protection relays via GOOSE and process the breaker failure protection function, then publish a breaker failure trip GOOSE message, where needed. Breaker management relays responsible for tripping the remote breakers will receive the GOOSE message for a breaker failure trip and trip the breaker after verifying the healthiness of the GOOSE message.
- Transfer Trip: Upstream breakers to a transformer will be tripped by local protection via GOOSE message. The breaker management relays responsible for tripping the remote breakers will receive the GOOSE trip signal and trip the breaker after verifying the healthiness of the GOOSE message.
- Zone Interlocking: GOOSE messages are utilized to communicate blocking signals in the Zone Interlocking Schemes, to mitigate high arc flash incident energy.
- Local/Remote Interlocking: The redundant bay controllers communicate their Local/Remote status via GOOSE to each other. The Logic inside the relays evaluates the status to ensure the two relays have the same status.
- Operating mode selector switch: All IEDs, 72kV and higher, are equipped with a selector switch to select between; “In Service”, “Out of Service” and “Test” modes. When an IED is in test mode, a GOOSE message will be published, and all of the subscribers block any trip signal from that publisher(IED). The built-in test mode capability of IEC61850 was not used in this project, as edition 1 of the standard did not specify requirements for implementing its testing methods.
- Provisions for load-shedding: GOOSE messages were considered as the communication means for the load shedding scheme. The load shedding scheme was to be implemented after the project. However, all of the required provisions had to be included into the design.

Diego Quintero P. Eng
Kari Blyth, P. Eng.

Substation Automation

The Electrical Protection Network (EPN) is an application designed for protection, control and monitoring. It ensures proper communications to implement the fast load shedding scheme, station inter-tripping and zone interlocking for the power system. Monitoring of the system takes place at both the station level as well as the control room level.

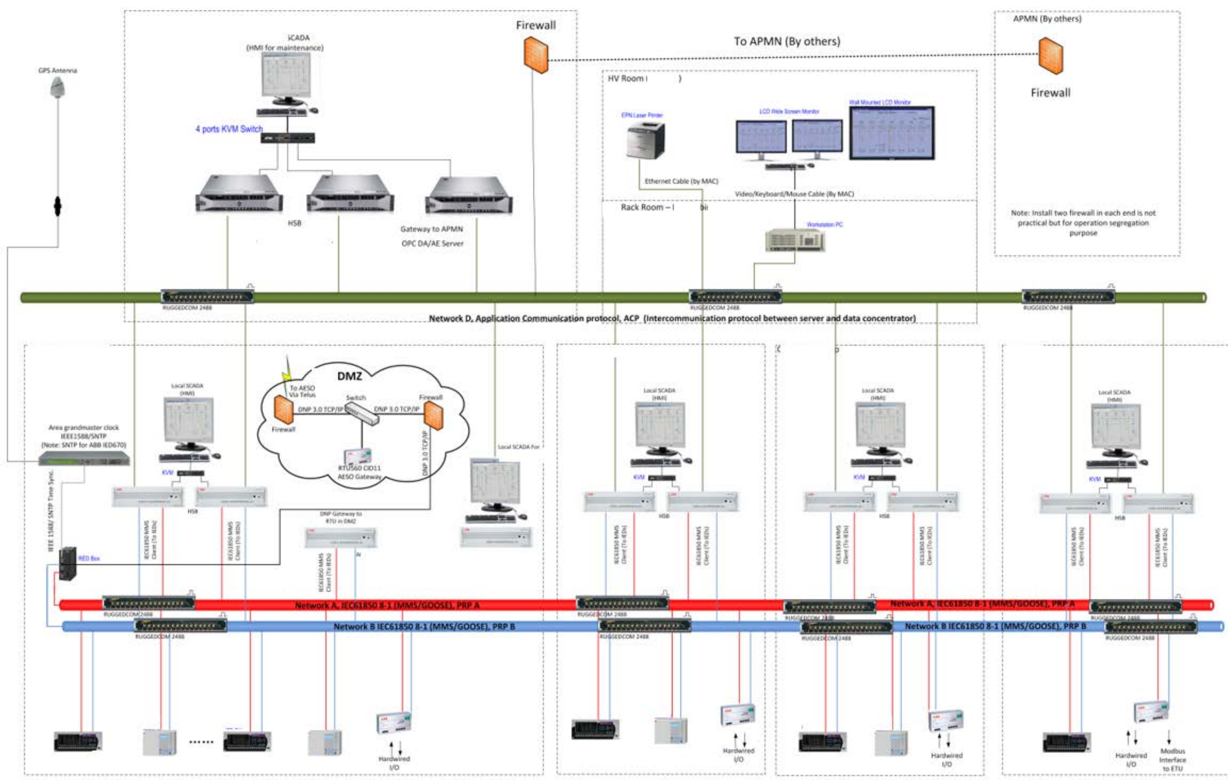

Figure 1: Conceptual System Architecture

There are three communication networks for the EPN:

- A and B for IEC61850 station communication, shown as red and blue in Figure 1.
- D (Data) for engineering (shown as green in Fig. 1) as well as plant wide data exchange, such as Central control room SCADA and AESO regional control centre.

The A and B networks utilize PRP, as per IEC62439-3, to increase the reliability of the system and minimize the network recovery time. A and B networks are utilized for electrical protection application, therefore ensuring fast and reliable protection. D network facilitates the information exchange between substations as well as both the local station and central control room SCADA.

In order to provide a network that services both protection and data sharing, the following components were utilized:

- IEDs
- Substation RTU
- Network
- HSB SCADA/Data concentrator
- AESO Gateway
- OPC Server

Time Synchronization

The EPN is broken into various time domains. A GPS clock capable of both SNTP and PTP (Precision time protocol) is located in different substations.

Scheme A IEDs utilize PTP from GPS. Scheme B IEDs utilize SNTP from the distribution/edge switches. A secondary source is provided by the local SCADA in each station.

SCADA / Gateway

A redundant hot and standby local SCADA provides local control and monitoring in each of the 56 buildings. IEC61850 MMS (Manufacturing Message Specification) is the main communication protocol. Modbus TCP/IP, DNP3 and SNMP are other communication protocols used in the local SCADA.

The main functionalities in this SCADA consist of :

- Visibility: Single Line Diagram, Measuring, System Supervision
- Control: 600 V breakers and above, MODs, Transformer Tap Changer Control
- Alarm List
- Event List

A centralized hot and standby SCADA in the centralized control center provides visibility of the whole facility. Additionally, a gateway provides data to two external SCADAs.

Network Design

Introduction

As described above, the EPN network consists of more than 1100 IEDs in 56 electrical rooms where GOOSE, MMS and PTP protocols are critical in the operation of the EPN. This telecommunication network was originally a flat, layer 2 network, whose redundancy was achieved using PRP architecture.

Client Concern

The implementation of a flat network and traffic management was a concern identified by Operations as the network was becoming flooded due to high levels of traffic, generated by protocols such as GOOSE and PTP during an abnormal operation, such as a trip or device malfunction.

In order to understand the cause of network flooding, a thorough review of the existing network architecture, provided by Operations, was performed. With this analysis complete, understanding of the cause of network flooding, as well as determination that a new segregated network architecture would support efficient data transport and eliminate network flooding, was attained.

Next Steps

The new segregated architecture design was based on the Purdue model. This architecture helps to define data flow between different devices like IEDs, servers, HMIs, switches, etc., based on the role of the devices.

The architecture uses all Purdue levels. Levels 0 to 2 are for Process, Basic Control and Area Supervisory Control hosting devices like sensors, IEDs, HMIs, control room workstations, RTUs, PLCs, etc. Level 3 covers site manufacturing operations and control, hosting services like historians, production/scheduling systems, IT services, engineering workstations, file sharing, etc. Level 4 is for site business planning and logistics, it hosts services like IT services, inventory systems, scheduling systems, print servers, email, etc. However, for the EPN project there is an improvement respective to the general model; it is the implementation of a new level between 3 and 4, named level 3.5. The purpose of this level is to create a buffer zone, called the DMZ, to host services like file transfer, data gateway, patch/av servers, remote access solution, etc., that allow information to be exchanged between operations and the business level. Finally, levels 5 and up cover the corporate services. In this way, any direct and uncontrolled connection between the corporate and the operations is avoided, thus guaranteeing a high level of cybersecurity of the EPN network.

This new architecture meets the EPN network requirements identified below, as well as provides changes to data transport and cybersecurity of the telecommunications network:

- Isolate GOOSE and MMS at substation level.
- Integrate new solution within PRP architecture.
- Replace distributed PTP sources to a single, centralized PTP network source.
- Both the existing and proposed architecture must interoperate without interruptions until complete deployment of the new architecture is achieved.
- Minimize substation downtime during architecture migration.
- Autonomy of the Operations team to implement the new architecture.

To design a new architecture that meets the requirements and carry out the migration efficiently and without interruption to the operating EPN, several different stages in the re-design were considered:

- Design review of the original design,
- Design of the new architecture,
- Transition between the new and the old architecture,
- Decommissioning of old infrastructure,
- Cleanup and final tuning.

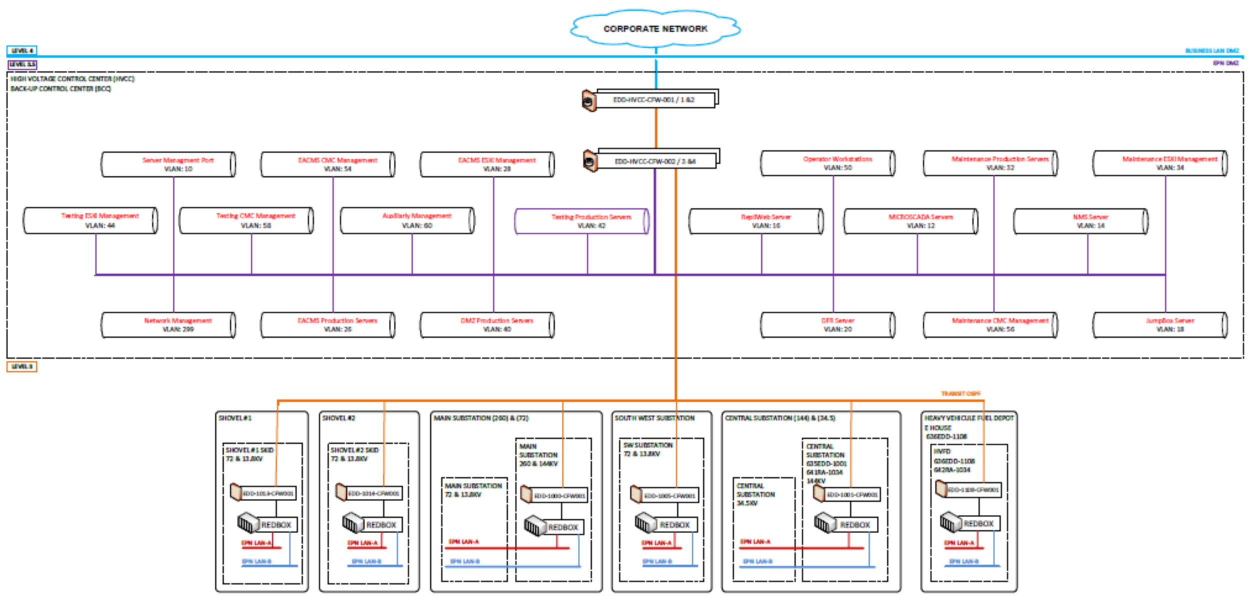

Figure 2: Network Architecture

Design Development

The new architecture segregates the previous flat network into a dedicated network per substation, with connectivity through the ‘D’ network to the upper network level. For each substation network, it would consist of three different VLANs:

- SCADA and MMS

- Management
- GOOSE

Special consideration was given when connecting end devices that send GOOSE and MMS messages, since GOOSE messages are tagged, and MMS messages are untagged at the switch.

IP Address Scheme

The first step was to define an IP address scheme. On the flat network a class B network was used to address every single device on the network. The new IP address scheme used a class A network, with subnets adapted, to cover each substation.

The main criteria for the new IP scheme is:

- Understanding the current and future IP addresses required per substation.
- Scalability to support future requirements like the addition of new end devices or a new sub-station.
- Manage the subnets in order to support summarization, for routing purposes or ACL definitions, if required.
- Isolation between management VLAN and SCADA VLAN.
- The first usable IP to address the default gateway.

Laboratory Testing and Configuration

In order to validate the new architecture, a test environment with site equipment and new configurations was established. This would ensure the following requirements were specifically assessed:

- Interoperability of technologies from different vendors for various devices such as switches, redboxes and firewalls,
- Redundant uplinks performance,
- Firewall failover and convergence time,
- OSPF convergence time,
- Centralization of PTP and multicast routing requirements,

- Protocol layer 2 or 3 behaviour of PRP, GOOSE, MMS, and PTP,
- GOOSE and MMS configuration of IEDs links.

During laboratory tests, all of the substation firewalls, as well as the core firewalls, were physically validated, upgraded, installed, and configured using the new architecture specifications.

Design Migration

The transition to the new segregated architecture was done through a rigorous process of development and validation, while maintaining a very fluid communication with the Operations team to understand requirements and needs of the EPN network (see figure 3).

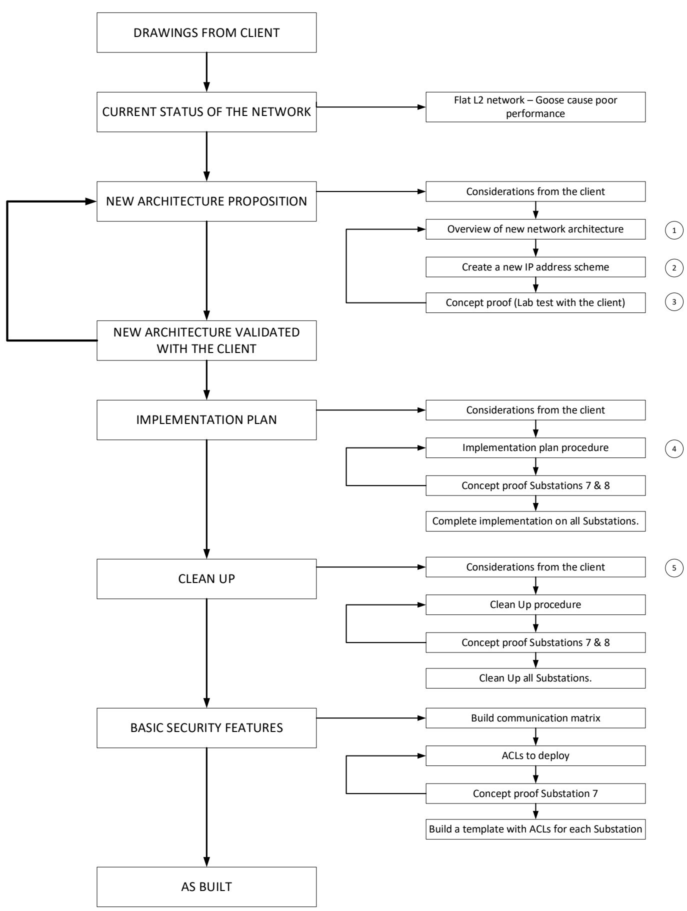

Figure 3: Segregation process

Flat PRP Network
Initial design of the EPN network was a PRP network connecting the end devices. The PRP network consists of two independent parallel networks (LAN A and LAN B) to communicate with the IED's. Therefore, the connected devices must support PRP to manage duplicated packets. Devices that do not support PRP were connected through a RedBox, acting as an interface, to allow connection to a PRP network.

All of the MMS data transfer between the devices and local substation SCADA was done through a flat LAN (LAN D). In this LAN segment, all of the core devices (clocks, HMIs, redboxes, etc.…) were connected, and this weighed heavily on the performance of the network.

Hybrid network
During the re-design, a specific challenge appeared, which was how to implement the new architecture while co-existing with existing architecture during transition to the segregated network. The main consideration was to migrate each substation to the segregated network without decommissioning anything, in the event a rollback was required. To achieve this smooth transition, the following changes at the core level were performed first:

- Installation, configuration and commissioning of two core firewalls to manage the communication with the substations.
- Configuration of new IP addresses on servers and devices to communicate with the new architecture, while keeping communications with the legacy network.

Segregated Network
The transition to the segregated network for each substation required the configuration of the new IP address scheme, installation of a firewall to isolate and control of the incoming and outgoing traffic. At the end of the migration, all substation firewalls were connected to an upper level firewall. This firewall is responsible for managing the traffic flow between sub-stations or with upper levels of the architecture.

The work required in the substations included:

- Installation, configuration and commissioning of substation firewalls (uplinks and downlinks).

- Change the old IPs to the new IP scheme on switches, IEDs, redboxes, etc.
- Remove any configuration related to the legacy network.
- Connectivity tests for each VLAN on the substation.
- Validate that operational requirements of the substation were met.
- Once a substation was migrated, all of the network traffic flowed through the new architecture and was controlled by the network firewalls.

Once the substations were migrated to the segregated network, all of the functionality of the new architecture previously tested in the laboratory were functioning and fine tuned.

The main features of the new segregated network were:

- The routing protocol used was Open Shortest Path First (OSPF) to grant the packet flow between all the network levels.
- Between the substation and core firewalls (see figure 2), redundant interfaces were configured to guarantee robustness in case of failures of a physical link.
- The two core firewalls were deployed in failover mode; this feature keeps the system up and running in case of physical damage or problems on one of the firewalls.
- The traffic flow is controlled by (Access Control List) ACLs configured on the firewalls based on the desired traffic flow of information.
- Since the firewalls did not support PTP, multi-cast routing was used to allow PTP traffic to reach the devices on each substation.
- Because of IEC61850 definition for GOOSE and MMS, the communication between the switch and the IED's must be configured using trunks on the switch.
- The allowed VLANs on the IED's trunks were the ones to transport GOOSE (tagged) and MMS (untagged).
- The native VLAN (untagged VLAN) on the trunk was defined as the one that transports MMS.

Once all of the substations were communicating through the new architecture and the performance was validated, a decommissioning process was carried out to clean up all cabling and legacy IPs. At this point, all communications between the core and substations were managed by the firewalls installed during the segregation process.

The final step was the deployment of minimal security features, laying the foundations for the next phase of the project in terms of cybersecurity.

Conclusion

Based on project experience in the last decade, the engineering of multi-vendor system needs additional considerations and controls in order to deliver a functional system meeting the requirements. Previous experience has demonstrated, time after time, that the following elements are key considerations to ensure project success:

- Emerging technologies, like IEC61850, depend heavily on the network requiring a strong collaboration between network designers and substation engineers.
- Introduction of new technologies requires system monitoring to ensure that it is performing as designed but, more importantly, as Operations requires. Often with new technologies, unexpected issues arise that need to be addressed.
- Understanding behavior of different protocols on operation networks, like the EPN, allows design of robust data networks that support the operations in a reliable manner and avoidance of problems related to performance loss, due to poor data network design.
- It is important to recognize that the new design must manage both the transition stage and the final stage equally, without unacceptable risk to Operations.
- Proof of concept validation (LAB testing) before deploying, validating the engineering process, system functionalities, performance, and interoperability is a proven method to manage both design and implementation risk.

About the Authors

Diego Quintero, P. Eng.

Telecommunication Engineer
Diego.Quintero@bba.ca

Diego is an engineer with over 15 years of experience in networks and telecommunications. His skills are primarily in the planning of interventions in network infrastructures, management of engineering packages (Satellite, LTE, FO, VHF, etc.), network support, and commissioning.

He was an active contributor to the EPN network segregation project. His leadership and involvement were in different stages of the project: detailed engineering, solution design, laboratory tests, commissioning and testing, as well as technical support.

Kari Blyth, P. Eng.

Protection and Control Engineer
Kari.Blyth@bba.ca

Kari's is an engineer with over 20 years of experience in electrical transmission and distribution systems. Her experience spans both system operation and engineering (Owner and consultant) of electrical systems from 600V to 260kV.

Kari lead the team that developed the EPN network.

BBA

bba.ca