DIGITAL TRANSFORMATION OF SUBSTATION THROUGH IEC61850 STANDARD: EXPERIENCE DEPLOYING DIGITAL SUBSTATION PILOT THROUGH DIGITAL SUBSTATION REPLICA

SAURABH TALWAR (ST), ERIC LOISELLE (ES), DAVID LAMBERT (DL), WILLIAM BOUTIN (WB), MICHEL LAVALLEE (ML), FELIPE SARUBBI (FS)

Siemens Canada Limited, Hydro-Québec
Canada

SUMMARY

Digital Substation is a term applied to electrical substations in which operational assets are interconnected by a communication network backbone. IEC61850 substation standard is not new in the industry but has been a strong enabler for digital transformation of substations. IEC61850 communication protocol enables digitalization at both Process and Station levels. This uniform communication protocol offers interoperability among products of different manufacturers and a platform for peer-to-peer communication though GOOSE (Generic Object Oriented Substation Events) messaging. More recently, IEC61850 application has been extended to include communication between substations and the upstream connection to control centres.

Most of the substations deployed at Hydro-Québec were deployed in the 80's and 90's and most of these substations have aging Protection & Control systems which require an upgrade in the coming years. Digitalizing a substation changes the Cyber Security risk management approach which in turn requires adjustments to substation security strategy. Cyber Security measures are essential for substations considering liability, operational reliability and 20-year lifespan.

This paper aims at sharing experience in deploying first ever IEC61850 digital substation pilot project at Hydro-Québec. This paper will also provide a utility's perspective into main drivers of digitalization along with the technical and organizational challenges faced during digital transformation. The concept of digital replication of substation to optimize testing and commissioning both during Factory Acceptance Test (FAT) and Site Acceptance Test (SAT) will be explained. Lastly, the importance of Operation Technology (OT) Cyber Security in a digital substation will be highlighted.

KEYWORDS

Digital Transformation, IEC61850 Standard, Protection & Control, Operation Technology (OT), Cyber Security, IEC62443, IEC 62351, Pilot Project.

1. INTRODUCTION

The protection and control system (P&C) are critical for the reliability of the transmission network. Performance issues, design and setting errors could cause power outages and electrical apparatus damages. To minimize malfunctions and mis-operation, strong knowledge of P&C is required and stringent tests and validation (homologation) are performed and needed. Power utilities tend to rely on standardization, which help in cost control and maintain reliability. To put in service a complete P&C system of an entire substation is a long process that requires lot of coordination.

Hydro-Québec owns approximately 550 substations. 325 of 550 are categorized as load substations feeding distribution networks. 180 of them are still equipped with conventional RTU that were deployed in the 80's and 90's and most of these substations have aging Protection & Control systems which require an upgrade in the coming years.

2. DIGITAL TRANSFORMATION

2.1 MAIN DRIVERS

Digital transformation allows for a new Protection & Control architecture with increased functional integration and project optimization opportunities. Moreover, digitalization helps to reduce the number of equipment / assets and wiring works within a substation which helps in overall cost reduction. Reduction in equipment or panels will further help reduction of control building size. In addition, digitalization through IEC61850 offers guideline for standardization of new technologies, including protocols, data model, configuration language, asset management and project specification. Conventional wiring is dramatically reduced alongside simplified engineering drawings through digitalization via IEC61850. The efforts in panel and cabling works are shifted more towards software configuration. This is significant and necessary considering substations which have complex environment with many hazards where special authorization, approval, training and supervision is required.

Digitalization means access to more data which can be used for asset management of electric network, and performance analysis.

2.2 CHALLENGES

Complexity
Digitalization brings new technologies, approach, processes and procedures which all require specialized expertise. As a result, all personnel (engineers, operators, technicians) need to be trained to the point where they are comfortable in handling new technologies.

Performance
New technology brings its own complexity. Extensive performance testing and validation of new technology is needed.

Business Coordination and New Technology Life-Span
Numerous business groups (OT, IT, Telecom, Cyber Security) are involved in a digitalization project. Seamless coordination is needed among different business groups to successful operation. Also, selection of new technologies must be made keeping in mind 20-year life span.

In-house Standards
Some utilities have their own in-house standards (for example, existing communication protocol) which are not supported by vendors. Finding ways to integrate new technologies with existing in-house standards adds a new challenge.

Cyber Security
With digitalization more devices are connected and integrated on the network thus increasing cyber threat landscape. Strong Cyber Security measures are needed to mitigate risk of cyber threats.

2.3 WHY IEC 61850

Digital Substation is a term applied to electrical substations in which operational assets are interconnected by a communication network backbone. IEC61850 substation standard is not new in the industry but has been a strong enabler for digital transformation of substations. IEC61850 standard was specifically designed for substation level and enables digitalization at both Process and Station levels. This uniform communication protocol offers interoperability among products of different manufacturers and a platform for peer-to-peer communication though GOOSE messaging (enabling de-centralization at a substation level).

In addition, digitalization through IEC61850 offers guideline for standardization of new technologies, including protocols, data model, configuration language, asset management and project specification.

The standardized approach of identifying signals and configuration language offered by IEC61850 standard provides efficiency in the following areas:

a. Signal structure remains the same at different levels (bay / relay level, substation controller level, gateway level and control center level)
b. Signal list generation
c. Seamless integration with configuration languages (SCD, CID, IID) at substation controller, gateway and control center levels (not supported by DNP3.0)
d. GOOSE (Generic Object-Oriented Substation Events) protocol for de-centralized communication and time critical applications
e. Troubleshooting and diagnostics
f. Cyber security related events / signals via IEC61850

With the above mentioned efficiencies more recently IEC61850 application has been extended to include communication between substations and the upstream connection to control centers.

2.4 NEED FOR PILOT PROJECT

The standard approach for Hydro-Québec is to carryout homologation (type testing, functional testing, application testing) for every IED as part of the design. This is an extensive process that requires strong expertise and many months of testing and validation. So far, Hydro-Québec does not have strong expertise and experience with IEC 61850 P&C deployment. Also, the requirements for integration of IT and Cyber Security are uncertain for Hydro-Québec. As a result, need for vendor to provide expertise and an overall solution is preferable (not conventional approach by Hydro-Québec) to reduce project risk and timeline.

To test, validate and approve vendor overall solution, Hydro-Québec decided to carryout IEC 61850 pilot project at Saint-Chrysostome site (120Kv with 5No. feeders, 2No. 47MVA transformers). The pilot project involved new IEC 61850 P&C architecture design (with single vendor solution and no process bus) with IT and Cyber Security integration in a pre-fabricated control building.

3. NEW IEC61850 PROTECTION AND CONTROL ARCHITECTURE DESIGN

Standardized P&C Architecture

The standardized P&C HQ system is made with dedicated IEDs for protection, control / measurement and automation controller for logics (voltage regulation, service restoration, line transfer, recloser, etc.). In a traditional way, all indications, initiation or blocking signals that are required to be exchanged between IEDs (protection, control and automation controllers) are wired [1] – [2].

New IEC61850 P&C Architecture

Digitalization with new numerical IEDs and IEC 61850 allow for more functional integration permitting reduction of number of P&C IEDs to carry out the same applications. IEC 61850 GOOSE protocol provides the platform for a de-centralized approach (peer-to-peer communication) and thus replacing hardwiring between IEDs. This new P&C architecture focuses on leveraging protection, control and measurement functionalities in the same IED. In addition, all automation logics are concentrated in one controller which is purely dedicated to exchange signals over communication protocol [1] – [2].

Figure 1 shows the major differences between standardized and new IEC 61850 P&C architecture design.

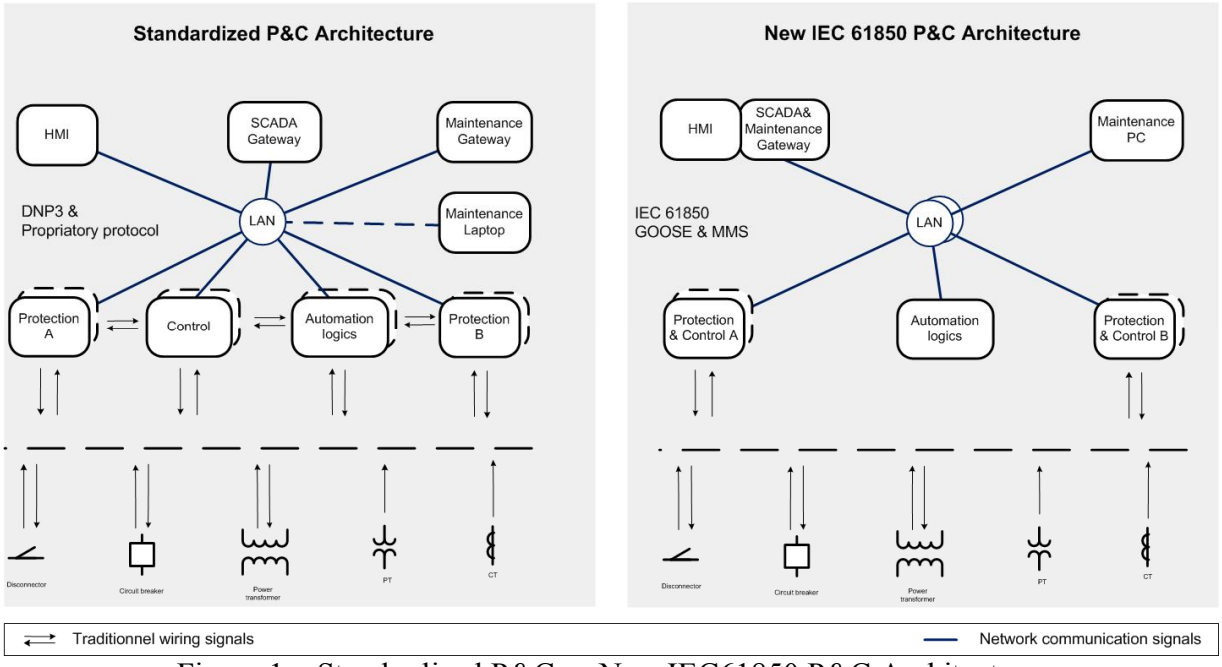

Figure 1 – Standardized P&C vs New IEC61850 P&C Architecture

4. DESIGN AND CONFIGURATION OF IEC61850 COMMUNICATION

The design and configuration process undertaken for this project is shown in figure 2. The

intent of this approach is to standardize the design and configuration of IEC61850 data modeling for all future IEC61850 digital substation projects at Hydro-Québec [3] - [7].

Phase 1 – IEC 61850 Data Modeling Requirements
This phase focused on identifying all the signal required at operator, maintenance and cyber security control centers based on Hydro-Québec TransEnergie guidelines and specifications.

Phase 2 – IEC 61850 Hydro-Québec Data Profile
The IEC61850 nomenclature of all signal required from different types of IEDs, station controllers, RTUs, gateway and automation functions are defined and the correlation is build and visualized in UML format. The result of this phase is generation of generic IEC61850 SSD file applicable for all IEC61850 digital substation projects.

Phase 3 – Hydro-Québec Specification
The generic SSD file from phase 2 is translated into project specific SSD file that is given to the vendor to comply and implement as part of their solution.

Phase 4 – System Configuration
The vendor should comply and implement with the SSD file provide by Hydro-Québec. The integration of SSD file was carried out with DIGSI 5 software for this project and a complete SCD file was generated for integration with substation controller, Hydro-Québec gateway and control center. The validation and compliance of SCD file is carried out by Hydro-Québec (in-house tool) prior to integration.

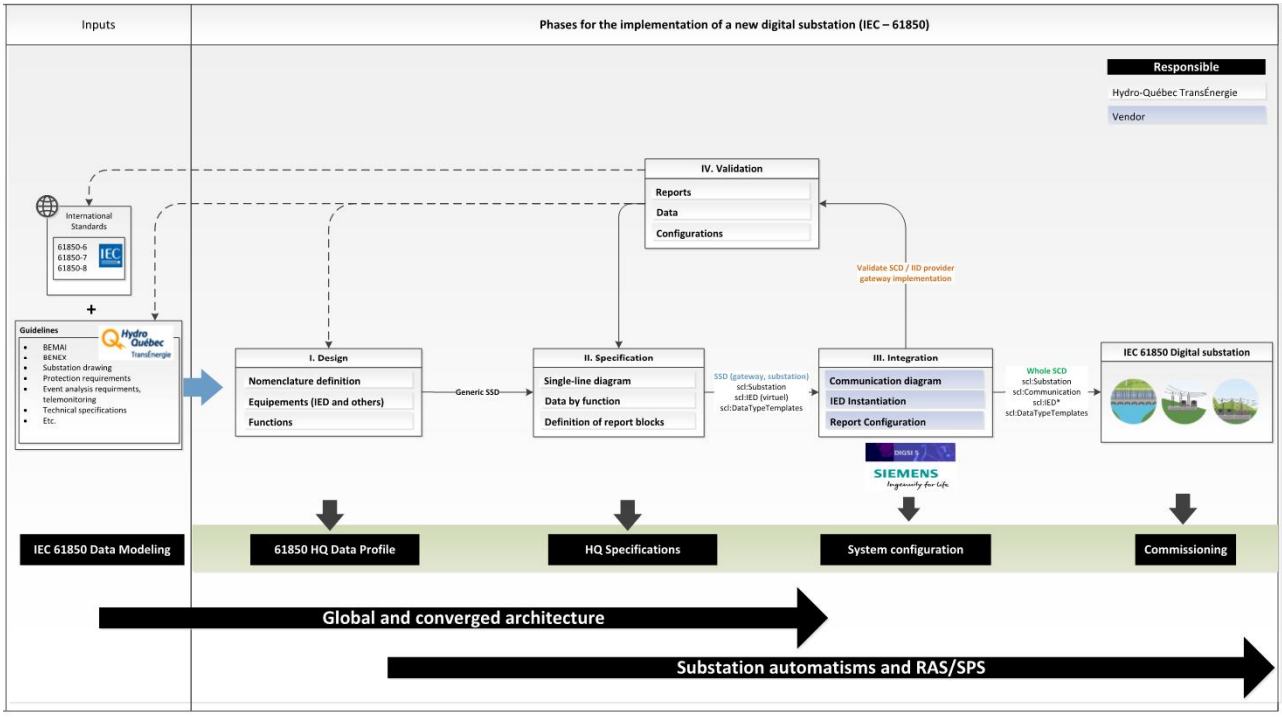

Figure 2 – Phases for implementation of IEC61850 in a digital substation

5. PILOT IEC61850 DIGITAL SUBSTATION PROJECT PHASES

Pre-project Phase
Consolidate requirements for digital substation project from all different business groups (OT P&C, IT, Telecom, Cyber Security and Civil) and generate new P&C / digital substation converge specification.

Replica Testing Phase
The replica is a panel that houses all the IT / OT IEDs to be installed and commissioned at site. All the IEDs on the replica are configured to match the configuration at site including all IT and Cyber Security measures. Solution-based functional testing is carried out on replica with the help of Hydro-Québec developed HyperSim (real-time simulator for mimicking actual power grid system). With the help HyperSim, the performance of the new P&C system was evaluated through simulating numerous different power system faults and by evaluating deterministic behavior of all automation logics. This specific substation simulation approach was new to Hydro-Québec and could be the norm moving forward.
After testing and validation, the configuration of the replica is frozen and the exact same configuration / measures are deployed at site to reduce significant testing time in the field.

FAT (Building / Panels)
During this phase, all the building and panel electrical wiring and OT / IT / Cyber Security functional tests are carried out. In addition, all communication testing with gateway and control center are validated with complete end-to-end enterprise connectivity.

SAT (MER / MES)
During site commissioning, it is extremely critical to implement the exact same configuration tested and validation on replica system to avoid re-testing of the complete system. The testing covered in this phase only focuses on the following:

a. CT / PT testing
b. Point-to-Point testing between the junction boxes in the field and the control building
c. IT and Telecom communication testing
d. Signal verification at gateway and control center

6. PILOT IEC61850 DIGITAL SUBSTATION PROJECT TIMELINE

The timeline comparison for IEC61850 digital substation project vs conventional Hydro-Québec standardized project is shown in figure 3. The conventional Hydro-Québec standardized project involves pre-qualified materials and standardized drawings and design and takes roughly around 20 months for Saint-Chrysostome equivalent size projects. On the other hand, the IEC 61850 digital substation project took roughly around 13 months involving new design, new materials and including new IT and Cyber Security requirements. The key factors that allowed for quick project delivery were:

a. Replica testing - for validation of new technology design / solution and reduction in SAT commissioning time
b. Hydro-Québec management support and dedicated converge business resources (OT, IT, Telecom, and Cyber)
c. Hydro-Québec and vendor flexibility to adapt and change plans in a pilot project
d. Strong technical lead from vendor

The timeline of IEC 61850 digital substation pilot project is a good estimate of what is achievable and can be expected for future IEC 61850 digital substation projects of similar size and complexity.

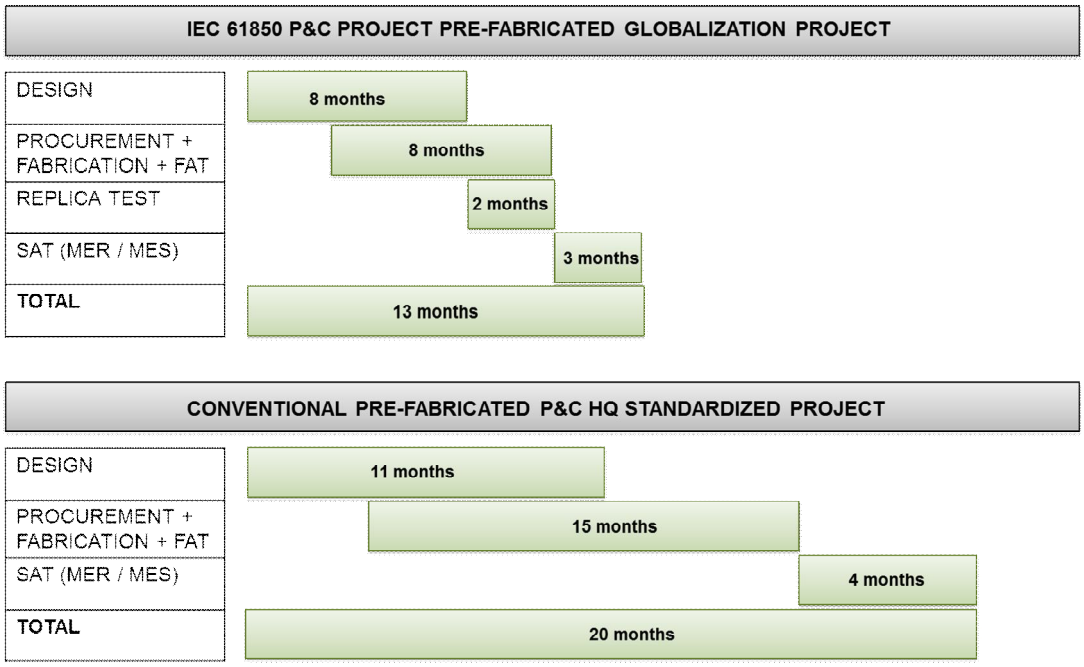

Figure 3 – New IEC61850 P&C digital substation vs Conventional P&C standardized project timelines

7. CYBER SECURITY

Cyber Security measures are well known, mature and already incorporated in Information Technology (IT) devices. On the other hand, operational technology (OT – primarily used in substations) were and are still being designed for liability and operational reliability. OT is inherently different, requires engineering know-how and not just IT expertise in order to secure them appropriately. As a result, digitalizing a substation requires changes to cybersecurity risk management traditional approach and adjustment to substation design and configuration strategy. A comprehensive risk analysis based on OT scenarios and combined OT cybersecurity frameworks (IEC62351, IEC62443, NIST) is needed to implement a tailored 5 step approach: identify, protect, detect, respond, and recover [8] – [10].

Collaborative Approach

In order to develop a tailored solution, cybersecurity experts could not work solitarily. Knowledge sharing and a collaborative approach were fundamental to the implementation of cybersecurity measures in digital substations. This project was close collaboration between the vendor and Hydro-Québec OT engineers and cyber security team. The vendor was best habilitated to explain the detailed specifications, the internal controls, and the technological limitations of their products. As well, the OT engineers were in the best position to identify the critical assets and functionalities of the digital substations. Therefore, working together and sharing our respective expertise allowed us to develop and implement cybersecurity controls without interfering with the good execution of P&C systems.

Identify

The project method consisted of a two-step approach: the first step was to use the best recognized standards in OT. The second step was to assess risk by conducting detailed

analysis. The combination of both these elements led to a conceptual framework. When applied, some challenges arose. For example, some OT cyber standards are still in development (ex. IEC62351, IEC62443). Others are approved, but suppliers have partially or are in the process of implementing within their Protection & Control systems. The solution deployed for this project not only focused on best practises but also on mitigation measures to bridge the gap until the standards are fully developed and mature.

Protect

Choosing the right OT cyber measures is essential to securing a digital substation. The measures selected for this project were based on the ability to adapt for a 20-year lifespan (for example: whitelisting, signed manufacture firmware), have no impact on liability and reliability, be tested and accepted by the engineers and the vendor, and lastly be compatible with other line of defence.

Below is a visual representation of the areas of Cybersecurity (figure 4) to be considered in a digital substation.

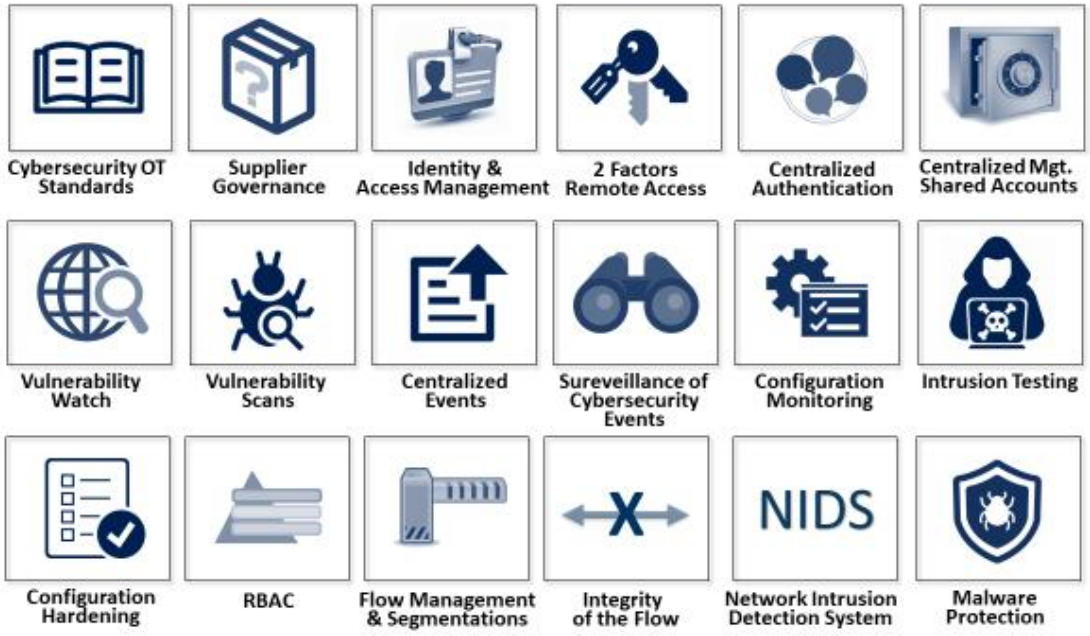

Figure 4 – Areas of Cyber Security for digital substation

Substation components are interdependent, and consideration of one measure may have an impact on another. This is paramount when choosing OT cyber measures. Moreover, it should be noted that each individual component had its own set of layers, as identified in figure 5, which also need to be secured:

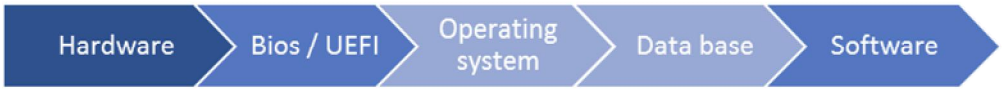

Figure 5 – Layers for different areas of Cyber Security

Detect & Respond

The digitalization of a substation provides the opportunity for better monitoring. This allowed for Security Operations Center (SOC) and OT resources to collect vital cyber security events

which helped in developing use case alerts tailored to OT technology. This is essential for the team to efficiently detect and respond to threats.

Recover
To restore the service of a substation interrupted by a cyber security incident, a detailed strategy is required. Recovery planning processes and procedures are implemented based on the recommendations of the manufacturer. Recovery plan is enforced based on criticality of the substation. To ensure the plan is current, it should also be frequently tested, and rely on previously learned lessons.

8. CONCLUSION

Digitalization for Good
Digitalization enhances P&C functionality allowing to do more with less equipments. In addition, it improves monitoring capabilities enabling asset visibility for better asset management inside a substation. Finally, digitalization provides remote access capabilities for improved troubleshooting & diagnostics and change / patch management.

Reduced in equipments and footprint
Digital transformation via IEC61850 allows for a new P&C architecture with increased functional integration and project optimisation opportunities. With increased functional integration of P&C IEDs, P&C panel footprint was reduced from 12 panels (inside existing building with conventional P&C architecture) to 4 panels (inside new building with IEC61850 P&C architecture). The 67% reduction comparison (highlighted in yellow) is shown in figure 6.

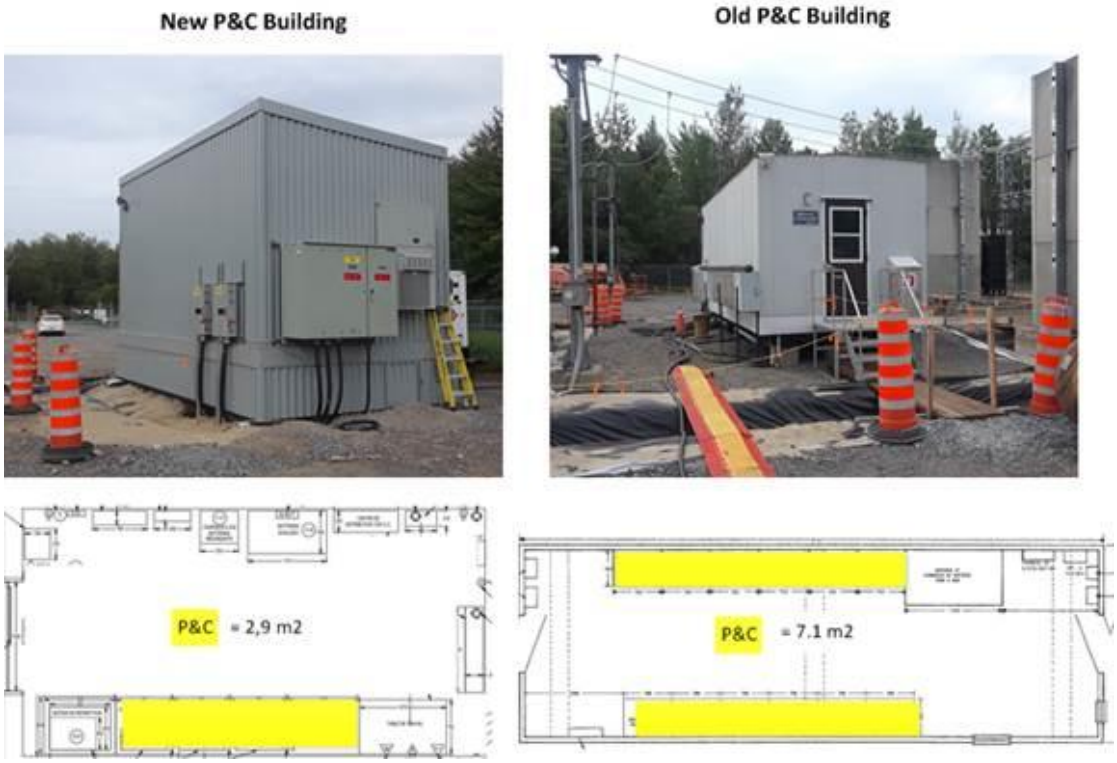

Figure 6 – Footprint comparison for New IEC61850 P&C digital substation vs Conventional P&C substation projects

Replica Approach
Introduction of replica testing approach allows for complete system testing prior to site commissioning. This approach has significantly helped to reduce the efforts and timeline associated with site commissioning. In addition, replica testing is carried out in parallel to project fabrication phase which helps to expedite the project schedule.

Future Improvement
IEC61850 provides a standarized approach for design and configuration which will allow to automate project processes (logic programming) further helping to reduce project efforts and timeline.

BIBLIOGRAPHY

[1] S. R. Chano et al., "Ancillary Protective and Control Functions Common to Multiple Protective Relays," 2011 64th Annual Conference for Protective Relay Engineers, College Station, TX, 2011, pp. 396-482.

[2] IEEE Working Group WGC15 - IEC 61850 Implementation "IEEE 2030.100-2017 - IEEE Recommended Practice for Implementing an IEC 61850-Based Substation Communications, Protection, Monitoring, and Control System," 2017.

[3] TC 57, "IEC 61850-6 Communication networks and systems for power utility automation - Part 6: Configuration description language for communication in electrical substations related to IEDs", 2009

[4] TC 57, "IEC 61850-7-4 Communication networks and systems for power utility automation - Part 7-4: Basic communication structure - Compatible logical node classes and data object classes", 2010

[5] TC 57, "IEC 61850-8-1 - Mappings to MMS (ISO 9506-1 and ISO 9506-2) and to ISO/IEC 8802-3", 2011

[6] R. Hughes and M. Jansen, "Engineering processes using IEC 61850," 2009 Australasian Universities Power Engineering Conference, Adelaide, SA, 2009, pp. 1-6.

[7] A. P. Apostolov, "UML and XML use in IEC 61850," IEEE PES T&D 2010, New Orleans, LA, 2010, pp. 1-6.

[8] R. S. H. Piggin, "Development of industrial cyber security standards: IEC 62443 for SCADA and Industrial Control System security," IET Conference on Control and Automation 2013: Uniting Problems and Solutions, Birmingham, 2013, pp. 1-6.

[9] TC 56, "IEC 62443 - Security for industrial automation and control systems," 2018

[10] TC 57, "IEC/TS 62351-1 Power systems management and associated information exchange - Data and communications security," 2007