

How a Utility Automated Its Distribution Network and Reduced Its SAIDI

Hervé Delmas, Engineer, Hydro-Québec
Robert O' Reilly, Senior Applications Engineer, Cybectec
Karine Simard, Marketing Coordinator, Cybectec



The road to a dramatic reduction in outage frequency and duration is marked by an intelligent distribution network and paved with technology. Even so, the human impact can never be ruled out.

Since 1999, the System Average Interruption Duration Index (SAIDI) in the Province of Québec had stabilized at 2 hours per customer, per year. However, 15% of Hydro-Québec's customers had a reliability index higher than 4 hours.

As Hydro-Québec decided to integrate and automate its entire distribution network in 2001, the challenge was daunting: close to 4,000 pole-top devices spread throughout a territory three times the size of California.

On a project of this magnitude, would the goal of achieving an 18% SAIDI reduction even be achievable?

Initial Pilot Project

Hydro-Québec undertook a small-scale pilot project to validate its distribution network automation approach of using the Cybectec SMP 4 Gateway to link the remote-control equipment and the control center. The objectives of the pilot project were twofold:

- Remotely operate control equipment for the 14 overhead line switches and 2 circuit breakers already on the distribution network.
- Install a dial-up telecommunication network.

After a period of nine months, an improvement of one (1) hour in service reliability (22%) was measured on the remote control feeders of the pilot project.

Project Goals

Based on the results obtained during the initial pilot project, Hydro-Québec

established specific short-term goals for the automation program:

- Reduce the ratio of customers with a reliability index above 4 hours from 15% (500,000 customers) to 8% (266,000 customers).
- Reduce SAIDI by a yearly average of 15 minutes per customer.
- Reduce labor costs significantly.
- Reduce customer claims by about \$300,000.

The automation program is based on the remote control of 3750 load break switches and breakers on 1100 feeders, over a 6-year implementation schedule.

While in the short term Hydro-Québec aims for a reliability gain, the utility also has longer-term goals. These are to evolve toward dynamic system management, followed by migrating from program-based maintenance to targeted maintenance, and then ultimately to predictive maintenance.

No Challenge Too Great

Planning a project of this magnitude was a challenge in itself. The first equipment installations took place in 2006, and the schedule stretched out 6 years to complete the installation at a rate of approximately 900 cabinets a year.

Communications would be critical to the project's success. With a territory nearing one million square miles (three times the size of the state of California), Hydro-Québec depends on reliable access to its remote devices to control and receive data in a timely fashion. Without a reliable communications infrastructure, the project would be ineffectual.

Hydro-Québec turned to Cybectec's development teams for the solution: The Cybectec SMP 4 intelligent

gateway was determined to be the device of choice to provide communication and remote-control capabilities, as well as protocol conversion and data concentration. It became the control center's single point of access to pole-top equipment.

Once the data is successfully extracted from the devices, the next challenge is to integrate this high quantity of data points within the system and control center levels. On average, each cabinet generates more than 100 binary and over 20 analog inputs, bringing the total data points for the entire system to over 450,000.

The solution to reading and integrating this massive amount of information was using Cybectec's Enterprise Gateways as a front-end processor. Since splitting up the information made the data more manageable, the Cybectec development team set up five regional control-center front-end systems to receive the information, each designed to handle a peak load of 250,000 data points. The front-end communication processors were designed to meet the following stringent specifications:

- Perform data acquisition, concentration and distribution from the 4,000 field SMP 4 gateways to the 5 regional control centers.
- Provide remote control of the switches and protection relays.
- Seamlessly handle the existing DNP3 protocol, as well as IEC870, IEC 61850, and Modbus protocols required for future installations.
- Provide North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) compliance.

- Provide support for redundancy and cluster architecture (fail over).
- Provide support for multiple communications links: modems, serial lines, cellular, TCP/IP.

The Unforeseen Challenge: The Human Factor

This project's span is unprecedented in Hydro-Québec's recent past: more than 2000 people are involved with the project, directly or indirectly. With the implementation phase underway, it is now subject to the human factor: from human resources and training needs to quality issues and installation challenges, Hydro-Québec has resolved to meet each of these head-on.

The first factor is human resources. With a project of this magnitude, personnel adjustments and training were required to ensure everyone would be comfortable using the new cabinets. Hydro-Québec undertook to work with its labor unions to resolve this issue in a way that would ensure cabinets would be installed at an acceptable rate, while the teams felt adequately staffed to complete the work.

The second human factor is equipment workmanship. Hydro-Québec and the cabinet manufacturer worked closely to ensure any unforeseen issues were quickly resolved.

The third human factor is environmental. The cabinets, designed to be accessible without a ladder, were installed four feet above the ground. In certain cities where sidewalk space is minimal, municipalities have asked for a different installation approach by Hydro-Québec. Hydro-Québec is currently negotiating with the municipal authorities and its engineering teams must now find a solution to be as unobtrusive as possible to pedestrian traffic, while still being able to operate the equipment without climbing up the pole.

These unforeseen issues have had an effect on the rate of installed cabinets in the network. Only a part of the planned installations were performed in 2006 (140 instead of the planned 400). However, now that these issues have been resolved, Hydro-Québec is confident that installations will reach the planned 700 cabinets per year in 2008 and the planned 1000 per year in 2009.

The Rewards of Innovation: Being at the Forefront of the Industry

While the technological side of the project was planned in detail, today we realize that those technical issues were easy to handle and foresee compared to the sheer number of people involved. The impact of the human factor on a project should never be underestimated.

From a technology point of view, the integration of great amounts of data and their associated hardware and software, both in the field and at the enterprise level, has been a great success to date and a wonderful opportunity for the Cybectec development team and Hydro-Québec to deploy a very innovative and replicable system to take us into the future. ■

Modern and Secure Networks

In recent years, many utilities have started using WAN technologies with the goal of upgrading their communications infrastructure and providing an improved data path between the substation and the enterprise. Modern communications technology between the substation and the enterprise provides utilities with numerous benefits:

- SCADA can now benefit from the additional operational data being produced by modern protective relays and the numerous IEDs being installed.
- Additional control center functions such as Demand Management Systems (DMS), Energy Management Systems (EMS) and Outage Management Systems (OMS) can now directly access data produced by substation devices.
- Engineering and maintenance groups can now remotely access substation devices to retrieve

equipment monitoring data or modify device settings.

Prior to September 11th, 2001, security was not as heightened as it is now. The concern for security was further increased with the August 2003 blackout. While it was not caused by a security incident, it provided a vivid demonstration of the vulnerability of the power grid and prompted regulatory bodies to tighten utilities' wiggle room when it comes to protecting their networks.

The traditional SCADA system has always been considered secure because it used proprietary technology and communicated using dedicated telephone lines. With the growing use of standard IT technology in the process network, the "security by obscurity" approach can no longer be considered valid.

The North American Energy Reliability Corporation (NERC) reacted to the growing vulnerability of control systems by setting the Critical Infrastructure Protection (CIP) standards. Utilities must now (Q2 2007) begin the work required to comply with these standards, and be auditably compliant by Q2 2010.

NERC CIP Requirements

A complete description of the NERC CIP requirements is beyond the scope of this article. However, these requirements can be summed up quite easily:

- Utilities must identify all critical assets—control centers, transmission substations, generation resources, systems and facilities critical to system restoration, and load-shedding systems capable of shedding 300 MW or more.

Continued on page 7.



Set-up of the Multi-Stress Test developed by Cooper Power Systems to quantify long-term performance of connectors.



Connectors after testing.

the new short tees after completion of the test are shown above.

Shanghai has adopted the quality system and procedures that are in use at the United States and Taiwan factories. The involvement of the older factories includes transfer of procedures and methods, training of the Shanghai personnel, and ongoing auditing and continuous improvement initiatives. The Shanghai facility is certified to ISO 9001:2000 quality management system.

Quality and Consistency

The Cooper Shanghai factory is a world-class addition to Cooper's global manufacturing base for medium-voltage screened separable connectors. It shares Cooper's 35 years of experience in manufacturing separable connectors, utilizing the same product designs, manufacturing methods and procedures, the same QA/QC procedures, the same high quality EPDM materials, and, most importantly, the same focus on customer satisfaction. ■

Modern and Secure Networks from page 4.

- Utilities must identify critical cyber assets. Critical assets that communicate using a routable protocol or a dial-up modem are considered to be critical cyber assets.
- All personnel that can operate critical cyber assets need to be security screened.
- All critical cyber assets must be enclosed within a secure physical perimeter.
- All critical cyber assets must be enclosed within a secure "electronic perimeter" that limits access to authorized users only, blocks all unnecessary ports and services, and provides complete logging and monitoring services.
- No unauthorized user can access substation equipment, in person or electronically. More than that, utilities must be able to restrict access to previously authorized users quickly and efficiently.

Utilities must now also document:

- Who has access to which equipment.
- Whenever equipment such as an IED is accessed: a log must be kept of who connected to it, what commands were sent or changes were made to the equipment, and when the event happened.

NERC CIP applies to all utilities that possess critical assets. Even if they do not, they still need to provide an inventory of all their assets and demonstrate that none are critical cyber assets.

For more information on NERC CIP standards, visit NERC's web site at www.nerc.com.

Cybertec Products are NERC CIP-Compliant

Unlike other solution providers, Cybertec does not rely on third-party products and solutions to provide a complete, NERC CIP-compliant enterprise and substation security solution.

Cybertec's security solution is twofold: substation and enterprise. Cybertec Enterprise Solutions modules (Cybertec Security Server, IED Manager and Passthrough Manager) are installed at the corporate level and the Cybertec SMP Gateways are installed at the substation level.

At the enterprise level, Cybertec Enterprise Solutions is a suite of modules that perform centralized security, event reporting, user and IED management, as well as secure access to remote devices by users within the corporate LAN. Cybertec's Passthrough Manager supports SEL 20xx gateways, direct IED connections and the Cybertec SMP Gateways.

At the substation level, Cybertec's SMP Gateway product line provides NERC CIP-compliant, secure, single-access-point to substation equipment and data. SMP Gateways feature secure access and logging capabilities locally. They can also connect to Cybertec Enterprise Solutions for centralized security, enhanced logging and reporting.

All Cybertec products are compliant with applicable NERC-CIP standards. For a detailed list of Cybertec Solutions for NERC CIP standards, visit www.cooperpower.com/nerc and link to "Meeting NERC Requirements with Cybertec Solutions."