21, rue d'Artois, F-75008 PARIS
http : //www.cigre.org

CIGRE US National Committee
2015 Grid of the Future Symposium

Standards Are Not Enough! Challenges of 61850 Interoperability

A. ESHPETER
SUBNET Solutions Inc.
Canada

SUMMARY

Open standards offer the promise of freeing users from the strings of proprietary technology and dependence on a single vendor. IEC 61850, above all, champions interoperability like no other, but continues to see issues in practical deployment. While the 61850 approach to integrated control and monitoring is philosophically good, real world projects continue to highlight the fact that seamless multi-vendor 61850 interoperability is still a work in progress.

Further, control and automation standards such as IEC 61850 remain focused on SCADA communications and configuration, leaving them far behind the rapidly advancing and increasingly important technology providing non-operational data access and remote substation and device management.

A recent project with Cross Texas Transmission (CTT) in the USA highlighted the challenges faced by users seeking true multi-vendor interoperability. These challenges can be summarized into three points:

1. Despite its maturity, IEC 61850 is not pervasive enough for a compatible option to be found for all applications.
2. Non-operational data has presented virgin ground for vendors to re-introduce proprietary solutions.
3. The standards do not guarantee consistency in experience, resulting in protracted integration efforts that are difficult to troubleshoot.

This paper also discusses the challenges of implementing a unified approach to non-SCADA management that doesn't require a utility to be locked into a single vendor solution, regardless of standards based SCADA compatibility. Secure multi-vendor password management, automated fault file collection, configuration management, historical data archiving and remote engineering access can be a reality.

The key to harmonization of utility standards lies in international standards adoption and alignment with solution providers who are truly committed to interoperability as much as the utilities.

anthony.eshpeter@subnet.com

KEYWORDS

Substation-Automation, SCADA, IEC-61850, Multi-Vendor, Interoperability.

Resolving the Challenges of Multi-Vendor 61850 Implementations

The 61850 Promise of Interoperability

The IEC 61850 standard is gaining wide spread adoption around the world in large part due to three benefits:

1. Replacement of hard-wired, point-to-point connections with shared Ethernet connections
2. The promise of plug and play interoperability across vendors
3. A common configuration language designed to simplify the substation configuration process

These three promises of the 61850 standard provide tangible value to utilities under growing pressure to get more done with fewer people. As the 61850 standard continues to mature we are seeing growing value in all three of these areas.

Substation LANs already reduce the amount of point-to-point wiring used for interlocking by replacing it with deterministic, high speed GOOSE messaging. The 61850 process bus standard promises to further reduce hard wired I/O with a high speed LAN for sampled measured values that can be accessed directly by any connected device. Any reduction in field wiring and the resultant savings in copper, troubleshooting and maintenance costs has long been a key driver for automation system purchasing decisions.

Utilities have been fighting for plug and play interoperability between vendors for decades. One of the biggest challenges for substation protection and automation teams has always been finding system solutions that don't lock the utility into a single vendor solution for all of the parts for years or even decades. The adoption of open communication protocol standards like DNP 3.0 and MMS has been a huge step forward in this area, but vendor lock-in continues to be a problem for utilities. Device vendors continue to find ways to use technology to specifically block their competitors from offering viable, interoperable solutions without a wholesale rip out and replace mentality.

A key part of the vendor compatibility puzzle is the definition of a common configuration settings language. The 61850 standard addresses this with SCL, and again it is a significant step forward for the industry. The ability to define the external interface to a device in a universally understood way is a critical component of the plug and play vision. This vision opens the door to further automation of the configuration process itself which can drastically reduce human error and the time it takes to configure a substation automation system.

The Missing Pieces

As much as the 61850 standard has helped drive productivity improvements, there are still some critical, real-world use cases that fall outside the current scope of 61580, but tie directly to the configuration and maintenance of substation protection and automation systems.

Even though SCADA protocol interfaces have become far more standard in recent years, the interfaces required to access non-operational data continue to diverge and remain very vendor specific. The amount of non-operational data required by teams who did not traditionally have access to information from substation devices is growing. The data available inside field devices that is useful to a variety of teams is growing to meet that demand. Post fault analysis, predictive maintenance, construction planning, and outage management are just a few of the teams looking for access to data not available from the SCADA master, but sitting inside various field devices at the substation. At the same time the

EMS and DMS masters are turning out not to be the most effective way to access and manage that data. An independent secure communication channel into the substation is turning out to be the answer to this problem.

The integration of non-61850 devices into the substation automation system is another area often overlooked in 61850 implementations. Although this is traditionally a problem in substation expansion projects, even new construction projects often encounter non-61850 devices that need to be integrated into the system. Vendors often recommend the replacement of those devices, but in the real world it is easier said than done and the odd Modbus and DNP device is still required for certain things. There needs to be a way to integrate these devices into 61850 systems without throwing out the advantages of a 61850 architecture.

One other missing piece that must be considered in 61850 system designs is how to move non-operational data outside the substation fence. Substation HMIs and data repositories are a start, but full data access from remote locations is fast becoming a must-have requirement of substation automation systems, regardless of whether or not that data is deemed worthy of mapping through by the EMS and DMS teams.

A Real World Example: Cross Texas Transmission Project

Cross Texas Transmission, CTT, is a relatively new utility established with the mandate of supporting the integration of distributed renewable energy to the grid. Their primary focus is on integrating wind farms into the transmission system. As a new utility building new substations CTT prefers to use new technologies and remain open to innovative ideas.

Among their first projects was a new 345 kV transmission switching station located in the Texas panhandle. The project scope was to tie into existing transmission lines and then tie in the first wind farm.

CTT specifically selected a contractor that was not tied to any specific device or equipment vendors. The reasoning was that vendor independence would provide the most innovation and allow them to look for the best in class solution for each project and challenge they encountered. This contractor then selected a remote device management solution from a company with a core business objective of integrating and supporting remote device management solutions for multiple vendors' protection and automation equipment.

CTT had four high level requirements for this project: consideration for remote stations, interconnection with other utilities using various vendors' relays, self-monitoring summary views for the operators, and easy expansion for additional wind farms.

CTT has several remote substations between 80 and 100 miles from their headquarters in Amarillo. This means driving to site for anything is time consuming and inefficient. To reduce this they required a system that would enable the use of remote HMIs for station monitoring over a secured Ethernet network.

CTT knows they will be interconnecting with other utilities that use protection relays and automation equipment from various different vendors. They also recognize that they have very little control over what equipment the other utilities select so they needed to have a system specifically designed for use in a multi-vendor environment, particularly with regard to data security and exchange. A 61850 foundation was selected to support this along with the knowledge that some non-61850 device coordination would likely be required.

The need for self-monitoring, summary views and data aggregation for the operators was driven by the fact that CTT has a very lean operations staff. Lean staffing levels meant that they needed to have easy

to use solutions for remote monitoring and control. These systems also needed to have intuitive user interface designs that don't require excessive training.

The final requirement of easy expansion is to support the planned integration of more wind farms in the future. The first phase of the project included forty six 61850 IEDs and was designed with room for additional tie-ins. The final system is expected to have more than 100 IEDs.

The contractor considered several possible alternatives and selected their vendor partners based on their alignment with the project goals. The remote device management system was selected based on advantages identified in the areas of ease of implementation, intuitive workflow, fast/easy HMI screen creation, extensive protocol library support, 61850 support and competitive pricing. Also considered was the business ability to understand the T&D utility space and provide assistance beyond the superficial.

The Deployed Control System Architecture

The final substation control system architecture was built around a dual redundant 61850 LAN using fibre and a total of 4 switches. Differential line protection relays, bus differential relays, and reactor relays are all located inside the control building.

Inexpensive programmable automation controllers with on-board I/O are located in the breaker and reactor cabinets to perform trip and close operations based on GOOSE messages. This approach of putting I/O in the switch cabinets greatly reduces the required wiring for alarms, breaker status, control outputs, etc. and simplifies future expansion.

The relays located in the control house do the majority of the logic and leverage the I/O on the programmable automation controls to provide the field I/O wherever it is needed. The control house relays were specifically chosen to be a mix of relays from two different vendors to provide vendor diversity and avoid being tied to any single source solution.

Since the remote utilities that CTT connects to also have different, and independent stipulations on what relays they use this multi-vendor approach is seen as being a key design decision that will make future interconnections easier.

For the substation gateway redundant servers were deployed in a warm standby primary and backup configuration. These gateways control all remote access to the station to secure the DMZ.

61850 Was Not Enough

This project used both GOOSE and MMS communications on the substation LAN. Process bus is also of interest but was not used in this project.

GOOSE was used to send control signals from the control house relays, where most of the automation logic resides, to the programmable automation controllers in the switch cabinets. This approach replaced a lot of copper wire and made it easier for the field technicians to troubleshoot wiring problems.

MMS was used as the primary substation communication protocol, but as the project moved forward other communication protocols were also required including DNP, Modbus and some proprietary fault file collection mechanisms.

Modbus was required to integrate a controller for a diesel generator controller used to power a repeater station. This controller did not have a 61850 MMS option available and the ability to integrate non-61850 devices into the system was very valuable.

An automated event file collection system was used to extract fault files and event files from various relays using the maintenance ports. Using the maintenance ports for this activity ensures that SCADA is never interrupted by a file transfer and allowed for collection of some types of event files that are not available over the SCADA connection. These event files are currently available to remote users over a remote desktop (RDP) connection. There are future plans to automate moving these from the substation server to a central server collecting event files from all stations.

Even though 61850 provides a solid foundation, the reality is that not every device we needed fully supports 61850, or made all the data we wanted fully available over MMS so the ability to still use other protocols turned out to be very practical.

Multi-Vendor Interoperability

Although the SEL and GE relays selected for this project are both compliant with IEC 61850, the true depth of this compliance is put to the test when attempting to get the devices to exchange GOOSE messages with each other. IEC 61850 has not provided any mandate on how vendors choose to implement their support, allowing for differences that make configuring GOOSE exchange between devices from the same vendor very easy, and between vendors quite difficult. Some specific examples include:

1. One vendor expresses addresses in hexadecimal, the other in decimal, allowing for many mistakes when manual data entry is required;
2. CID and SCD files from different vendors, despite the standard's goal of interoperability, often generate errors and/or warnings when imported due to differences in interpretation, or in the selection of optional content to include or exclude, or in the vendor tool's tolerance to the presence of private data;
3. Relating changes in point mapping from one relay to another typically requires time-consuming exporting and importing of data between vendor tools in order to achieve the remapping.

The burden of troubleshooting errors in interoperability is most often borne by the integrator, not the equipment vendors. Vendors commonly imply or outright declare that any error in interoperability is the other vendor's problem. The result is that the integrator is largely alone when diagnosing the root source of the problem, expending more time proving to a vendor that their product is the root cause before any time can be spent on resolving the problem.

One of the biggest aids in diagnosing interoperability issues was the inclusion of an HMI on the gateway. This tool allowed the integrators to build screens to monitor communications health, which in turn helped pinpoint the source of many issues. This substation HMI was so useful in in diagnosing communication problems, it likely paid for itself in the commissioning time saved when diagnosing problems.

The multi-vendor interoperability design of the station with a gateway from an independent vendor was a tremendous boon for troubleshooting. It aided technicians during commissioning to highlight and diagnose problems. It helped identify that the right relays were plugged into the right ports. It reported how the system was connected at any time and what parts were working at the moment.

This same tool is also very helpful with preventative maintenance. It provided a way to create custom alarms that go beyond equipment status to areas such as control state alarms, relays left in local or test mode, communication failures, clock status, and network status (e.g. was primary fibre link not working for some reason).

Secure Remote Access

The substation server and local HMI were primarily used in the CTT transmission station project for commissioning and troubleshooting, but can also be accessed over RDP for remote access to the station. Moving forward there are plans to expand this system to automatically transfer fault files from the station to a central repository, making it even easier for the Engineering team to get to the work of post fault analysis rather than spending their time collecting event files manually from the impacted stations. The CTT team has recognized that a true remote device management system requires the integration of a centralized system into the substation gateway network. The gateways alone are not enough.

Lessons Learned During the Project

At the end of the day the project team learned some very valuable lessons:

- 61850 multi-vendor interoperability is achievable, but it is not seamless
- A vendor agnostic server and HMI are very helpful in diagnosing where problems are originating
- In 61850 stations, a vendor agnostic server and HMI can pay for itself in just commissioning time saved
- 61850 is not yet the answer to every problem. A gateway that integrates in other protocols as well is very valuable and can save the project

Beyond the CTT Example

In our example project CTT was able to successfully address several challenges within the 61850 framework by employing vendor agnostic solutions for:

- Easy multi-vendor interoperability
- The need for self-monitoring, summary views of multiple vendors' equipment
- Secure remote engineering access for data not available over MMS
- Easy expansion
- Fault file management

In addition to these challenges, some other common requirements have been highlighted by the North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) standards. Adherence to these standards is now being mandated in North America for substations classified as critical infrastructure:

- Password Change Management (CIP-005[1], CIP-007[2])
- Configuration Management (CIP-010[3])

The NERC CIP standard is being referenced world-wide as a best practice set of requirements.

Password Management

Password management ties into every aspect of secure remote access outside the substation DMZ. The ability to access a device maintenance port, to push or pull a configuration, and to access system logs, all require the use of one or more passwords. Just as importantly, the ability to provide audit trails on who is doing these things requires passwords to be kept secret until they are required and a system for tracking who knows the passwords at any given time.

These password management requirements mean that a password management system must be an integrated part of your total remote device management solution.

Configuration Management

Configuration management is highlighted by the NERC CIP standards to be of critical importance to the safe and secure operation of utility automation systems. While 61850 defines some of the mechanisms to handle this there can be more to it than first meets the eye.

The main configuration management functions include configuration uploads, version control, permission policies, approval processes, and change notifications. While these features are critical they only touch the surface of what can be done.

Other configuration management possibilities include considering all device configurations as one holistic substation configuration, providing comparisons and differences between different configuration files, ensuring compatibility with non-61850 devices, considering IT devices as part of the system (routers, switches, and radios), synchronization between the corporate environment and the substation, active monitoring of device configurations in the substation and automatically extracting changed configurations from devices. 61850 concepts can, and are, being applied and extended to accomplish all of these things.

Conclusion

The IEC 61850 standard is a huge step forward for utilities. It brings us all one step closer to the vision of interoperability. What is clear is that we still have a long ways to go. The 61850 standard is not enough.

A single point of access for non-operational data interfaces, the integration of non-61850 devices into working systems, and secure mechanisms for moving non-operational data outside the substation fence are all point not fully addressed by the 61850 standard.

Many device vendors have partial solutions to these issues, but the best solutions seem to be coming from truly device agnostic suppliers who get a bigger business benefit from providing true interoperability and vendor equality then they do from leveraging vendor lock-in strategies.

BIBLIOGRAPHY

[1] CIP-005-5, “Cyber Security – Electronic Security Perimeter(s)” (North American Electric Reliability Corporation)

[2] CIP-007-5, “Cyber Security – Systems Security Management” (North American Electric Reliability Corporation)

[3] CIP-010-1, “Cyber Security – Configuration Change Management and Vulnerability Assessments” (North American Electric Reliability Corporation)