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

CIGRE US National Committee
2016 Grid of the Future Symposium

Intelligent Electronic Device Gateway Case Study

A. SALVADOR, C. CARNEGIE
SUBNET Solutions Inc.
Canada

SUMMARY

A utility was dealing with the problem of trying to manage all of the distribution automation devices they have on their network. There were too many devices to manage manually, and access to device event data was non-existent or difficult which prevented the ability to perform root-cause analysis of circuit reliability. There were security and worker safety risks in managing the device passwords, settings, and configuration changes. Because of this, the utility executed a project to develop a solution that overcame these challenges. This solution focused on:

1. Efficient access and management of device settings
2. Traceable settings configuration and device operation
3. Open access to data for analytics
4. Centralized access for equipment information security
5. Centralized password management
6. Centralized access & management for commissioning devices
7. Logging of activities on the equipment/devices
8. Support NERC/CIP compliance
9. Manage the configuration and firmware upgrades with versioned configuration file control

This paper summarizes the lifecycle of this project, including a description of the problems and challenges the utility faced during the implementation to meet their unique challenges, while keeping in mind their expansion plans over the next few years.

KEYWORDS

Legacy Devices, Multi-Vendor, Interoperability, Device Management, Integration

chi.carnegie@subnet.com

Project Goals

The utility’s main goal is to meet NERC CIP standard by implementing an IED management system that securely allows personnel to access remote devices, manage its passwords, obtain configuration files and retrieve event files without physically accessing these devices. By allowing personnel to remotely manage the devices, the utility expects to save labor cost, equipment maintenance cost, and increase safety and reliability within its system.

Background

The utility’s generation plants consist of 41 dam sites, 30 hydro facilities, and 9 thermal sites. They have approximately 18,000 kilometers of transmission lines, 260 substations and 56,000 kilometers of distribution lines. The utility is providing electricity to approximately 1.8 million customers in the region.

Due to the utility’s size and coverage area, approaching a solution to manage all their remote devices, which is estimated to be around 10,000 devices, is not a simple task. The utility is not only faced with a quantity problem but also terrain issues. Due to the mountain range nearby, certain substations and devices are difficult to communicate with due to a complex communication infrastructure as well as the possibility of bad weather. Depending on the location of the devices, bandwidth can be a scarce commodity and only operational data is collected over the communication lines. To obtain important non-operational data such as event files and configuration files, personnel are forced to physically access these remote devices, which introduces expensive labor cost and safety issues due to the terrain. Since non-operational data was so difficult to collect, analysis of the data is intermittent and fails to produce a clear picture of the system for data trending and predictive maintenance.

Another problem the utility faces is the vast number of brands of devices that are implemented in the field. Each vendor provides devices that use a different protocol or protocol variant and, most of the time, a proprietary configuration software application that must be learned by the utility’s personnel that are collecting the data. The utility sought out for a single solution that will be able to manage devices from multiple vendors and proprietary protocols. Within the utility industry, there are many central management solutions but most of the vendor for these solutions also provide protection devices. Therefore, the central management solution may only support their own devices and support for other vendor devices are either non-existent or limited.

Solution Design

To reduce labor cost and increase safety, the utility focused on providing their distribution engineers a solution for managing IEDs on their distribution network. The project scope included reclosers, voltage regulators, switchgear relays and capacitor bank controllers and allowed for future expansion to substation and transmission equipment. The solution was required to be device/vendor agnostic with the ability to secure access to, and manage non-operational data of these IEDs remotely. Due to the unforgiving terrain of the utility’s distribution network, the solution needed to be robust enough to handle low performance communications such as satellite and cellular connected IEDs. As well, the solution would allow them to become NERC CIP compliant.

The utility selected a software integration company as the contractor to drive this project to completion. Together, they designed a central IED management solution to overcome these challenges. Unlike other existing solutions, the platform is vendor agnostic, provides a means for remotely maintaining non-operational IED data, and is scalable for future expansion. It supports remote connection to IEDs regardless of the communication protocol or connection media that is utilized by the devices. This remote connectivity provides users with the ability to configure and/or retrieve data, as if the user is directly connected to the device. Most importantly, it provides them a secure method of accessing the remote IEDs for various management tasks. Furthermore, the system is designed to significantly aid the utility for compliance with guidelines, standards, and policies for critical cyber assets as outlined within NERC CIP requirements.

The solution is installed in the corporate local area network (LAN) and natively integrated with the utility's active directory. The system is isolated in a demilitarized zone (DMZ) utilizing firewalls with strict access rules. An example of the rules on the firewall between Corporate LAN and the DMZ include ports required to access the system with Microsoft Remote Desktop client, authenticate with the Microsoft Active Directory and send outbound email notifications. The firewall between DMZ and remote device network is configured to only allow access to the distribution IEDs intended to be managed by the solution.

The solution is modular, allowing the utility to pick and choose which modules were relevant to their system. The modules available and implemented by the utility were for remote engineering access, password management, configuration management and event file management.

The Remote engineering access module allows personnel at the utility to remotely access the field device securely from the centralized system. The module only displays the devices that the user has permission to access, and other devices are completely hidden and are inaccessible to the user. The system is configured with pre-approved vendor applications and is linked to the proper field devices. The user has the option of what pre-approved applications they want to use to connect to each device. Once connected to the field device, the system monitors the user's activity such as commands sent and/or mouse clicks used within the system. If the user sends an un-approved command or clicked on un-approved item, the system intercepts the action and prevents the command or action being sent to the field device. All remote connections made by the user to field devices are logged and auditable for NERC CIP or for internal purposes.

The Password management module allows the system to manage the field devices' passwords. Passwords are encrypted and centrally stored within the system. The system automatically accesses the device and changes its passwords based on utility's preference; for example, at a configurable interval, such as once a year, or when an employee uses a password and no longer needs the current password. The Password management module assists the utility's compliance with NERC CIP where it requires that field devices have their passwords changed to its highest complexity every 15 months. Making password changes on all field devices manually can be tedious and very expensive for the utility.

The Configuration management module allows the system to automatically retrieve configuration files from field devices. It compares any new incoming configuration file against a previous configuration file that was retrieved from the same device. If the module detects any differences, it can initiate work flow events that can alert specific personnel allowing them to examine the new configuration file, and determine if new changes should be approved or denied. The new configuration file can stay in the device or the old configuration file can be pushed down to the device if the changes were rejected. All versions of the configuration file are centrally stored, archived and are accessible to utility's personnel.

The Event file management module allows the system to automatically retrieve new event files from field devices. When a new event file comes into the system, the module can alert subscribed personnel via email. Personnel can then analyze the new event file and determine the importance of the event. All event files are centrally stored and archived within the system where personnel can access multiple files and analyze them for predictive maintenance on the field device or its corresponding equipment.

In addition to the modules that the IED Management system provides, new software features and enhancements are required to meet all of the project requirements. One of the key concepts used to tackle the design of these new features is the process of Agile Development. This iterative approach to the software development process introduced two important benefits to the project, evaluation and transparency.

Many times, high level requirements defined in a project's scope of work are not enough to fully understand the expected function or use case. To reduce wasted time and money, the requirements are discussed and defined in detail with the utility. After development of a function is complete, the utility is given the opportunity to evaluate it. Going through this iterative process several times throughout the project provides transparency, demonstrates progress, and confirms the solution for the utility. The Agile approach is a win-win scenario for both the utility and the integration company. The utility receives the functionalities they are looking for and the integration company increased its product's functionalities and capabilities for other utilities to take advantage of.

In addition to the benefits of the agile approach mentioned above, the process helps drive innovation for advancements in vendor agnostic solutions, specifically, advancements in the ability to manage and interoperate with closed and proprietary IEDs. A key requirement for the utility is to automate time consuming and inefficient tasks for their distribution teams. Tasks such as collecting and organizing IED event data, collecting and looking for out of band IED configuration changes, and changing IED passwords. For some IEDs, these tasks can easily be automated if they support open standard protocols such as Modbus, SEL ASCII, and telnet. The utility requires automation of these tasks for the several devices such as the SEL 751 and Eaton Form 6. The SEL 751 provides well-documented, open standard protocols and is easily automated in the system through a protocol driver. This type of driver automates tasks to the end device using the native communication protocol. However, it was clear in the initial investigations that the Eaton Form 6 was a closed system, and did not support open standard protocols. Analysis of the communication protocol showed messages were encrypted or hashed. Users are forced to manually manage these IEDs with vendor-specific software.

Lacking the ability to communicate with the Form 6 device using an open standard, the concept of an Application Driver in the IED management system was developed during the project. This type of driver is based on a software wrapper developed to remotely drive a vendor application to communicate with an IED. It provides the ability to automatically mimic the mouse clicks, keyboard entries, and file saves normally performed by a human. Working with the utility's distribution teams, several workflows were created for all the mouse clicks and keyboard entries for communicating with the Eaton Form 6 using the ProView application. These workflows were turned into Jobs within the system. These Jobs can be issued to a specific device on demand by an authorized user or scheduled on a recurring basis by the system. The jobs are generalized to be vendor agnostic providing users with a standard mechanism for interacting with all devices being managed by the system. Jobs such as change password, get fault files, get configuration, get SOE, and get data profiler can be issued against an Eaton or SEL device. Jobs can also be disabled by users in the event that a device is physically being worked on in the field. It is also the responsibility of the system to determine if the device required using an Application Driver or a Protocol Driver to complete the job. The jobs would also only upload new information from an IED by comparing it to the last known configuration, last collected fault file, or last retrieved SOE. This comparison becomes invaluable when configured on a scheduled basis, as the system can then watch for out-of-bounds configuration changes or event fault data for post-event analysis.

Further, the Application Driver can permanently hide or restrict access to menus, buttons, and/or dialogs within the vendor application. This concept is incorporated in the remote engineering access module to improve security and reduce human error. In the case of the Eaton ProView software, a user is required to log into the application first, followed by also logging into the end device. By utilizing the Application Driver capabilities, a workflow was developed to automatically log into the application and device, without any user interaction or knowledge of the passwords. Following this workflow, the user is then given control of the application to remotely communicate with the IED. Extending this concept to security, depending on the user's authorized permissions, certain menus and buttons in the application like Trip or Close can be disabled throughout the remote engineering access session with the user. This is important to the utility, as the ProView software provides these buttons to the user, no matter what device access level or application role was used to connect to the device.

The concept of logging is also an important requirement for the utility. The goal was for the system to provide situational awareness. In terms of individual devices, the concept of device state was created to allow users to immediately understand if a device was normal, disabled, tagged or decommissioned when users navigated to devices in the system. All jobs issued, either by a user or the system, are also displayed and logged for the device. The jobs contain state information indicating if the job completed successfully or if it failed for a specific reason. Furthermore, all IED specific documents that are managed by the solution, such as configuration files, point mappings, drawings, stencils, etc. are versioned controlled. The version history for each file indicates the modified date, modified user and comments associated with the version. It also allowed users to retrieve previous versions for recovery situations. In addition, configuration files are integrated in document workflow approval processes. For all files in the "Working" library, users are required to exclusively check out the file before they are allowed to edit them in the system. When a user checks out a file, the system indicates which user is working on the file. When a user checks in a file and attempts to approve it to a major revision, other users with authorized approval permissions are notified by email of the new configuration. Only the users with the approval permissions can approve or reject the file after verifying the changes.

Once the entire solution was developed, the utility upgraded their lab system and perform user's acceptance test against the system. Lab system was designed to simulate similar environment as the field remote devices; for example, low bandwidth and same device model and firmware. Once the acceptance test was completed and utility was pleased with the results, a production system was set up to remotely manage the multi-vendor field devices. To add field devices to the system, the implementation was done in stages. First the utility added about 50 devices, then 100, then 200 etc. Currently, the utility is managing over one thousand devices in various locations and terrains. For devices in low bandwidth environment, the system will only connect to the device once a week or at a higher period, to collect configuration files and fault files. The utility ensures that while the collection of configuration file and fault file is occurring, operational data was still being collected from the device and was not affected by the non-operational data retrieval. Once configuration file and fault file are retrieved, the solution performs a comparison and any changes to these, proper personnel will be notified and will perform analyses on the changes. As with any other solution, the utility is continuously providing feedback and updates are provided to the utility to test on their lab system and then implemented on production.

Conclusion

As experienced in this case study, it is not uncommon for hardware vendors to implement proprietary protocols within their devices and their software application hoping the utility will keep using the same vendor's hardware because they do not want to go through another process of learning another vendor's protocol or application. Implementation of proprietary protocol encourages the utility to implement a single-vendor system instead of implementing the best equipment available on the market to do the job required regardless of its vendor. To implement a highly reliable and secure system, the utility needs to encourage multi-vendor systems. Multi-vendor systems will force vendors to move to open standard applications as well as force integration companies to develop true multi-vendor total device management solutions that will promote cost savings, personnel safety and system reliability.