

Remote online management for protection and automation

Dennis K. Holstein
on behalf of CIGRE B5.09 Working Group

Abstract

CIGRE Study Committee B5 commissioned a study to explore the use of Information Technology (IT) application for remote online management of substation protection and automation. Information technologies were to be considered as a general concept; intranet and internet technologies are subsets of IT. This paper, which summarizes the work of CIGRE B5.09, discusses the impact of remote on-line management for substation protection and automation on the operation of equipment to reliably deliver electricity for distribution. Discussed are not individual functions of modern intelligent electronic devices (IEDs) but the overall aspects of how to use information technology to remotely manage the protection and automation functions. It applies for new substations as well as for refurbishment of secondary equipment in existing substations. Examples of core information technology used for secure remote online management of protection and automation are presented to highlight the operational advantages of the enabling technologies. It is our belief that remote online management will play a fundamental role in helping utilities to integrate the capabilities within a scaleable enterprise. It will also stimulate the research community toward greater advances in remote online management techniques and technologies – advantages that will arise from a growing ability to integrate a collection of protection and automation techniques and to use the community's collective capability to provide results of much higher quality.

Key words: Remote control and monitoring, Protection and automation schemes

Imagine a utility that can securely access and automatically mine the protection and automation data from any repository to find the evidence needed to characterize and correct a particular fault before it mushrooms out of control. Such a capability will dramatically lower the cost and time to take corrective action and maintain reliable power deliver services.

The capabilities are now emerging from the research laboratories and being deployed by forward thinking utilities to address a multitude of operational opportunities. As the technologies for remote online management mature, new solutions that merge the value of controlled access and use of protection and automation data will become ubiquitous.

In this paper, examples of core information technology used for remote online management of protection and automation are presented to highlight the operational advantages of the enabling technologies. It is our belief that remote online management will play a fundamental role in helping utilities to integrate the capabilities within a scaleable enterprise. It will also stimulate the research community toward greater advances in remote online management techniques and technologies – advantages that will arise from a growing ability to integrate a collection of protection and automation techniques and to use the community's collective capability to provide results of much higher quality.

1 INTRODUCTION

The opportunity presented by remote online management for protection and automation is enormous, and we believe it will significantly change how utilities operate the electric power transmission and distribution systems over the next decade. Communication technologies offered by new standards such as IEC 61850, 61968 and 61970 will enable the management of their operations in a coordinated and integrated fashion through the use of secure access to all data. Protection and automation data all share the characteristic of being predominately structured; that is the context is mainly well defined by the configuration parameters and limits of measured data.

2 OUR MOST IMPORTANT DISCOVERIES

Although still a work in progress, members of CIGRE B5.09 discovered four issues that need further study by future CIGRE B5 working groups and by those standards making groups responsible for advanced automation schemes that rely on remote management of protection and control mechanisms to ensure the reliability of the electric transmission and distribution services.

2.1 *Version control of IEC 61850 settings*

Version control of device settings is absolutely required to ensure reliable operations of the network during pre-configuration, commissioning, and operation.

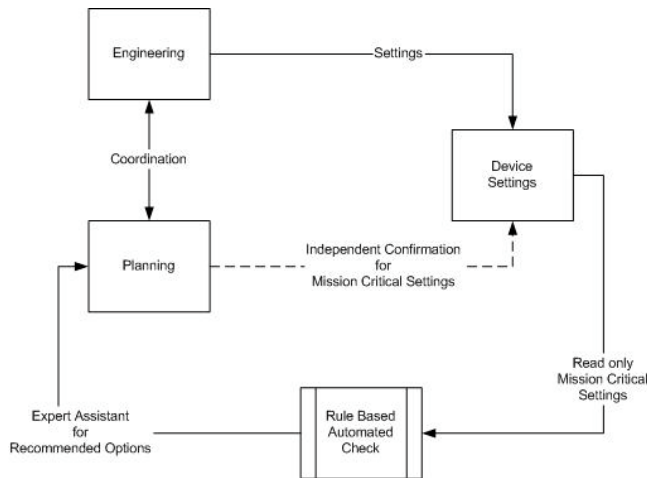
IEC 61850 is a new international standard designed to significantly enhance remote management of device settings over approaches offered by other communication protocols. An object like approach is used in 61850 to define “logical nodes” of a device containing the data objects that define the behavior of a specific device function. These logical nodes contain the device settings. One logical node, called LN0, contains the information about the device as a whole, such as nameplate. LN0 also contains the version of the device configuration.

Settings however, are contained in other logical nodes, LN_x, where x=1, N; and, herein lays the problem. If the settings in LN1 are changed, those LN1 settings need to have new version control number. Settings in other LN_s have not changed and their version control number should not change. But the only place to store the version control number is in LN0, which applies to all LN_s of the device.

Device vendors can write extensions to each LN to provide the needed version control of settings, but because this is not part of the standard, interoperability will be problematical. CIGRE B5.09 suggests that the IEC TC57 working groups responsible for 61850 data objects consider a common approach to version control of settings that can be standardized for all implementations.

2.2 Improving the bridge between coordination studies and remote management

An advanced concept to improve the bridge between coordination studies and remote management is illustrated in the figure below.



An advanced concept to improve coordination

It is common practice today to coordinate device settings between Engineering, who is responsible for the settings, and Planning, who is responsible for overall system safety, reliability and stability. Two conceptual improvements are highlighted in the figure. First, enabling read only privileges for mission critical settings by an automated remote online rule-based expert system can provide expert assistance of recommended options to Planning. Secondly, if settings are going to be changed, a two person enabling

rule can be implemented to securely provide independent coordination of mission critical settings.

Before leaving the subject of coordination, a brief summary describing why a “one person” approach is not a good idea and the vulnerability of automated tools needs to be addressed.

2.2.1 Why a one person approach is not a good idea

Depending on one person (for example, the protection engineer) for mission critical settings has two serious weaknesses. If the person with this responsibility makes an error, which frequently happens, and that error is not found through automatic checking, which also happens, then because the setting is mission critical, reliability is degraded – sometimes leading to blackout and damage to expensive equipment. Furthermore, from a security point-of-view, it is not a good idea to rely on one person for mission critical settings because utility surveys have shown that the “insider” threat is their number one concern.

2.2.2 Automated tools – another vulnerability

Depending on automated tools to “assist” is always a good idea; but the operative word is “assistance.” Settings are not real time, they need to be verified. Automated tool verification is one approach, but if the tool has a bug or is compromised from a security point-of-view, then mission critical settings are not reliably verified. CIGRE B5.09 concluded that tools should be used to assist an operator, not to replace the operator.

2.3 Information security for access and use control

Information security for access and use control is either non-existent or largely inadequate in most installations. This in the opinion of CIGRE B5.09 is a major concern because remote management for mission critical functions requires positive control of access to device communication ports and use of the functions and data once access has been granted. From an end-user perspective, CIGRE B5.09 concluded that the following security requirements need to be enforced:

1. Control access to selected devices, information or both to protect against unauthorized interrogation of the device or information.
2. Control use of selected devices, information or both to protect against unauthorized operation of the device or use of information.
3. Ensure the integrity of data on selected communication channels to protect against unauthorized changes.
4. Ensure the confidentiality of data on selected communication channels to protect against eavesdropping.
5. Restrict the flow of data on communication channels to protect against the publication of information to unauthorized sources.

6. Respond to security violations by notifying the proper authority, reporting needed forensic evidence of the violation, and automatically taking timely corrective action in mission critical or safety critical situations.

These security requirements are intentionally couched in language that do not imply a specific implementation, but do relate the requirement to the threat issue. The word “selectively” is used to enforce the idea that what is selected should come from the user’s risk assessment, and not imply how the user should perform the risk assessment and quantify its results.

With these requirements in hand, B5.09 informally surveyed the work in progress in several venues and concluded the following:

1. There is no overall systems approach to perform a systems analysis and develop a comprehensive model to address all these requirements. Most venues are focused on a specific aspect of the problem and are constrained by the scope of their parent study or standards making organization and constraints of their approved work item.
2. IEC 62351, a work-in-progress, will cover 61850, 60870-6 (also known as ICCP or TASE.2), 60870-5 and derivatives (DNP) and in the future 61970; but it addresses only requirements 1, 2 and 3. [6] [9]
3. IEEE C37.115-2003 recommends the use of security agents in response to requirements 1 and 2 only. [7]
4. AGA Report 12 (a series of reports), a work-in-progress has defined the general requirements to protect SCADA communications and dial-up access to the maintenance ports of field devices. AGA 12 is one of the most definitive specifications for cyber security; it does address all requirements except #5 in terms of SCADA communication channels and dial-up to the maintenance ports of field devices. [1]
5. ISA SP99 and IEC 61784-4, works-in-progress, are focused on all requirements except #6 in terms of process control systems for manufacturing. Although there are strong similarities between the requirements for Manufacturing and Control Systems and those for electric power transmission and distribution SCADA and protection systems, there are differences that must be addressed. [2][8]
6. ANSI X9.69, X9.73 and X9.96 provide the framework for key management extensions. Although focused on the financial industry, analysis for the development of AGA Report 12 has shown that this framework is applicable to key management in general and addresses requirements 1, 2, 3 and 4. Work is in progress to adopt these ANSI standards as ISO standards. [10][11][12]

The United States Department of Homeland Security has funded a new venue called the Process Control Security Forum to raise the awareness of requirements across all critical infrastructure domains. Within this forum there are

two particular groups that have the potential to address all the requirements listed above.

- The Congress of Chairs group provides a venue for all those working on cyber security standards or study projects to share their scope of work and to establish personal relationships to further enhance the recommendations of their work.
- The Systems Analysis and Modeling group provides a venue to examine, at high level, several comprehensive solutions for these requirements.

2.4 Common information modeling coupling for asset management

IEC 61968 [4] and 61970 [5] use a Common Information Model (called CIM) for specifying common interfaces to support application integration in terms of system interfaces for distribution management and for Energy Management System Application Program Interface (EMS-API) respectively. CIM data is populated and maintained by reading the values of IED parameters, and then used to perform a large number of the asset management tasks.

To cope with the complexity of the interrelated processes involving asset management, field maintenance, and engineering it is essential to keep track of which change is implemented, where it was implemented, by whom it was implemented, why and when it was released. As described earlier, version control implemented throughout the processes is the best approach track these changes.

CIGRE B5.09 concluded that to make version control useful it should be designed to facilitate the smallest data object that can be tracked in the devices. The reasons to manage these changes at this low level are identification of families of devices to be maintained, replaced, or upgraded, as well as to effectively manage spare parts.

Lastly, CIGRE B5.09 suggests that to efficiently manage the version control process one must address the strong coupling between capabilities provide by the intelligent electronic device (IED) manufacturer and the utility asset manager (person or tool).

The IED manufacturer provides the capability to identify and communicate at least the version of each domain (hardware, software, pre-configuration, configuration, and setting), facilitate the migration from one version to another, and to document and publish the changes and their reasons made at hardware or software in order to enable an asset management decision.

If the IED manufacturer has provided the capabilities, then the asset manager access this data on a timely basis can be used to keep descriptions of the network including topology, fault simulations, system protection scheme, etc. Furthermore, the asset manager now has timely data to evaluate system setting consistency through predefined rules, derived from coordination studies, between distributed IEDs in order to insure an overall protection scheme.

3 REMOTE DATA MANAGEMENT

CIGRE B5.09 concluded that selecting the most effective remote data management tool requires understanding of several functional, environmental, and technology factors that are important to timely and responsive operations for power system safety, reliability and stability.

Efficient control of remote data requires setting a central rule one and implementing it throughout operational planning and engineering to provide effective coordination. Using the standards-based tools offered by IEC 61850, a centralized rule can be enabled without managing activities individually at different sites with multiple separate vendor-specific (or ad hoc) policies and tools. IEC 61850 offers the capability to provide a “set it and forget it” approach that automates policy communication to the remote nodes and provides integrated notification if something does not proceed in accordance with policy.

Available bandwidth, as well as tolerance to a range of varying network conditions or conduits, must be considered. Remote locations frequently have varying bandwidth availability that needs to be shared among multiple applications and users. For this reason, remote data management and movement solution (particularly large data files) should have features that enable efficient use of available bandwidth such as byte-level differential data transfer, bandwidth throttling, multi-streaming, and compression.

Understanding the rate of data change between backup periods is also very important. The rate of change in a fairly busy remote typically ranges from three percent to five percent per day. In addition to data rates, the amount of network overhead (or information) needed is also an important consideration – with less being better. Finally, some remote connections will likely be impaired during some processes, the ability to restart at the point of failure is critical, as is the ability to reroute information flow to alternate networks.

To minimize or eliminate the need for manual effort at remote locations, the management solution must be able to automate processed and interface with remote applications to securely access data. Therefore, the remote data solution must be able to integrate with the application and invoke the native application processes automatically – without human intervention.

A utility with multiple remote locations will commonly have a variety of computing platforms and applications at those locations requiring a solution to function within a heterogeneous environment. While this seems simplistic, many SCADA systems and engineering tools today only work with homogeneous environments.

Relying on individual backups and separate point processes for each remote site is not effective. Solutions should be able to set policies pertaining to the data, automate process to execute those policies on remote servers in the substation, and to move data between remote or edge servers (at the substation level), sometimes called a proxy

server, and central or core systems within the control center.

In this model, individual remote backup and archive processes at the remote sites are replaced with a consolidated process that moves remote data to a hub site for backup and archive. This requires moving the pertinent data over available networks in an efficient, secure, timely fashion, and therefore requires technology that can deal with many issues associated with remote online management of data among many sites and network connections.

4 WHEN WILL CIGRE B5.09'S WORK BE AVAILABLE

CIGRE B5.09 is on track to complete their technical brochure in April 2006, at which time it will be sent to CIGRE for final editing and publication. If you are interested in following this work please contact the author holsteindk@adelphia.net who is the Convenor for this working group.

5 REFERENCES

- [1] AGA Report 12 “Cryptographic Protection of SCADA Communications.”
- [2] IEC 61784-4 “Digital Data Communications for Measurement and Control - Part 4: Profiles for Secure Communications in Industrial Networks”
- [3] IEC 61850 “Communication networks and systems in substations”
- [4] IEC 61968 “Application Integration at Electric Utilities – System Interfaces for Distribution Management”
- [5] IEC 61970 “Energy Management System Application Program Interface (EMS-API)”
- [6] IEC 62351 “Data and Communication Security”
- [7] IEEE C37.115-2003 “IEEE Standard Test Method for Use in the Evaluation of Message Communications Between Intelligent Electronic Devices in an Integrated Substation Protection, Control and Data Acquisition System”
- [8] ISA SP99 “Security Technologies for Manufacturing and Control Systems”
- [9] “IEC TC 57 Security Standards for the Power System’s Information Infrastructure – Beyond simple encryption”, by Francis Cleveland
- [10] ANSI X9.69-1994, “Framework for Key Management Extensions”
- [11] ANSI X9.73-2003, “Cryptographic Message Syntax”
- [12] ANSI X9.96-2004, “XML Cryptographic Message Syntax (CMS)”