

industry reports

77

Remote On-line Management for Protection and Automation



B5 is one of 16 Study committees of CIGRE. Its scope is to facilitate and promote the progress of engineering and international exchange

CIGRE STUDY COMMITTEE B5 COMMISSIONED A STUDY to explore the use of Information Technology (IT) application for remote on-line management of Substation protection and automation. Information technologies were to be considered as a general concept; intranet and internet technologies are subset of IT. Study Committee B5 limited the scope of work to the management of protection and automation functions, and explicitly excluded any analysis or implication related to the execution of protection and automation functions. Specifically, traditional Energy Management System (EMS), Distribution Management System (DMS), and adaptive (and automated) protection operations are excluded.

Remote on-line management refers to an application “remote” from the substation (where the IEDs are located) and using data exchanged with the IEDs. 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; the context is mainly well defined by the configuration parameters and limits of measured data. Imagine a utility that can automatically obtain the protection and automation data from any repository to find the



by Dennis Holstein

evidence needed to characterize and respond to a particular fault before it grows out of control. Such a capability could dramatically lower the cost and time to take corrective action and maintain reliable power delivery services.

Imagine a utility that can automatically obtain the protection and automation data from any repository to find the evidence needed to characterize and respond to a particular fault before it grows out of control. Such a capability could dramatically lower the cost and time to take corrective action and maintain reliable power delivery 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 on-line management mature, new solutions that merge the value of controlled access and use of protection and automation data will become ubiquitous.

Examples of core information technology used for remote on line management of protection and automation are presented to highlight the operational advantages of the enabling technologies. It is our belief that remote on line 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 on-line 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.

There are several possible applications but only some of them are within the scope of this technical brochure. Figure 1 describes a series of applications categorized by names; there is no agreed taxonomy here, so the definition is within the scope of this technical brochure only. The brochure is restricted to three categories: Network Maintenance, Product Maintenance, and Product Coordination.

Recommendations and Findings – what we learned

This work has considered the various experiences gained in many locations over a number of years in the use of remote on-line management of protection devices. It is recognized that there have been a number of levels and complexities of such techniques and technologies employed to date and several new ones that are already being deployed.

This work cannot hope to define “the” right technology to use to meet a particular utility’s

operational objective. However it can serve as a guideline to utilities seeking to determine the range of solutions available and the issues that need to be considered in the final choice.

The following findings and recommendations are considered highest of importance and deserve to be addressed in more depth by future CIGRE working groups

Version control for asset management

Version control is required for reliable operations of the power system during pre-configuration, commissioning, and operation.

Suppliers need to provide version control at every level needed by the user. Version control requirements are driven by:

Hardware: Define maintenance lots, keep asset records, ensure appropriate training of maintenance operators, and define recertification requirements.

Software: Define when to upgrade software based on functional or bug correction, optimize cost, and define recertification requirements.

Pre-configuration: Define IED generic behavior for a given use in order to simplify the final setting and configuration.

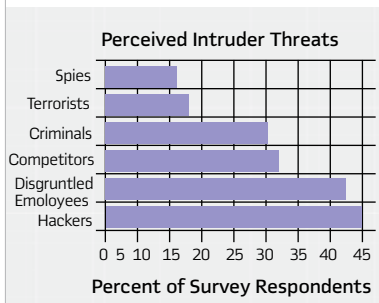
Configuration: Define consistent functions split between IEDs and client software.

Setting: Optimize the system behavior for both local and global network use.

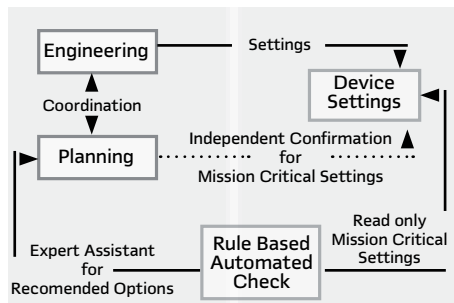
Improving the bridge between coordination studies and remote management

An advanced concept to improve the bridge between coordination studies and remote management is illustrated in Figure 2. 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 Figure 1. First, enabling read-

1 Perceived threats to power supply control



2 An advanced concept to improve coordination



only privileges for mission critical settings by an automated remote on-line 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.

A brief summary describing why a “one person” approach is not a good idea and the vulnerability of automated tools is discussed in the technical brochure.

Information security – you can’t do without it

Surveys by EPRI and others have identified the Insider threat as one of the highest intrusion threats in today’s environment. Clearly, one can deduce from Figure 1 that Identity Management (IM) and Role Based Access Control (RBAC) are required to minimize these threats. For example, the Engineering and Planning group within a Utility may have the role of controlling the setting of parameters in IEDs while the Operations group may only have the authority to monitor these parameters and behavior of the system with these parameters. After an individual has been identified as a genuine member of an organization and member of one of these groups, separation of these levels of authority may be achieved with a standards-based RBAC scheme.

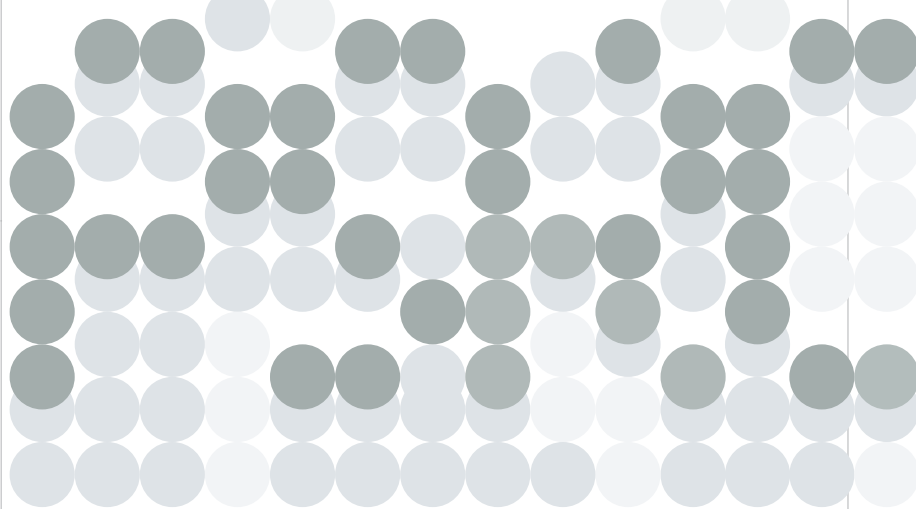
The way forward

The CIGRE technical brochure provides a roadmap for your consideration of new technologies for remote on-line management.

- How best to improve coordination of mission critical device setting to prevent blackouts.

- Role Based Access Control schemes to improve access to and use of data and field device operations.

- Use a proxy server to improve security without changing existing protection and automation equipment.



Beware Substations are not like offices



The Power System
Relaying Committee is in
the Power Engineering
Society of IEEE.

by John T. Tengdin, P. E. - Life Fellow
IEEE, USA

WITH THE GROWING POPULARITY OF IEC 61850, there is a mistaken belief by some that office grade Ethernet devices may be used with impunity in an electric utility substation. But there are substantial differences between these two environments that cannot be ignored. As a starter, substation control houses are usually not air conditioned, insulated, or forced ventilated. So the equipment in those house must withstand temperatures never seen in an office.

Then when high voltage disconnect switches are opened (not a fault, just a switching operation), transients are generated that couple on to the control wiring that runs from the high voltage yard into the control house. And in the control house, the simple act of de-energizing an auxiliary dc relay (one designed to have a low battery drain) will create fast rising transients in the control wiring. The vital equipments, that must operate during loss of station power, are supplied by DC from the station battery. Roving operators are still using five watt transceivers

(walkie-talkies) in close proximity to critical equipment that can cause malfunctions. And new substation control houses have floor coverings that will produce high levels of electrostatic discharges.

The industry’s protective relay engineers recognized these environmental hazards to critical equipment in a substation control house, and developed a series of standards addressing each of the issues. IEEE Std™ C37.90 defines control power voltage ratings and tolerances, insulation testing, altitude and derating factors for altitude. The latest update (2005) includes a requirement that the temperature ratings be achieved without fans or forced ventilation. The switching surge and fast transient immunity is defined in IEEE Std C37.90.1. RF immunity to hand held walkie-talkies is defined in IEEE Std C37.90.2. Electrostatic discharge immunity is defined in IEEE Std C37.90.3. All of these are appropriate for protective relays interconnected by direct wiring. The criteria for passing these tests is, in essence, no physical damage and no false trips.



by John T. Tengdin

Then along came communications networks in substations. Some early installations used Ethernet devices from commercial suppliers – which were only designed for pristine office environments – and there were failures. The electric utility industry and its suppliers recognized the need for a substation oriented standard and formed a task force in 2002 within the IEEE Power Engineering Society’s Substations Committee. The goal of that task force was to develop a standard for communications networking devices (hubs, switches, routers, modems, firewalls, etc.) in substations by building on the work done in the IEEE C37.90 series of existing protective relay standards. But since this was to be a standard for communications devices, the major challenges were 1) to define the communications that were to be ongoing during the C37.90 series defined tests, and 2) to define the criteria for passing the tests.

The result was the publication in 2003 of IEEE 1613 Standard Environmental and Testing Requirements for Communications Networking Devices in Electric Power Substations.

That standard defines these two performance classes for these devices:

“Class 1. This performance class is for communications devices used for general purpose substations communications where temporary loss of communications and/or communications errors can be tolerated during the transients. All devices shall meet Class 1 requirements unless Class 2 is specified by the user or manufacturer.

“Class 2. This performance class is for communications devices used in substations communications where it is desired to have error-free, uninterrupted communications

during the occurrence of the transients.” The transients include switching surges, fast transients, RF immunity from five watt walkie-talkie transceivers, and from electrostatic discharges.

The standard also defines the method of capacitive coupling the switching surge and fast transient voltages to the comm lines during the tests. Given the severity of these transient tests, the net effect of this Class 2 requirement (error-free, uninterrupted communications during the occurrence of the transients) is that only fiber optic comm lines will pass the test. The only exclusion is from this test is “Connections that, as stated by the manufacturer, shall be less than 2 m in length”.

In addition, IEEE 1613 states: **“The following conditions are to be met by both Class 1 and Class 2 devices:**

- No hardware damage occurs.
- No loss or corruption of stored memory or data, including active or stored settings, occurs.
- Device resets do not occur, and manual resetting is not required.
- No changes in the states of the electrical, mechanical, or communication status outputs occur. These outputs include alarms, status outputs, or targets.
- No erroneous, permanent change of state of the visual, audio, or message outputs results. Momentary changes of

these outputs during the tests are permitted.

- No error outside normal tolerances of the data communication signals (e.g., SCADA analogs) occurs.”

Due to an oversight, IEEE Std 1613-2003 does not include the altitude and altitude derating factors that are a part of IEEE Std C37.90. So work is now underway on an amendment to add those requirements to IEEE 1613. No other changes have been proposed. It has been a very stable standard. As one can see, the requirements in IEEE 1613 are comprehensive (and soon to be more so). For the utility, compliance with IEEE 1613 is the best way to specify equipment expected to not only survive, but to operate correctly, in a substation environment.

Since its publication in 2003, IEEE Std 1613 has been regularly cited by major manufacturers of substation communications equipment (modems, Ethernet routers, switches, etc.) and by many specifying utilities. When a manufacturer states their equipment is “substation hardened”, one should ask “Does it meet IEEE 1613?” To this writer’s knowledge, this is the only standard for substation communications devices that requires transient immunity testing while communications are underway.

With the increased popularity of IEC 61850, communication devices are becoming part of the protection system and have to withstand the substation environment.