307

REMONTE ON-LINE MANAGEMENT FOR PROTECTION AND AUTOMATION

Working Group
B5.09

October 2006

Remote On-line Management for Protection and Automation

Working Group B5.09

At the time this report was completed, Working Group 09 of CIGRE Study Committee B5 had the following membership [Corresponding Member is designated CM]:

Dennis Holstein (United States), *Convenor*

Alex Apostolov (United States),
Peter van der Meer van Houtum (The Netherlands),
Emanuele Ciapessoni (Italy),
Tetsuo Matsushima (Japan - CM),
Jose Diaz (United States),
Albertino Meneses (Portugal),
Luc Hossenlopp (France),
Juan Torres Pozas (Spain)

Table of contents

1. Introduction 1
   1.1 Scope 1
   1.2 Purpose 1
2. Findings and recommendations – what we learned 2
   2.1 Version control for asset management 2
   2.2 Version control of IEC 61850 for each logical node 3
   2.3 Improving the bridge between coordination studies and remote management 3
      2.3.1 Why a one person approach is not a good idea 4
      2.3.2 Automated tools – another vulnerability 4
   2.4 Information security 5
3. Organizational issues related to employees and 3rd- party personnel 6
   3.1 The situation today 6
   3.2 Suggested organizational improvements 7
4. Architectural view 7
   4.1 Functions to be managed 7
      4.1.1 Monitoring and event reporting 8
      4.1.2 Status monitoring 8
      4.1.3 Data quality analysis 9
      4.1.4 Alarm processing 9
      4.1.5 Control functions 9
      4.1.6 Special considerations for access to the maintenance ports 10
   4.2 Communication configurations 10
      4.2.1 Dedicated communication channel configurations 10
      4.2.2 Communication protocols 11
      4.2.3 Communication links 11
   4.3 Operational constraints 12
   4.4 Architectural impact due to functional integration and migration strategy 13
5. Access control and information security 14
   5.1 Physical security assumptions 14
   5.2 Security domains 15
   5.3 Access control mechanisms 17
      5.3.1 Authentication 17
      5.3.2 Authorization 18
   5.4 Message integrity 18
   5.5 Confidentiality 18
6. Application objectives of the remote on-line management 19
   6.1 Version control 20
      6.1.1 Categories 20
      6.1.2 Reasons for change and consequences 21
      6.1.3 Management 21
   6.2 Recording and storage 22
   6.3 Automated fault analysis 23
   6.4 IED testing 24
   6.5 Power system analysis 24
   6.6 Quality of Service calculations 24
   6.7 Primary equipment asset management 25
   6.8 IED data for the operator 25

7. State of efficiency improvement in protection relay maintenance and operations 25
7.1 Substation control technologies in 21st century 25
7.2 Efficiency improvement items 26
7.3 Present state of remote management 28
7.4 Expectations of remote management 28
8. Definitions of terms and acronyms 29
8.1 Definition of terms 29
8.2 Definition of acronyms 30
9. References 30

Table of figures

Figure 1 Example of an advanced concept to improve coordination 4
Figure 2 Typical communication links 11
Figure 3 Example of a notional proxy server 14
Figure 4 Perceived threats to power supply control: Results of EPRI survey of electric utilities 15
Figure 5 Example of an organization for energy services 16
Figure 6 Categories of IED applications 19

Table of tables

Table 1 Version control requirements 20
Table 2 Reason for change and consequences 21
Table 3 Measures for improving efficiency 26

1. Introduction

Remote on-line management refers to an application “remote” from the substation (where the IEDs are located) and using data exchanged with the IEDs. The opportunity presented by remote on-line management for protection and automation is enormous, and 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; 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 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.

In this technical brochure, 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.

With this technical brochure, we welcome you into the next decade of remote on-line management for protection and automation of electric power delivery.

1.1 Scope

CIGRE Study Committee B5 commissioned this 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.

1.2 Purpose

This technical brochure 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

(IT) to remotely manage the protection and automation functions. It applies for new substations as well as for refurbishment of secondary equipment in existing substations.

The purpose is to assist engineers who have not yet had experience with modern IT applications for remotely managing equipment by providing useful information gained by utilities, manufacturers, and system integrators.

Unless otherwise stated, the definitions provided in the IEEE 100 dictionary are used in this brochure [22] .

2. Findings and recommendations – what we learned

This report 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 report 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.

2.1 Version control for asset management

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

IEC 61968 [10] and 61970 [11] use a Common Information Model (called CIM) for specifying common interfaces to support application integration in terms of system interfaces. IEC 61968 is used for distribution management, and IEC 61970 is used for Energy Management System Application Program Interface (EMS-API). 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.

This study concluded that to make version control useful it should be designed to facilitate the smallest data object that can be tracked in the devices (see Section 2.2). 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, to efficiently manage the version control process one must address the strong coupling between capabilities provided 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 to 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 ensure an overall protection scheme.

2.2 Version control of IEC 61850 for each logical node

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 logical device as a whole, such as nameplate. LN0 also contains the version of the logical device configuration.

Settings however, are contained in other logical nodes, LNx, 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 LNs 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 LNs 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. IEC TC57 working groups responsible for 61850 data objects should consider a common approach to version control of settings that can be standardized for all implementations.

2.3 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 1.

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 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.

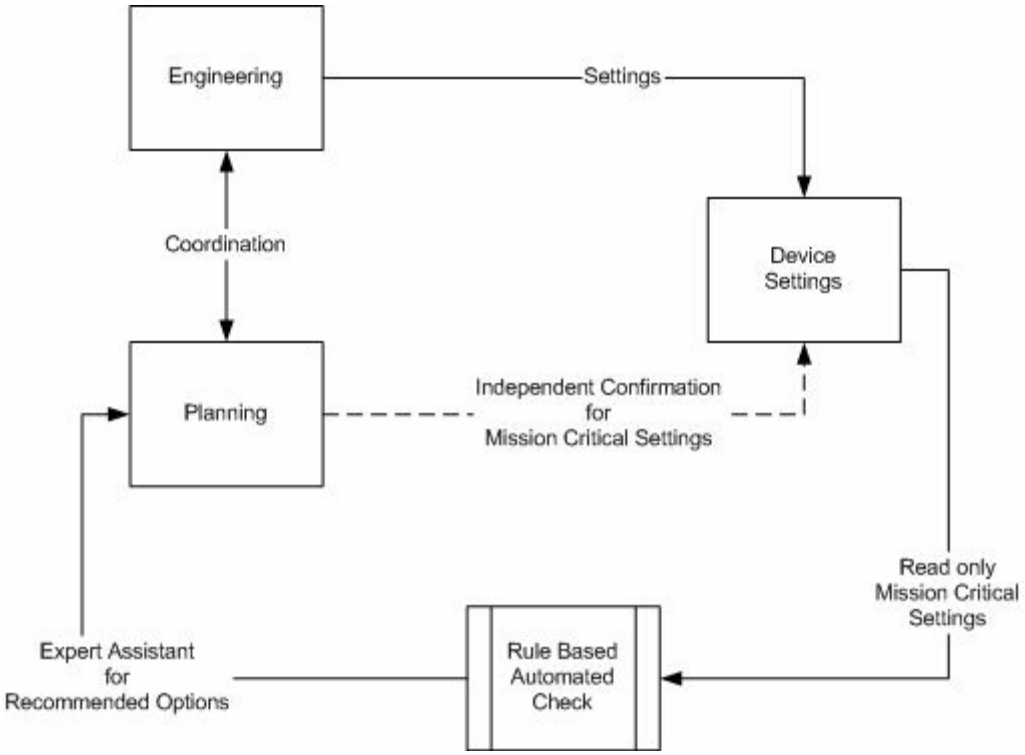

Figure 1 Example of an advanced concept to improve coordination

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. Dynamic adaptive protection also needs to be addressed, but is out of scope for this paper.

2.3.1 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, 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[1]. 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.

2.3.2 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. This study concluded that tools should be used to assist an operator, not to replace the operator.

[1] The 1965 blackout in the Northeast of the United States was due to a setting that was established 7 years before the blackout and never checked to be sure it was correct for the loading conditions in 1965.

2.4 Information security

Information security for access and use control is currently either non-existent or largely inadequate in most installations. This is a major concern because remote management for mission critical functions requires positive control of access to communication ports of the device and the use of the functions and data once access has been granted. From an end-user perspective 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 recording the violation, 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.

These security requirements are not met in today’s legacy devices. For this reason, external hardware or software components are needed to realize a degree of security, which should be aligned with the risk assessment and security policy of the user.

With these requirements in hand, an informal survey of work-in-progress was conducted. Results obtained from this survey showed 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. [12] [13]

3. IEEE C37.115-2003 recommends the use of security agents in response to requirements 1 and 2 only. [17]

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. [4]

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. [8] [20]

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. [1] [2] [3]

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.

3. Organizational issues related to employees and 3rd- party personnel

Organizational issues related to employees and 3rd-party personnel are an important consideration for remote on-line management.

3.1 The situation today

Remote on-line management must consider all issues related to how each organization within a company will make use of the same data from IEDs that are a part of the required equipment to perform their intended functions.

Before the introduction of modern IEDs, each piece of equipment was developed to perform a specific function within substations. People within the company were in charge of one or several functions (local operation, maintenance, planning, system protection, telecontrol), and devices were assigned to the corresponding organization. Because of this relationship, it was easy to identify which IED was assigned to a function and the organization to which that IED belongs.

New technologies have now merged the protection, measuring and control functions (local and remote) into the same IEDs, so the situation is now completely different.

- One IED (called a multi-function IED) performs more than one function.
- More than one organization makes use of the same IED, one function is also performed by means of a set of several IEDs, and everything is mixed.
- Most importantly, data has a point of presence. It is no longer communicated from A to B; but it is available to all those who have a legitimate use for the data.

In view of this situation the company needs to decide how best to structure its organizations to better (more efficiently) perform the roles and responsibilities needed for reliable power delivery.

3.2 Suggested organizational improvements

Normally, technical skilled personnel working on protection and control are very close within a company, so it is a common practice to merge these functions into one department. Sometimes telecontrol functions can also be merged into this department.

However even with this merger one issue remains - configuration changes (names, measuring ranges etc) may come from the local control personnel. These configuration changes should be controlled and managed in accordance with company policy.

Furthermore, the introduction of remote IED management should be coupled to the formalization of an asset management structure.

Where integration between organizations is not feasible, very strict and restrictive practices and rules are commonly established. The problem with this approach is that it usually leads to higher costs and less efficiency for the maintenance and operational activities.

4. Architectural view

Electric utilities need to remotely monitor and control all aspects of protection and automation operations continuously – 24 hours a day, 7 days a week.

This section describes some of the high level functions to be managed, then the most common communication architecture used for remote on-line management of protection and automation, operational constraints that must be considered for remote on-line management, and the appropriate levels of functional integration and migration strategy.

4.1 Functions to be managed

Supervisory Control and Data Acquisition (SCADA) systems were developed to reduce labor costs, and allow system-wide monitoring and remote control from a central location. At each remote site, an Intelligent Electronic Device[2] (IED) may be connected by local wiring to other field devices to be controlled and monitored. The IED also has a communication port, which is used to communicate with the control center over a communication link. The communication link can be dial-up phone, leased line, spread spectrum radio, Intranet/Internet, etc., depending on cost, availability, and operating constraints. Using the communication links from the control center, an operator can thus perform remote on-line management of protection and automation functions, or perform direct control of substation circuit breakers, switches, etc.

In addition to using the SCADA communication channels, other communication channels are used for remote access to IED maintenance ports. Depending on the utility's operating policy, an engineer's or technician's notebook computer is commonly used to change IED settings, download software, and perform other non-control functions.

[2] An IED may be implemented as a Remote Terminal Unit (RTU), substation computer, relay, measurement unit, etc.

4.1.1 Monitoring and event reporting

Acquired control data is automatically monitored to ensure that measured and calculated values lie within permissible limits. The measured values are monitored with regard to rate-of-change and for continuous trend monitoring. They are also recorded for post-fault analysis. Status indications are monitored with regard to changes, and may be time tagged by the IED if it contains an internal clock.

Monitoring these data may have various objectives and of course differs between different data. If the monitoring detects a violation of limits and changes of status indications, event processing reports such events to the operators via the SCADA communication link.

4.1.2 Status monitoring

At the control center, each status indication is compared with the previous value stored in the database. An event is generated when the status changes. The status is usually monitored against a pre-set “normal” status, thus creating a normal/off-normal operation state (of the device), which can be presented to the operator. The reporting of status changes can be delayed by a number of seconds. This is useful for suppressing transient alarm signals and temporary intermediate positions of two-state devices.

Special delaying schemes are also often implemented, for instance to detect automatic reclosure operations by combining electric circuit breaker changes and status signals for the automatic equipment itself. In the case of a successful reclosure of local automatic equipment, alarms are suppressed.

4.1.2.1 Limit value monitoring

Each measured value can often be monitored at the IED or at the control center against a set of limit values. Limits can be introduced on both sides of a typical, or reasonable, value. This value may correspond to the physical quantity or the normal zone of that physical value. Some possible reasons for their existence are:

- Upper and lower reasonable limits which are used for specifying a range where a reasonable value should appear. If the limit is violated, there is a failure in the control system itself.
- Upper and lower alarm limits used to specify operating limitations. Violation of an alarm limit normally results in an alarm message to the operator.
- Upper and lower warning limits used to alert the operator, enabling intervention before an alarm limit is exceeded.
- Zero value limit, used to specify a dead-band around the zero value. A value inside the zero dead-band can then be regarded as zero, not making the violation subject to event processing.

There are various solutions for implementing limit value monitoring. It can be implemented at the control center or remotely. The more advanced remote data collection schemes always use limit value monitoring. When implemented in the control center, the monitoring is usually carried out in connection with updating values in the database.

The limit values are specified individually for each measuring point and can be changed by the operator at the Graphical User Interface (GUI). When limit value monitoring is

performed remotely, the new limits are transferred to the IED via the communication network.

4.1.2.2 Trend monitoring

There are many types of monitoring of trends in measured values. Some possibilities are:

- Rate-of-change detection for trend detection.
- Presentation of values in curve displays. This is often combined with some sort of algorithm for extrapolation; e.g., load forecasting.

4.1.3 Data quality analysis

All data collection and monitoring functions normally result in a set of status flags associated with the individual data. These flags constitute data quality attributes associated with the individual data as they are presented to the operator. Some commonly used data quality attributes are blocked for updating, blocked, substituted, manually entered, out of limit (reasonable/alarm/warning/zero), alarm state, and unacknowledged.

4.1.4 Alarm processing

At remote sites, automatic (non operator initiated) changes may occur on critical pieces of equipment. These changes of state are detected by the master station during the next systems scan, or are reported immediately in “report by exception” systems, and are immediately presented to the operator as alarms on the GUI, and logged with a time tag of when the event occurred. In the case of a major disruption many alarms may be generated in rapid sequence. The operator’s GUI only presents them all as alarms. In some more advanced SCADA systems, alarm-processing software may be employed to establish the root cause of the incident.

4.1.5 Control functions

Control functions are grouped into four subclasses: individual device control, control messages to regulating equipment, sequential control schemes, and automatic control schemes.

4.1.5.1 Individual device control

Executing ON/OFF, START/STOP, or TRIP/CLOSE commands are used to control simple on/off devices.

4.1.5.2 Messages to regulating equipment

Transmission of messages to regulating equipment represents a more advanced control function, and is performed on an as-needed basis. Applications include RAISE/LOWER regulation and set point adjustment.

As an example of RAISE/LOWER control, the operator selects the control point of a regulating valve controlled by an IED and issues a single RAISE or LOWER command, which will incrementally raise or lower the flow. The operator observes the change of flow in the analogue value, and issues another command if additional change is needed.

In the case of set point regulation, the operator sends a new set point to an IED control function. The new value is checked against predetermined limits, to prevent abnormal

values from being entered. The IED responds with the new set point which it has implemented.

4.1.5.3 Sequential control schemes

Sequential control means that a series of correlated individual control commands are executed. Sequential control schemes are designed to permit a sequence of such control commands to be executed automatically in predefined order, including suitable logical checks and time delays. Typically, only one operator command is required to initiate the control sequence.

4.1.5.4 Automatic control schemes

Automatically initiated commands are represented by closed control loops.

4.1.6 Special considerations for access to the maintenance ports

Engineers and technicians commonly use separate (non-SCADA) communication channels (e.g., dial-up) to access maintenance ports. They change settings, download programs, and perform other non-control functions. Typically, two or more levels of password protection are implemented by the IED manufacturer to discriminate between authorization levels. For example, one level may authorize read only privileges and another level is needed to authorize read and write privileges. Passwords only security is not very secure. Technology is readily available to retrofit existing communication channels to improve security by providing a minimum of two factor authentication to open the communication channel.

More security to control use of data can be enforced to a data object level of granularity. These methods are not generally available as a retrofit solution because they require changes to the embedded software in the IEDs.

4.2 Communication configurations

SCADA is generally implemented as a distributed process control system. Data acquisition and control are performed by remote IEDs, and by field devices that include functions for communications or signaling.

4.2.1 Dedicated communication channel configurations

Dedicated communication channel configurations may be implemented in any of several arrangements as shown in Figure 2.

The equipment shown in the control center is a simple example. The operator and engineer displays are interfaced to a master station. And, the master station is interfaced to a front-end processor (FEP), which is then connected to communication modems, one for every dedicated communication channel. Some smaller control systems combine the FEP with the master station. Others incorporate the display system in workstations that include the master station and FEP functions.

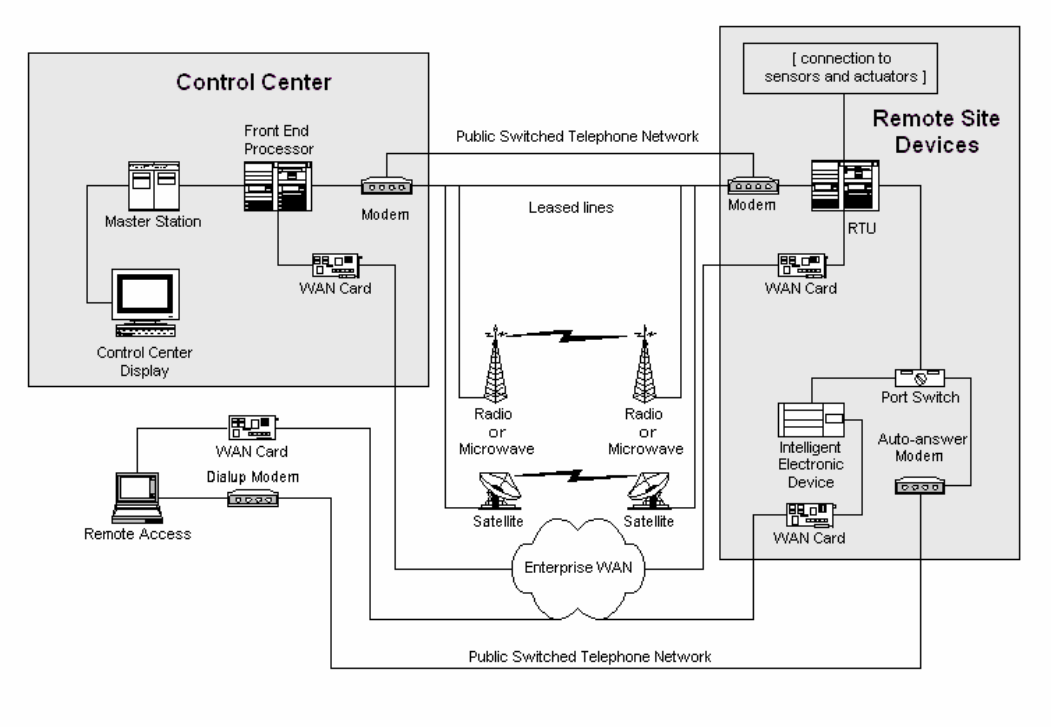

Figure 2 Typical communication links

4.2.2 Communication protocols

Different principles were described above to establish communication between two entities – a sender and a receiver of data. All these fundamentals are parts of rules, which make the two entities able to understand each other. A set of rules defining a communication procedure is called a communication protocol. Without a communication protocol the two entities would not be able to understand each other; they will not agree upon how to start and maintain a dialogue. A communication protocol defines for example:

- The structure of messages.
- Dialog semantics, rules and acknowledgement procedures.
- Establishment of error detection and correction.
- Recovery rules.

Commonly used protocols for SCADA include IEC 60805-101, DNP3, and Modbus. IEC 61850 is rapidly gaining acceptance for substation automation within the substation, between the substation and engineering workstations, and for special situations between the substation, and between the substation and the control center.

4.2.3 Communication links

A communication link is that part of the communication system used to connect two pieces of equipment that are going to communicate with each other. The link is the path for the movement of data. Typical communication links used for SCADA include leased

lines, dial-up phone lines, Intranet/Internet, radio, microwave and satellite. Some SCADA systems provide broadcast or multicast capabilities, and a few provide message store and forward capability.

Some SCADA systems use two or more communication links to provide backup communication should the primary link be compromised or fail. Some systems also use a backup control center. Should a problem develop with the primary control center, then the “hot” backup can then take over because it knows the status of the field equipment. If the backup control center is in the listen mode it will have received and logged all of the messages sent in either direction. If it does not receive all of the messages, it should force a scan of all substations to update its database.

Figure 2 shows some of the ways to communicate between equipment used to control electricity networks. RTUs and IEDs are located in transmission and distribution substations.

Figure 2 shows that each control center can be configured so that the FEP communication is through a modem or includes a WAN card if SCADA communication is over the enterprise wide area network (WAN). A remote access computer can communicate over the enterprise WAN, or over the public switched telephone network (PSTN) using a dial-up modem.

RTUs and IEDs may also include WAN cards for communications. If the PSTN is shared, at each remote site an auto-answer modem and port switch[3] is needed to communicate with the RTU or IED. Figure 2 shows sensors and actuators connected to the RTUs. Although not shown, sensors and actuators are also connected to IEDs.

None of the example communication links (channels) shown in Figure 2 are secure. Field data from sensors and actuators may transverse these insecure channels and consequently cannot be trusted, nor can the integrity of controls to output devices be guaranteed if those devices are connected by insecure channels, or if there are unprotected back doors to those devices. See Chapter 5 for an expanded discussion on access control and information security.

4.3 Operational constraints

The most important operational constraints are:

- Diversity of the communication infrastructure existing between the substation and the management center. It varies from leased telephone lines to fast speed intranet. This has consequences on the availability, costs, speed and security of operations.
- Diversity of the communication protocols impairing the ability to efficiently retrieve the necessary information. Substations have devices from different generations and IEDs that use different communication protocols. The lack of a standard defining the semantics of settings is particularly troublesome and tends to result in higher cost to establish the overall infrastructure.
- The need for a common approach defining the substation configuration. This is needed to get a logical view of the topology and functions of the substations IEDs.
- The need for access security better than password protection as discussed in Chapter 5.

[3] A port switch is only needed if the port is shared.

4.4 Architectural impact due to functional integration and migration strategy

For existing substations the most promising functional integration and migration strategies for substation automation are to:

- Use a well defined substation configuration language such as the IEC 61850 Substation Configuration Description (SCD), which includes a description of the communication architecture.
- Implement a secure access mechanism to the IED serial port shown in Figure 2. The substation could be equipped with a line multiplexer with one line per IED or group of IEDs, and one line connected to the management center. The benefit is the substation cost, the drawback is that all storage of disturbance records, processing and communication protocols must be handled at the central level since each IED has a limited storage capability.
- Use a gateway (also called Substation Host) to locally solve the communication protocol issues and possibly store information (such as disturbance records) in case of a communication failure or congestion. It is suggested (although not the unique solution) that this gateway communicates with IEC 61850 to the management center. The benefit of using IEC 61850 is to provide a non ambiguous way to designate information, thus linking applications to these data is facilitated. See also WG B5.11 for a more complete discussion. This solution provides also a smooth migration toward a full IEC 61850 substation.

For new substations, the gateway is a solution, even if IEDs are fully compliant with IEC 61850. In this case, the gateway could also provide proxy services. The benefits of the proxy are to:

- Concentrate the requests from various external “clients” desiring to communicate with each “sensitive server” (i.e. typically a protection relay); thus avoiding that a server performance degradation suddenly caused by several clients requiring data.
- Isolate messages generated within the substation from messages coming from outside the substation. As a minimum logical isolation is recommended (i.e. different client/server sessions), but it can be also physical (i.e. different Ethernet networks).
- A proxy server can also facilitate the integration of security on the network handling external data flows.

Figure 3 shows the use of a proxy[4] coupled with a “box” performing the security filtering. Each IED is communicating in IEC 61850; the proxy is providing a logical and physical isolation. The security layer has been represented as a separate box, but is actually a function that might be integrated into the proxy. The support of the further IEC 62351 standard (defining the security for TC57 defined protocols) within the proxy is a natural extension.

[4] A proxy server sits between the client application and the real server. It intercepts all requests to the real server to see if it can fulfill the requests itself. If not, it forwards the request to the real server. It has two main purposes, improved performance and filter requests.

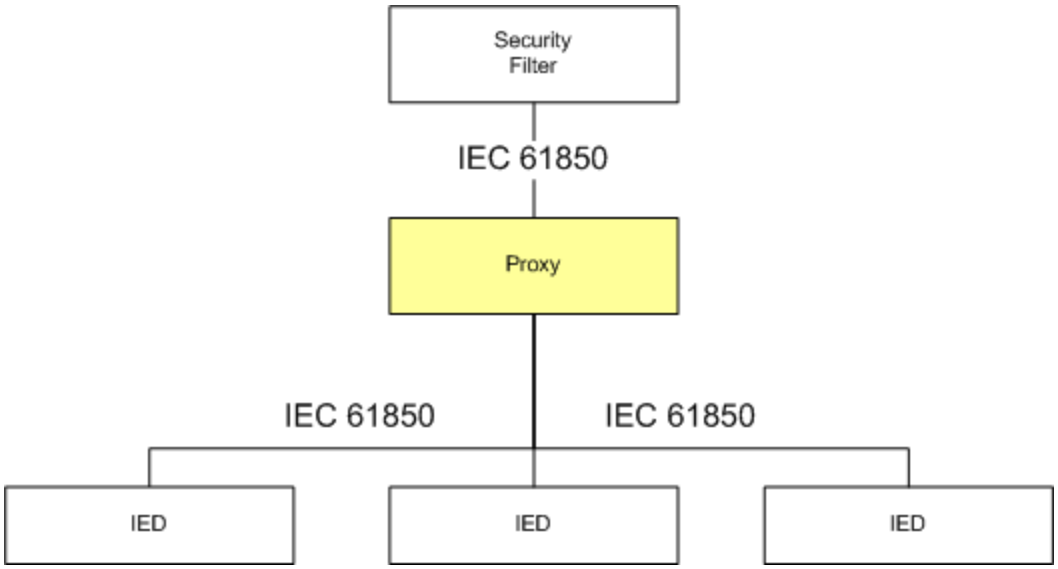

Figure 3 Example of a notional proxy server

5. Access control and information security

Remote access is an essential part of asset management since it provides an efficient method for configuration and management of remote assets. For example, consider the case where a modification of system configuration requires setting changes in devices located in various field sites. Without the benefits of remote access, physical visits to multiple sites, potentially in distant locations, would be required to implement the modification. Not only does the availability of remote access control provide an overall benefit for system operation, but it also increases security concerns due to the relatively poor control mechanisms presently in place to authenticate users during the access process and to determine their authority to perform a particular task. Furthermore, few, if any, mechanisms are in place to protect the information being obtained or exchanged between an operator and an asset.

This section provides a framework for analyzing specific areas of security that should be considered in the implementation of remote on-line management of devices. First, a high level view of security from an organizational perspective is presented in Section 5.1. Then, the various mechanisms required to provide a secure environment are described in order to establish a high level of overall system security.

The sensitivity of the information being exchanged also has to be evaluated in order to determine the applicability of the framework described. In some cases, all of the security mechanisms should be implemented while in others, perhaps only specific ones are required. In the next sections each of the categories will be discussed along with some guidelines for when the particular protection scheme should be utilized.

5.1 Physical security assumptions

For the purposes of this technical brochure we assumed that each of the facilities housing the assets to be protected using the described framework are physically secured sites with controlled access and monitoring. Only authorized individuals should have physical access to the protected assets and any unauthorized access should be detected and reported according to documented procedures.

5.2 Security domains

Surveys by EPRI [14] and others have identified the Insider threat as one of the highest intrusion threats in today's environment. Figure 4 shows the results of EPRI's survey of electric utilities reported in Reference [14]

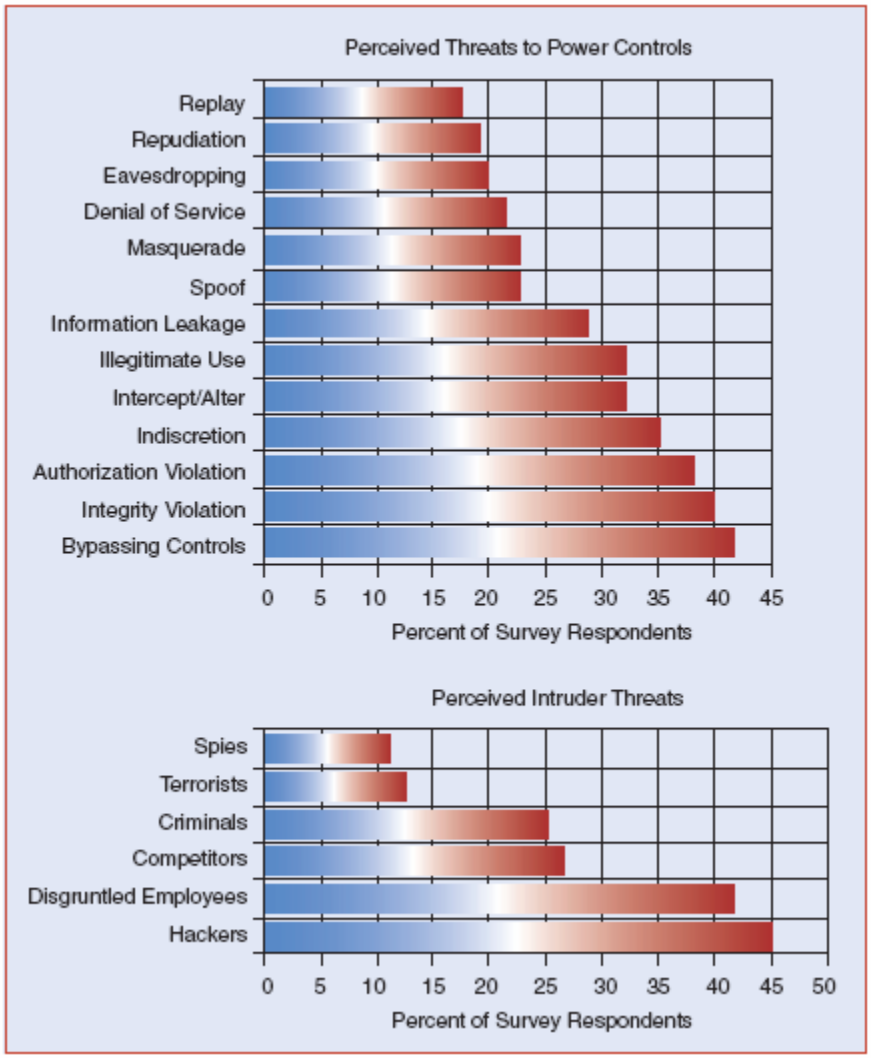

Figure 4 Perceived threats to power supply control: Results of EPRI survey of electric utilities

Clearly, one can deduce from Figure 4 that Identity Management (IM) and Role Based Access Control (RBAC) are required to minimize these threats; perhaps by using a proxy server as described in Figure 3. 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.

Therefore, the first task in defining a security framework is to identify the various groups within an organization and establish “highly trusted” individuals responsible for each group. This involves identifying the area responsible for each asset and the individuals which are to be authorized to access a specific asset as well as the level of access required by each one. The highly trusted individual responsible for each group will be the one that manages the authorization and controls granted for members of the group under his control or any external individual requiring access to an asset. Figure 5 describes a hypothetical example of an organization for a Utility with both Gas and Electric services.

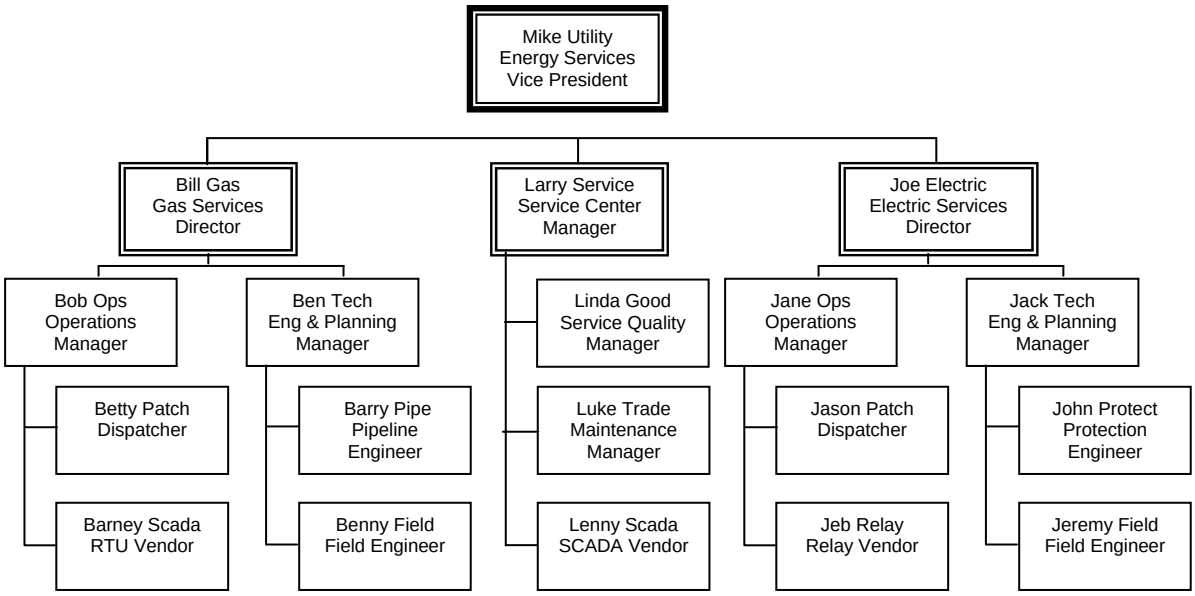

Figure 5 Example of an organization for energy services

In this example, the Gas and Electric Services Directors, or their designate, would be the most logical candidates for the highly trusted individual role within their groups. Likewise, the Service Center Manager would be the most logical candidate to carry the responsibility for the service group. It is also possible that only the Gas and Electric Services Directors would carry the responsibility and the Service Center Manager would only submit access requests for his personnel to a particular Director.

Each organization will have an established organizational structure, with assigned levels of responsibility, so the scenario may be different for each organization. The requirement is to review the existing organizational structure and the levels of responsibility in order to identify the highly trusted individuals that will have overall responsibility for the various assets in an organization so that an authorization structure for security can be defined.

It is also important during identification and definition of the various security groups that the implementation of an authority structure is put into practice as an overlay to the existing working environment thereby providing a security infrastructure without adversely impacting the required work flow presently in place. This may include establishing sub-organizations for work areas which require certain level of autonomy within a particular organization. A particular case of this requirement may be the management of vendor personnel requiring access to specific assets within an

organization. Excluding the use of a trusted third party service[5], there are two approaches to support this requirement.

- One approach is to only allow vendors to identify who will support a specific task, and the group owning the particular asset will then issue the needed credentials for the individual. This minimizes the trust needed in the vendor's internal control processes, but adds to the work load of the group owing the asset.
- Another approach is to empower the vendor as a sub-organization authority, which would allow the vendor to manage identity and authorization privileges in accordance with pre-specified agreements. This reduces the work load on the owner of the asset but requires more trust in the vendor's internal control processes.

5.3 Access control mechanisms

Undoubtedly, the most critical issue when dealing with management of assets, locally or remotely, is whether the activities being carried out are being performed by authorized personnel. It is crucial for overall system reliability that only authorized personnel perform any changes in configuration, operational parameter settings, and perhaps even status gathering from assets, if the information being obtained is of a sensitive nature, such as network topology and configuration information, which can be used to target cyber attacks.

The impact of potential unauthorized changes to assets is more straightforward to understand and the scope of the damage that can be caused by unauthorized changes to a particular asset will need to be assessed in order to determine the potential impact on system reliability. However, the potential damage which could be caused by unauthorized access to asset information is much more difficult to grasp. An analysis of the information which could be gathered from various assets and pieced together to provide significant and sensitive knowledge about the system would be required to determine if the information could be used to mount a cyber attack, a physical attack, or a coordinated combination of both.

In today's environment, most devices only require the use of fixed passwords for access to the various levels of control. In many cases, these passwords are the default password defined by a particular vendor. Any person that can establish remote access to the device can bypass physical security barriers implemented at a particular site. There is a requirement to establish a similar secure boundary for remote access to critical assets. In establishing these secure boundaries, there are two levels of security that need to be established – Authentication and Authorization.

In addition to authentication and authorization, other security mechanisms such as non-repudiation, are not addressed in this brochure, but should be the subject of future CIGRE work.

5.3.1 Authentication

For access control, strong authentication using at least two factors is the minimum requirement that should be considered. The typical implementation follows the "something you have" and "something you know" principle. Basically, this involves a

[5] Using a third party service is a definite possibility, but requires an extended discussion of its merits and requirements, which is outside the scope of this technical brochure. It certainly is a strong candidate for a future work item.

token that is PIN or Password protected so that only the individual with knowledge of this information can utilize the token. The accessed device should maintain a log of all authorized accesses as well as any attempts to access the device without proper credentials. The ideal implementation of the access control is on the device itself. However, an external device (such as the proxy server described in Figure 3) may be required to protect an asset in existing systems where the asset does not have “two factor” authentication for access control. Where an external device is utilized, the external device authenticates the user prior to establishing a connection to the protected asset.

Authentication only serves to identify an individual and whether that individual has the permissions required to access a device. It does not control or limit what an individual is allowed to do once they connect to the device. That process is managed by the authorization granted to the individual.

5.3.2 Authorization

When managing assets, it is also important to ensure that the functions an individual is allowed to perform are controlled by the “owner” of the asset. For example, a specific individual or service personnel may only be allowed to read information from a device but not change the configuration of the device. In general, this concept is part of Role Based Access Control (RBAC). It is important to keep in mind that when an external device is utilized to protect access to an asset, the level of authorization that could be exercised may be limited and only controlled by the various levels of passwords implemented by the device.

5.4 Message integrity

Communication systems are prone to potential “errors” in the transmission of data between devices due to noise on circuits, connection fallout, signal drift, etc. It is typically up to the protocols used by the communication systems to identify potential errors in messages but, depending on the nature of the “error” and the strength of the detection scheme used by the particular protocol, it may be difficult to detect a change in message data. As a result, a protocol independent scheme is advantageous to verify the integrity of messages being received by an asset, or the information it is reporting, particularly when slight changes in a message can have adverse effect on system reliability. A methodology for verifying message integrity would prove useful not only in messages between an authorized operator and an asset but also for messages exchanged between devices particularly if the information being exchanged can impact system reliability.

5.5 Confidentiality

The confidentiality of information being exchanged between an authorized operator (and workstation) and an asset should also be considered as part of an overall security policy for a system. It may be necessary to protect certain information being exchanged from exposure to unauthorized parties. The issue of data confidentiality should be considered during the determination of authorization levels for system operation since selection of the authorization levels is the first stage in segmenting the type of control or access being granted to a specific operator or group of operators.

For example, if only certain operators are granted access to specific data from an asset, then the data should be considered confidential and subject to protection. From a control perspective, confidentiality of data can prevent unauthorized persons from recognizing

the specific actions directed to an asset. Although knowledge about the protocols would be required to recognize specific commands and responses from assets, information about the protocols are common knowledge to personnel working in the operational environment and in many cases, information about the protocols is available from Internet sources. As a result, “security by obscurity” is not a reliable method for protection of sensitive information being exchanged between authorized operators and assets.

6. Application objectives of the remote on-line management

Remote on-line management refers to an application “remote” from the substation (where the IEDs are located) and using data exchanged with the IEDs. There are several possible applications but only some of them are within the scope of this technical brochure. Figure 6 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. EMS/DMS as well as Network automation categories are out of scope. This brochure is restricted to the three remaining categories: Network Maintenance, Product Maintenance, and Product Coordination. Each category contains several applications some of which are discussed in the following sections of this chapter.

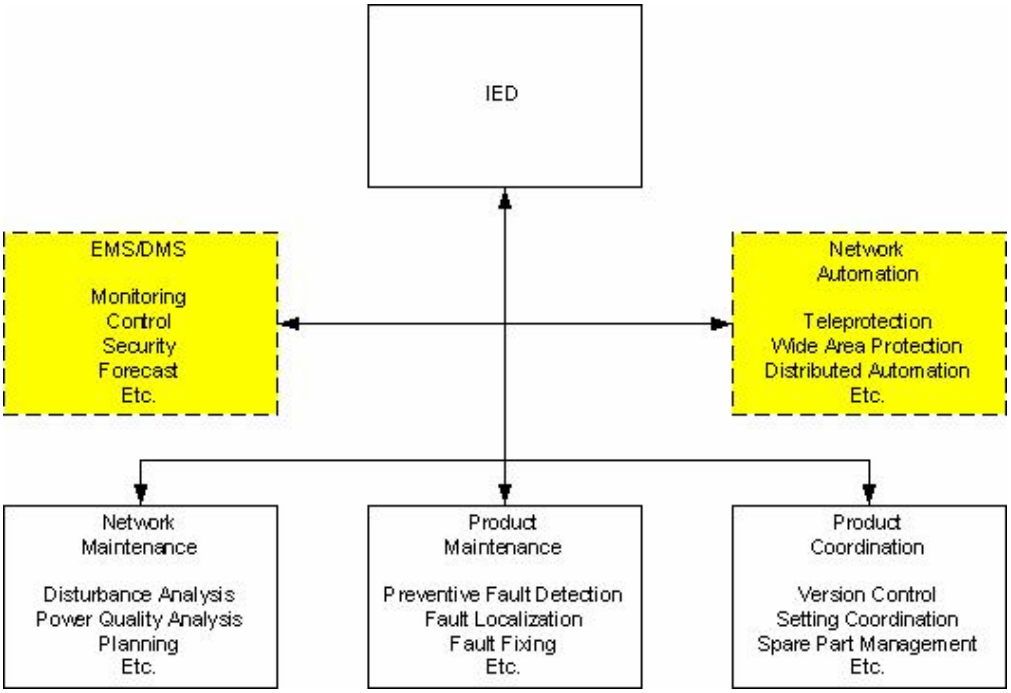

Figure 6 Categories of IED applications

Remote access to IED data is extremely important for many applications used by utilities. And it is cost effective because it eliminates the need to have qualified people on site with specific diagnostic equipment.

Automatic extraction of event related data, either locally or remotely, can prevent loss of information in the case of multiple events. The ability to remotely retrieve data and combine it with data from different locations facilitates timely power system analysis.

6.1 Version control

Versions control - from hardware to setting – is expecting to play a key role for the overall network management. The IEDs must be able to provide a minimum set of information to support this requirement. A central asset management tool can then be used to actively manage the IEDs; i.e., not only store the version, but make appropriate decision to optimize the overall costs.

Setting coordination workflow is another activity where changes could fully use secure remote IED management to better use the power delivery resources.

Version control refers to the identification of the version of an IED, the way to decide when to change them and the way to change them. It refers to hardware, software and setting and is today rarely stated explicitly in the procurement specification. This is managed by the supplier and the user. A common practice is to have the same version of hardware and software for all IEDs, and a specific setting file for each version.

Version control is expected to play an increasingly important role in order to cope with the rapid software evolution, the expansion of data exchange within the system and the need for maintenance cost reduction.

The analysis of the recent black-outs all over the world has often shown that setting of the IED was an issue. A study made in Scandinavia has shown that a large proportion of the IEDs (protection) failures were linked to the wrong configuration (settings and programmable scheme logic) of the device [21] . While version control is not the universal remedy against such problem it should help the situation.

6.1.1 Categories

Suppliers need to provide version control at every level needed by the user. In general, version control spans five domains, some traditional such as hardware and some quite new such as settings. Table 1 summarizes the version control requirements[6] in terms of why the supplier needs version control and why the user needs version control.

The following notes apply to pre-configuration and configuration in Table 1.

1. Pre-Configuration is defined here as the database loaded to the IED, prior to the final setting, in order to define default setting for a given use, and to limit the final setting operation to a minimum (this is in reaction to the generic capability of modern IEDs).
2. Configuration is defined here as the database loaded into the IED, prior to the final setting, in order to share common static data reference with other IEDs or client software program (in case of a distributed function such as substation interlocking).

Table 1 Version control requirements

Domain	**Supplier needs version control to**	**User needs version control to**
Hardware	Manage hardware obsolescence	Define maintenance lots, keep asset records, ensure appropriate training of maintenance operators, and define recertification requirements.
Software	Provide efficient and timely correction of software errors (bugs)	Define when to upgrade software based on functional or bug correction, optimize cost, and define

[6] Note, this level of refinement is not currently described in the data model of IEC 61850, and should be a candidate for future upgrade.

Domain	Supplier needs version control to	User needs version control to
		recertification requirements.
Pre-configuration (See Note 1)	Maintain a trace of the information needed for IED certification.	Define IED generic behavior for a given use in order to simplify the final setting and configuration.
Configuration (see Note 2)	Not applicable (user specific)	Define consistent functions split between IEDs and client software.
Setting	Not applicable (substation specific)	Optimize the system behavior for both local and global network use.

6.1.2 Reasons for change and consequences

Table 2 identifies the reasons for change in each domain, and the actions that will be taken in an asset management center in response to these changes.

Table 2 Reason for change and consequences

Domain	Reason for change	Consequences
Hardware	Component obsolescence Software error (Bug) New feature	Stock spare, move to new version Update if possible consequence Update if function of interest
Software	Component obsolescence Software error (Bug) New feature	Stock spare, move to new version Update if possible consequence Update if function of interest
Pre-configuration	Internal standard evolution New application HW/SW evolution Software error (Bug)	Update
Configuration	System function evolution New application HW/SW/Pre-configuration evolution Software error (Bug)	Update
Setting	Network evolution Other IEDs evolutions HW/SW/Pre-conf/Configuration evolution Software error (Bug)	Update

6.1.3 Management

To efficiently manage the version control process two levels of management need to be implemented: what needs to be done at IED level (typically by the IED manufacturer) and what needs be done at asset manager level (either by a person or a tool).

6.1.3.1 IED level management

The following capabilities are needed to effectively manage version control at the IED level.

- Capability to identify and communicate at least the version of each domain (hardware, software, pre-configuration, configuration, setting). Further modules version might be identified in order to permit a selective replacement of an IED component.

- Capability to facilitate the migration from one version to another. Import/export facilities and differences identification between versions. This is typically achieved by the IED engineering tool.
- Capability to document and publish the changes (including the reason for the change) in hardware or software in order to provide the information needed for asset management decisions. This is typically published on a supplier's web site.

6.1.3.2 Asset level management

The following capabilities are needed to effectively manage version control at the asset management level

- Capability to keep a description of the network including network topology, fault simulations, system protection scheme, etc. Also, an on-line access to information defined in the Common Information Model (CIM), or equivalent, version of the network is needed.
- Capability to keep a description of the associated IEDs in each substation together with their functions, communication, etc.
- Capability to keep an updated description of all versions, possibly by uploading information through a standard protocol – IEC 61850 is a logical choice.
- Capability to identify hardware, software and pre-configuration differences between IEDs in order to detect possible inconsistencies between IEDs.
- Capability to identify system setting consistency through predefined rules, derived from coordination studies, and between distributed IEDs in order to ensure the integrity of an overall protection scheme.
- Capability to check that the new version will at least improve the existing situation. For the situation that addresses pure obsolescence, the new IED should at least perform the previous functions, and for software or setting upgrades it should avoid regression as well as improve the situation.
- Capability to estimate the costs and benefits of a version update. This includes engineering costs, stock and maintenance contract costs, risk of malfunction on the network upon given events (including black-out), benefits of better setting coordination, update vs. new device evaluation, etc.
- Capability to manage version update once decided. This includes manufacturer interface, prioritization, work follow up, etc.
- Capability to manage the people authorized to do each type of version evolution in line with the security policy.

6.2 Recording and storage

It is important to normalize the storage of the information to facilitate the use of analysis tools. Analysis tools range from simple tools, commonly in use today, to more a powerful tool that can facilitate the maintenance of the overall network assets.

Archived data are used to optimize the preventive maintenance actions, improve restoration of service, and to increase the security of the network. This optimization is performed at several levels.

- **Network level:** capacitor or Flexible AC Transmission System (FACTS) for instance driven by power quality measurements.

- **Line level:** tree trimming for instance as result of recurrent faults.
- **Primary equipment level:** identification of maintenance intervals taking into account operation time, last operation, etc.
- **Secondary equipment level:** protection setting by checking the expected time coordination vs. measured results.
- **Operator level:** need for training course in case of wrong setting for instance.

The archived data used for asset management derived from IEDs contain “non-operational data,” which is data not normally used for Control Center applications. Non-operational data includes disturbance records, power quality reports, self-diagnosis made by IED, and version control data.

Timely reporting of these data is needed in the control centers, and secure mechanisms are needed to retrieve “operational data” from the IEDs to perform high level diagnosis of an event. The data needed are:

- Primary device data, such as circuit breaker operation time or transformer overload conditions, and more generally deep condition monitoring data.
- Detailed secondary device data such as start or directional information.

6.3 Automated fault analysis

The fast changing market environment, and the need to operate networks closer to their technical limits, is forcing utilities to take a closer look at every fault, both to improve maintenance techniques and to be able to quickly respond to events of significant public consequence.

Implementation of automated fault analysis tools present new requirements for IED and software and benefits from new technologies, namely high speed communication and standard communication protocols.

The impact of new standards and technologies, as well as the need for new analysis functions and their potential benefits, are being studied by CIGRE WG B5.20, which will elaborate on the work already done by CIGRE WG B5.03 (see CIGRE report: “Fault and disturbance data analysis, including intelligent system”).

Analysis is used for several purposes:

- **Single device event:** deep condition monitoring of a circuit breaker, transformer or IED. The objective is to optimize the preventive maintenance by predicting symptoms of a future problem if nothing is done.
- **Single process event:** fault or power quality violation, associated to one or more bays and substations, generation plants, etc. The objective is to understand the type of fault, the propagation in the network, the way to improve network stability, etc.
- **Correlation between events:** sequence of events of the protection system, reaction of the primary and secondary equipment in presence of fault, etc. The objectives are to check that the assumptions and setting are consistent, to restore quickly the network, etc.

Analysis needs timely data, which requires the capabilities to retrieve real time data from the remote IEDs, and to perform timely off-line analysis of complex situations so as to generate timely alarms for corrective action.

6.4 IED testing

Functional IED testing, given the risks involved for network operation, is a task utilities almost universally perform on site and with disconnected feeders or with protections disconnected. Nevertheless, data gathered in this process is of great importance to assess the behavior of protection and control systems during normal operation.

Some utilities are already adopting preventive maintenance strategies that take into account correct or incorrect IED behavior during disturbances, and from that derive larger or shorter intervals between maintenance actions and, in extreme cases, opt for outright replacement of underperforming equipment.

Remote on-line access to testing data also enables engineering staff to monitor IED response and eventually acts, together with the field team, to correct parameters and/or settings in a timely manner.

6.5 Power system analysis

Retrieval of actual short circuit data, together with the relevant event lists, is crucial not only for system behavior analysis but also, used with appropriate software tools, for more accurate simulations of network operating conditions and its response to major disturbances.

Retrieval of disturbance records allows the verification of models used for dynamic stability studies.

Retrieval of wave form records can be used to improve the models for transient stability studies and verify the correct operation of protection relays.

Coordination tasks, in a growing or fast changing network, consume an important part of existing (and usually limited) resources, so remote access to IEDs, together with the ability to retrieve and centrally store primary values and settings, significantly contributes to optimum use of those resources.

6.6 Quality of Service calculations

Qualities of Service (QoS) indices are generally used to assess the quality of power delivery within a country, region, sector, customer group or utility company. Different methods and concepts are used, usually depending on local common practices or regulations. However, the most widely used indices are:

- ENS (Energy not Supplied)
- EIT (Equivalent Interruption Time)
- SAIDI (System Average Interruption Duration Index)
- SAIFI (System Average Interruption Frequency Index)
- SARI (System Average Restoration Index)

Basic data needed for all of the above mentioned indices are the interruption time and the total affected load. Currently, data is retrieved from SCADA event logs and active power measurements. Future applications include remote retrieval of power data from intelligent meters and automated calculation processes based on remotely accessed IED event logs.

6.7 Primary equipment asset management

The traditional approach to preventive primary equipment maintenance is based on the estimation of a fixed maintenance interval (so-called time-based maintenance). The time cycles are derived from the experience gained through repetitive maintenance actions (which involve risks in equipment performance, either by direct human error or by an increased probability of intervention-induced failure) and from historical analysis of equipment behavior in service.

However, some factors can determine either the anticipation or the postponement of maintenance actions. Modern IEDs can give those responsible for asset maintenance valuable information on the actual condition of the substation primary equipment.

One example of data stored in substation IEDs which can easily be retrieved and used for maintenance planning purposes is the CB Interrupted Current (total and per trip operation), which, together with the number of trip operations, allows maintenance planners to assess the condition of the circuit breaker and optimize maintenance operations and costs.

The self-diagnosis capabilities of IEDs are also a valuable tool for deciding between corrective and preventive maintenance.

6.8 IED data for the operator

Many EMS and DMS applications already rely on data gathered and transmitted from remote IEDs. However, due mainly to bandwidth limitations of existing RTU communications channels, most of this information is presented to the operator in the form of grouped alarms which can sometimes mislead the operator.

The growing implementation of company intranet extensions to substations will allow the control room operator to have immediate on-line access to substation IED event logs but also to retrieve waveform and disturbance records.

7. State of efficiency improvement in protection relay maintenance and operations

The following summarizes parts of two Japanese Electric Technology Research Association (ETRA) reports [6] and [7] that are relevant to remote management. The ETRA study committees are composed of all Japanese utilities, manufacturers, research institute, and some universities. In each study committee a subject is studied based on detailed questionnaires answered by utilities, manufacturers, etc.

7.1 Substation control technologies in 21st century

A brief summary of the network systems in Japanese utilities is best characterized by the in introduction of token passing LAN with an optical star coupler in 1990, then an Ethernet LAN in the late 1990s. After 2000, protection relays with built-in web servers are common.

Each division, such as power transmission or distribution requires various kinds of data for facility maintenance, commercial use or service for customers, remote monitoring and control operations, efficiency of facility operation and energy trading. Data required for operation must be delivered within several seconds, on-demand data is needed for installation planning (once a month on average), data for maintenance is required once or twice a month, and data for commercial use and customer service is needed every ten minutes with a one minute response time.

In the future, the following data is required:

- High quality and stable power supply data for operation such as flicker voltage, harmonic voltage, unbalance voltage, active/reactive power, frequency, temperature of transformer windings, oil temperature (tending data), and gas density in the oil.
- Data for installation planning includes flicker voltage of bus-bar (trending data), reactive power, and load ratio of transformers (trending data).
- Data for maintenance includes information about transformer tap position (trending data), oil temperature, and moisture or gas density in the oil, circuit breaker operating times (trending data), partial discharge, cut-off current, intrusion surveillance, and natural disasters such as an earthquake. .
- Commercial or service for customers includes operating voltage and frequency, instantaneous voltage dip, bus-bar flicker (maximum and minimum) and on-off condition of circuit breakers.

Some of these pieces of information are now obtained in the operation center; however, the data is not delivered to maintenance, engineering and commercial centers.

Maintenance and operation jobs of protection relays in Japanese utilities are classified as follows:

- Facilities introduction
- Setting
- Analysis of relay operation
- Facilities monitoring
- Periodic or temporary inspection
- Actions for facility trouble resolution
- Facility refurbishment
- Actions for scheduled power system interruptions

A brief summary of the network systems in Japanese utilities is best characterized by the in introduction of token passing LAN with an optical star coupler in 1990, then an Ethernet LAN in the late 1990s. After 2000, protection relays with built-in web servers are common.

7.2 Efficiency improvement items

Table 3 shows expected improvement in the efficiency of the maintenance and operation jobs.

Table 3 Measures for improving efficiency

Maintenance & Operation Jobs	**Details**	**Measures for Efficiency Improvement**	**Notes**
Facility Introduction	Acceptance test Commissioning test	Simplify test items	

Maintenance & Operation Jobs	Details	Measures for Efficiency Improvement	Notes
Setting	Setting calculation Setting value management Setting change	High efficiency of settings using support tools Overall management with electronic data Visualization of setting values Remote setting	Efficiency improvement when required in conditions of inclement weather or temporary changes for some trouble situations
Relay operation analysis	Fault data collection and analysis	Quick response from a remote maintenance center and a reduction in restoration time Higher efficiency of fault analysis with automatic analysis system Solving data delay issue for multi-faults that happen at the same time	Data congestion occurs when multiple power system faults occur the same time Timely response requires information processed from raw data
Facility monitoring	Automatic monitoring	Remote monitoring	Need trend records of facility conditions
Inspection	Patrol Periodic inspection Special inspection Results management	Reduce frequency of patrol Simplify items of inspection Unify management of inspection and maintenance Link inspection interval to actual operation results	Abnormal conditions (such as noise, smell, roughness of surface contact) limit remote inspection Because all equipment is not connected to the communication network, remote monitoring is difficult
Actions for facilities trouble resolution	Situation investigation Restoration	Quick response from a remote maintenance center and a reduction in restoration time Higher efficiency of fault analysis and quick action in accordance with degree of emergencies Quick search for failed part	Required information • Relay operation record • Oscillograph record • System operation status • Fault condition • Setting values • Power system status • Maintenance record
Facility refurbishment	Schedule management	Acquisition of data for judging facilities aging	

Maintenance & Operation Jobs	Details	Measures for Efficiency Improvement	Notes
	Aged facilities diagnosis Refurbishment	level	
Action for scheduled interruption	Refurbishment Inspection Trouble investigation	Unified information management	

7.3 Present state of remote management

There are two types of remote management applications in Japanese utilities: limited application within a substation and application between the substation and operation center (control center). Data needed from protection relays are equipment attribute status, settings, operation results (abnormal alarms), and disturbance records. These data are needed to decide how best to introduce remote management.

Security is a major issue for the remote management. Utilities take precautions for active operations such as setting change or status change of devices. They impose some limitations, for example:

- Remote setting change operations are forbidden in some utilities because they lack confidence in the verification procedures.
- In some utilities, they require that a new setting be guarded by another command sent via a different data transmission route before the setting is enabled, or a direct switch on the relay panel is required to start when a setting is changed.

When introducing a remote management system, it is important to consider the number of substations and their importance, number of devices that are connected to the communication network, and the state of the data transmission infrastructures. The main reasons not to install remote management are:

- The expected efficiency improvements cannot be realized because other equipment (except relays) cannot provide the data needed by the remote management system.
- The frequencies of relay setting changes do not justify the cost of implementing a remote management system.
- Data transmission infrastructure is too expensive when the equipment is located in inaccessible (mountainous) areas.

7.4 Expectations of remote management

Japanese utilities continue to examine the benefits of future remote management systems because they offer the promise to unify various kinds of data transmission infrastructures, the enabling technology provides the basis for common use of data between various departments, and manufacturers are offering software that improves remote change of relay settings and functions.

Some recent Japanese applications of network technologies are:

- Use of a token passing LAN for protection and control system based on IEEE 802.4 using a star coupler was replaced by an Ethernet LAN (802.3).
- The use of protection relay built-in web servers so that maintenance can get data (such as settings, relay operation records, alarms, facility status) using the browser on their computer.
- The deployment of a fault locator system and disturbance recorder system.

8. Definitions of terms and acronyms

8.1 Definition of terms

Term	Definition
Asset	A useful or valuable quality, person, or thing; an advantage or resource.
Authentication	A process that establishes the origin of information, or validates an entity's identity
Authorization	Access privileges granted to an entity; conveys an "official" sanction to perform a security function or activity.
Confidentiality	The property that sensitive information is not disclosed to unauthorized individuals, entities, or processes.
Entity or agent	An individual (person), organization, device or process.
Integrity	The property that sensitive data has not been modified or deleted in an unauthorized and undetected manner.
Non-repudiation	A service that is used to provide proof of the integrity and origin of data in such a way that the integrity and origin can be verified by a third party as having originated from a specific entity in possession of the private key of the originator.
Password	A string of characters (letters, numbers, and other symbols) used to authenticate an identity or to verify access authorization.
Proxy server	A process providing a cache of items available on other servers which are presumably slower or more expensive to access.
Quality of Service	The performance properties of a network service, possibly including throughput, transit delay, priority. Some protocols allow packets or streams to include QoS requirements.
Revocation	The state of being cancelled or annulled.

8.2 Definition of acronyms

Acronym	Definition
AC	Alternating Current
AGA	American Gas Association
ANSI	American National Standards Institute
API	Application Program Interface
CB	Circuit Breaker
CIGRE	Conference Internationale des Grandes Reseaux Electriques (International Conference on Large Electrical Systems)
CIM	Common Information Model
CPU	Computer Program Unit
DMS	Distribution Management System
DNP	Distributed Network Protocol
EIT	Equivalent Interruption Time
EMS	Energy Management System
ENS	Energy Not Supplied
ETRA	Electric Technology Research Association (Japanese)
FEP	Front End Processor
FACTS	Flexible AC Transmission System
FEP	Front End Processor
GUI	Graphical User Interface
H/W	Hardware
IEC	International Electrotechnical Commission
IED	Intelligent Electronic Device
IEEE	Institute of Electronic and Electrical Engineers
IM	Identity Management
ISA	Instrumentation, Systems, and Automation Society
IT	Information Technology
LAN	Local Area Network
LN	Logical Node
PIN	Personal Identification Number
PSTN	Public Switched Telephone Network
QoS	Quality of Service
RBAC	Role Based Access Control
RTU	Remote Terminal Unit
SAIDI	System Average Interruption Duration Index
SAIFI	System Average Interruption Frequency Index
SARI	System Average Restoration Index
SCADA	Supervisory Control and Data Acquisition
SSD	Substation System Design
S/W	Software
TC	Technical Committee
WAN	Wide Area Network
WG	Working Group

9. References

[1] ANSI X9.69-1994, “Framework for Key Management Extensions”

[2] ANSI X9.73-2003, “ Cryptographic Message Syntax”

[3] ANSI X9.96-2004, “XML Cryptographic Message Syntax (CMS)”

[4] AGA Report 12 “Cryptographic Protection of SCADA Communications”

[5] BS 7799-2:2002 “Information management security systems – specification with guidance for use”

[6] ETRA Report, Vol.59 No.1 Jul. 2003 “Study of Efficiency Improvements in Protection and Relay Maintenance Operations.”

[7] ETRA Report, Vol.58 No.2 Jul. 2002 “Substation Control Technologies in 21 Century.”

[8] IEC 61784-4 “Digital Data Communications for Measurement and Control - Part 4: Profiles for Secure Communications in Industrial Networks”

[9] IEC 61850 “Communication networks and systems in substations”

[10] IEC 61968 “Application Integration at Electric Utilities – System Interfaces for Distribution Management”

[11] IEC 61970 “Energy Management System Application Program Interface (EMS-API)”

[12] IEC 62351 “Data and Communication Security”

[13] “IEC TC 57 Security Standards for the Power System’s Information Infrastructure – Beyond simple encryption”, by Francis Cleveland

[14] IEEE Power & Energy Magazine, September/October 2004 “The Future’s Smart Delivery System” by Clark W. Gellings, Marek Samotyj, and Bill Howe

[15] ISO/IEC 17799:2000 “Information technology – Code of practice for information security management”

[16] IEEE 1646-2004 “Standard Communication Delivery Time Performance Requirements for Electric Power Substation Automation”

[17] IEEE C37.115-2004 “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”

[18] IEEE Report “Application of peer-to-peer communications for protective relaying”

[19] 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”

[20] ISA SP99 “Security Technologies for Manufacturing and Control Systems”

[21] CIGRE Paper 34-103 “Fault statistics as a basis of designing cost-effective protection and control solutions”, Session 2002.

[22] IEEE 100: “The Authoritative Dictionary of IEEE Standard Terms”, Seventh Edition.