ELECTRIC POWER
RESEARCH INSTITUTE

IEC 61850 Technical Integration Evaluation

IEC 61850 Technical Integration Evaluation

1015962

Interim Report, December 2008

EPRI Project Manager
J. Hughes

ELECTRIC POWER RESEARCH INSTITUTE
3420 Hillview Avenue, Palo Alto, California 94304-1338 ▪ PO Box 10412, Palo Alto, California 94303-0813 ▪ USA
800.313.3774 ▪ 650.855.2121 ▪ askepri@epri.com ▪ www.epri.com

DISCLAIMER OF WARRANTIES AND LIMITATION OF LIABILITIES

THIS DOCUMENT WAS PREPARED BY THE ORGANIZATION(S) NAMED BELOW AS AN ACCOUNT OF WORK SPONSORED OR COSPONSORED BY THE ELECTRIC POWER RESEARCH INSTITUTE, INC. (EPRI). NEITHER EPRI, ANY MEMBER OF EPRI, ANY COSPONSOR, THE ORGANIZATION(S) BELOW, NOR ANY PERSON ACTING ON BEHALF OF ANY OF THEM:

(A) MAKES ANY WARRANTY OR REPRESENTATION WHATSOEVER, EXPRESS OR IMPLIED, (I) WITH RESPECT TO THE USE OF ANY INFORMATION, APPARATUS, METHOD, PROCESS, OR SIMILAR ITEM DISCLOSED IN THIS DOCUMENT, INCLUDING MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, OR (II) THAT SUCH USE DOES NOT INFRINGE ON OR INTERFERE WITH PRIVATELY OWNED RIGHTS, INCLUDING ANY PARTY'S INTELLECTUAL PROPERTY, OR (III) THAT THIS DOCUMENT IS SUITABLE TO ANY PARTICULAR USER'S CIRCUMSTANCE; OR

(B) ASSUMES RESPONSIBILITY FOR ANY DAMAGES OR OTHER LIABILITY WHATSOEVER (INCLUDING ANY CONSEQUENTIAL DAMAGES, EVEN IF EPRI OR ANY EPRI REPRESENTATIVE HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES) RESULTING FROM YOUR SELECTION OR USE OF THIS DOCUMENT OR ANY INFORMATION, APPARATUS, METHOD, PROCESS, OR SIMILAR ITEM DISCLOSED IN THIS DOCUMENT.

ORGANIZATION(S) THAT PREPARED THIS DOCUMENT

Open Secure Energy Control Systems, LLC

NOTE

For further information about EPRI, call the EPRI Customer Assistance Center at 800.313.3774 or e-mail askepri@epri.com.

CITATIONS

This document was prepared by

Open Secure Energy Control Systems, LLC
8070 Georgia Avenue – Suite 205
Silver Spring, MD 20910

Principal Investigator
S. A. Klein

This document describes research sponsored by the US Department of Homeland Security, the US Department of Energy, and Open Secure Energy Control Systems, LLC, with the document itself being sponsored by the Electric Power Research Institute (EPRI),

This publication is a corporate document that should be cited in the literature in the following manner:

IEC 61850 Technical Integration Evaluation. EPRI, Palo Alto, CA, 2008, 1015962.

PRODUCT DESCRIPTION

Designs and implementations of standards can reveal portions of formal standards that need to be further defined and/or issues that emerge in the integration or harmonization of two standards. This report captures the experience of using IEC 61850 and other related standards such as IEC 61970/61968 as part of an implementation in a Tool Kit. It also describes the implementation as well as the issues that have emerged from the experience of a tool developer.

Results and Findings

Results are presented in three areas:

- IEC 61850 Integration Technical Issues: Documents the issues and solutions identified.
- Standards Integration and Strategies: Provides information contributing to educating utilities on the issues and benefits of IEC 61850.
- Recommended future areas of study.

Recommendations for future R&D work on these topics are also provided.

Challenges and Objectives

Several standards are in development to address different distributed computing environments within the power industry. Among these are the standards developing for “real-time” advanced automation: IEC 61850 and those developing for back office or information system environments such as IEC 61970/61968 and Multispeak. The objective of this report is to summarize one developer’s experience in the use of IEC 61850 as well as related standards in the development of a tool.

Applications, Values, and Use

This report captures some of the issues and suggested resolution related to the implementation of IEC 61850 and related standards. These issues and proposed resolution can be presented to UCA International User Group to assist in the further development and definition of the 61850 and other related standards. The report also serves to illustrate that benchtop-level design and implementations can play an important role in identifying issues and ambiguities in standards and can contribute to the maturity and development of those standards. This report should be read by participants in development of IEC 61850 and related standards, EPRI project managers involved with Smart Grid projects, and utility personnel considering use of 61850 and related standards.

EPRI Perspective

The industry now faces issues surrounding the appropriate development and integration of key standards including IEC 61850 for field equipment as well as those developing for Back Office and information systems, such as IEC 61970/61968 and Multispeak. This project presents the results of a developer seeking to integrate across these standards and capture lessons and issues necessary to assist in both the maturity of individual standards as well as how they may integrate. Standards integration and harmonization is a key emerging topic in the ongoing development of an industry-level architecture. This work is one of two reports on IEC Standards harmonization for 2008.

Approach

The goals of the report were to document lessons learned and issues identified in the development of a design and implementation of a tool to assist the use of IEC 61850. The research captured lessons from prior and ongoing work to develop a tool kit. The contractor, Open Secure Energy Control Systems, LLC (OSECS) has been developing a Secure 61850 Toolkit and has been directly involved in designs and implementation issues related to the use of the IEC 61850 Standard. In the course of developing the Toolkit, OSECS has encountered some implementation issues and potential solutions that could assist the further development of the 61850 standard.

Keywords

Harmonization
IEC 61850
Technical issues
Common information model
Multispeak
Open standards

ACKNOWLEDGEMENTS

This report contains proprietary information that is the intellectual property of Open Secure Energy Control Systems, LLC and is used with permission.

CONTENTS

_1_ INTRODUCTION 1-1

1.5 Background On the OSECS Toolkit Development 1-2

_2_ ISSUES AND LESSONS LEARNED 2-1

Substation to Control Center 2-1

Limitation in IEC-61850...2-1

Current Proposals for substation to control center 2-2

Tendency to focus on GOOSE Messaging...2-2

OSECS Toolkit Approach 2-2

Substation Configuration Language (SCL) 2-3

Hard Wired Hierarchy 2-3

Workaround for Bay Naming...2-5

Extension to Overall Power System 2-5

Focus on Design Patterns Rather than Individual Equipments..2-5

Edition 2 draft appears focused on non-US practices 2-6

There may be multiple name versions needed for the same Logical Device (LD) 2-6

The use of IEC-61346 nomenclature is unhelpful...2-7

Proposed approach 2-7

Issues Reported but not Satisfactorily Resolved..2-8

IED parameters not exposed in object models (Tissue 179) 2-8

Status of "bay" in SCL (Tissue 286)..2-8

Ambiguous treatment of FC (equivalent abstract syntax for FC) (Tissue 287)................2-9

Presence Attribute (Tissue 295)...2-9

Web Services in 61850...2-10

W3C is an Open Standard 2-10

W3C Web Services Mapping Included in 61400-25-4 2-10

W3C has an Applicable XML Compression Standard 2-11

Benefits of 61850 W3C Web Services 2-11

A Proposal for future work on 61850 Web Services 2-12
Security and NERC CIP Standards Compliance 2-13
Identification of critical assets and critical cyber-assets (CIP-002) 2-13
Documentation and Enforcement of Access Control Policies (CIP-003 and 005) 2-13
Formalization of Categories in 61850-7-4 2-14
Simplified Implementation of Role Based Access Control 2-14
Defense in Depth (related to CIP-005) 2-15
Simplified Surveillance of Device Settings 2-15
Comparison of Common Information Model (CIM) and Multispeak 2-15
Multispeak interface to 61850 can be relatively simple 2-18
Use of 61850 at the Customer Interface 2-18
Feasibility of Using 61850 for Advanced Metering Infrastructure (AMI) 2-18
Need for Customer Communications Integration with 61850 2-18
Relation of 61850 and BACnet 2-19
Standards Processes - IEC Versus IETF 2-19
Other Issues 2-20
Only Device Identification is Reported in Self-Discovery 2-20
Need of a Fictitious Utility for Testing 2-21
Open Source Software 2-21

_3_ ISSUES IN ADOPTION OF 61850 3-1
Management and Regulatory Description of 61850 3-2
Technically-Oriented Overview and Benefits of 61850 3-7

_4_ RECOMMENDATIONS 4-1
Develop Use Cases for Tools 4-1
Follow Up Proposals for SCL and Object Model Improvements 4-1
Develop AMI and customer communications approaches based on 61850 4-1
Sponsor Needed Research, Development, and Demonstrations 4-2
Educate NARUC members and staffs 4-2
Develop reference implementation(s) 4-2
Conduct a Survey of Member Utility Naming Conventions 4-3
Develop a Fictitious Utility to Serve as Data for Testing 4-3

_A_ APPENDIX: OVERVIEW OF THE OSECS TOOLKIT PROJECT A-1
Open source components A-2

B **APPENDIX: SELECTED MATERIAL EXTRACTED FROM IETF RFC 2026/BCP-9.......... B-1**

C **APPENDIX: UNDERLYING TECHNICAL PRINCIPLES C-1**

D **APPENDIX: REFERENCES.. D-1**

LIST OF FIGURES

Figure 2-1 Example section of a wind farm feeder 2-4
Figure 2-2 Three Layer Database Model..2-17
Figure 3-1 Example of 61850 naming 3-9
Figure A-1 Overview of Toolkit Architecture A-3
Figure A-2 Workstation Functionality... A-4
Figure A-3 Example Application of Toolkit for Access Control A-5
Figure C-1 Underlying concept of the legacy technology..C-2

LIST OF TABLES

Table 2-1 Examples of Access Control Rule Expression 2-14
Table 3-1 Summary of 61850 Benefits (Management/Regulatory Version) 3-6
Table 3-2 Summary of 61850 Benefits (Technically-oriented Version) 3-11

1
INTRODUCTION

Open Secure Energy Control Systems, LLC (OSECS) has been developing a Secure 61850 Toolkit and has been directly involved in designs and implementation issues related to the use of the IEC 61850 Standard. In the course of developing the Toolkit, OSECS has encountered some implementation issues and potential solutions that could assist the further development of the 61850 standard. This report is a summary of the OSECS experience in the use of IEC 61850.

The report addresses three areas:

IEC 61850 Integration Technical Issues documents lessons learned, technical issues identified, potential solutions, and other information that will contribute to advancing the maturity and adoption of IEC 61850 in North America, hastening the maturity of 61850, improving its usability, resolving technical issues, improving its security, and promoting harmonization of related standards with each other.

The discussion is based on efforts by OSECS in developing a Secure 61850 Toolkit, and documents the lessons learned, technical issues, potential solutions, and other information in the context of those efforts. The OSECS Toolkit uses open source software and is being released under open source licensing. Toolkit development has been funded by the US Department of Homeland Security, the US Department of Energy, and internally by OSECS. An overview of the relevant OSECS efforts is provided in Appendix A.

Section II provides the results in this area. Topics addressed include substation to control center, substation configuration language, technical issues ("Tissues") reported but not satisfactorily resolved, 61850 Web Services (XML/SOAP messaging), security, NERC CIP standards compliance, comparison of CIM and Multispeak, use of 61850 at the customer interface, standards processes, and other issues such as open source software.

Standards Integration and Strategies surfaces issues and provides inputs to a white paper and other materials to educate utilities on the benefits of 61850 and its Distributed Energy Resources (DER) related extensions. The extensions include 61400-25 (for wind power) and 61850-7-420 (for other DER facilities).

Section III provides the discussion in this area. The focus in this area is on preparing educational material for two audiences:

- Minimally technical material focused on utility management and regulators, and
- Technical summary material for utility technical personnel.

An important consideration is placing 61850 in the context of the Smart Grid standards mandated in Title XIII of the Energy Independence and Security Act of 2007. The 61850 standard is recognized by many as being core technology of the Smart Grid.

Future Study Recommendations provides recommendations for future areas, especially in identifying benefits of 61850, ways of capturing those benefits, and ways of informing utilities about 61850 and related standards. These recommendations are presented in Section IV.

There are also three appendices and a list of references.

1.5 Background On the OSECS Toolkit Development

The OSECS Toolkit provides components that can be integrated and configured to build SCADA and automation systems such as:

- System for secure remote non-real-time data access
- Control system for distributed generation facilities, including wind power
- Workstation for equipment maintenance or substation local Human Machine Interfaces
- Substation and control center security appliances (application firewalls and access control gateways)
- Starter or enhanced SCADA for small utilities

The Toolkit also serves to represent a specific implementation of the IEC 61850 Standard and assist others in using the standard. Several features of IEC 61850 can be useful for developing tools of this nature and for developing well documented field equipment as well as doing some levels of quality control and meeting emerging requirements coming from the North American Electric Reliability Council (NERC).

Appendix A provides further details on the toolkit components and potential application.

2
ISSUES AND LESSONS LEARNED

This section documents the lessons learned, issues identified, proposed solutions, and other relevant information resulting from the OSECS Toolkit development activity. Areas addressed include substation to control center, substation configuration language, technical issues ("Tissues") reported but not satisfactorily resolved, 61850 Web Services (XML/SOAP messaging), security, NERC CIP standards compliance, CIM versus Multispeak, use of 61850 at the customer interface, standards processes, other issues, and open source software.

Substation to Control Center

Limitation in IEC-61850

IEC-61850, Edition 1 is formally a substation automation standard, although it was envisioned for supporting feeder equipment and other real-time environments beyond substations. Edition 1 excludes substation-to-control-center communications. However, Edition 2 is termed a utility automation standard, and substation-to-control-center is a work item. The Utility Communications Architecture (UCA), predecessor to 61850, was conceived and piloted as including substation-to-control-center communications.

Thus far in developing the Toolkit, we have encountered no technical issues that justify exclusion of substation-to-control-center communications from IEC 61850 as it exists in Edition 1. Indeed, we view the client-server profile as highly capable of supporting substation-to-control-center. At one time it could have been argued that significant use of low speed (e.g., 1200 bps to 4800 bps) communication channels is a difficult environment for 61850. The MMS mapping of 61850 is relatively verbose, and is best supported by high speed communications. There are other needs emerging for high speed communications to the substation (e.g., for video monitoring of the physical site), high speed communications are becoming more available, and there has been discussion of low speed communications offerings being withdrawn by providers.

Interestingly, 61400-25, the wind power extension to 61850, does not exclude communications with a control center. It also provides additional mappings beyond MMS, including Web Services (W3C SOAP), OPC, and 60870-5/DNP-3. The mapping to W3C Web Services supports all of the client-server services supported by 61850. The mapping to 60870-5/DNP-3 is limited in scope to services supportable by those protocols.

The W3C Web Services mapping is also relatively verbose, but W3C has on track for standardization a draft entitled Efficient XML Interchange (EXI). The EXI draft is based on technology for efficiently sending web pages to cell phones. It essentially provides smart compression based on whatever prior information, such as the Web Services Definition Language (WSDL) schema, is available and uses technology similar to gzip compression as a fallback in the absence of prior information. The WSDL schema for the W3C Web Services mapping is included in Annex A of 61400-25-4. It is entirely possible that 61850 Web Services could be supported on low speed communication channels, to the extent they remain in service.

Current Proposals for substation to control center

The current proposal for substation-to-control-center communications in TC 57 Working Group 19 is focused on harmonization of 61850 SCL and the 61970/61968 Common Information Model (CIM). The proposal uses Web Ontology Language (OWL) to map the 61850 semantics to the CIM semantics. The CIM was originally conceived as a means of allowing interface of third party advanced applications to control centers, thereby avoiding "forklift replacement" of the control centers. The approach of interfacing 61850 to control centers via the CIM suggests that the 61850 SCADA function is being treated as a third party application.

There is also discussion of a need for a "substation proxy server" to implement 61850 substation-to-control-center.

Tendency to focus on GOOSE Messaging

We have observed that demonstrations and discussions tend to focus on GOOSE messaging as the principal functionality of 61850. The client-server profile tends to be ignored. This especially applies to the interoperability demonstration at the 2006 T&D (that was based partly on planning for the TVA Bradley Substation project) and to a new product announcement made at an IEEE Power System Relaying Committee (PSRC) H6 Working Group meeting in 2008. The T&D demonstration appeared exclusively focused on exchange of GOOSE messages, and the new product announced at H6 appears to use GOOSE messaging for purposes (such as configuration, maintenance, and management) that seem more natural for the client-server profile.

The focus on GOOSE messaging and lack of focus on client server is likely related to the exclusion of substation-to-control center functionality in Edition 1. GOOSE messaging is a major intra-substation function. Inside a substation, the major use of client-server is likely to be the substation Human Machine Interface (HMI). Client-server will be much more important in substation-to-control center and wind power applications. The wind power extensions do not include GOOSE messaging, although it is available, if needed, through 61850 proper.

OSECS Toolkit Approach

The OSECS Toolkit approach has been to develop a "native 61850" SCADA application suitable for expansion into a control center. The Toolkit objects are accessed by their 61850 names. Although we have not yet developed a CIM interface, one approach to developing such an interface would be to add CIM names as attributes of the relevant objects and incorporate them into the object model. The objects have their inherent information, and the 61850 and CIM names are just means of accessing the information. The mapping essentially occurs at the object.

There is information addressed in 61850 that CIM appears to ignore and information in CIM that might not be of interest in 61850. However, it is likely in the future that it might become relevant to navigate such information. The potential ability to do so is an important feature of the combined 61850 and CIM standards.

Substation Configuration Language (SCL)

Hard Wired Hierarchy

SCL has a defined hierarchy of Substation, Voltage Level, and Bay hard wired into its definition. This has at least two serious problems:

- The hierarchy is unsuitable for wind power and is likely to be unsuitable for distribution.
- Bay remains a mandatory level even though bays are not named in North America.

In addition, the naming examples provided in 61850-6 are based on an IEC standard that is not part of 61850 and has not been generally used in North America. Utilities in North America tend to have their own naming conventions for substation equipment, and we have accommodated that practice in the Toolkit.

Unsuitable Hierarchy - A wind farm is organized around feeders that gather the power from the individual wind turbine units. Figure 2-1 shows an example section of a wind farm feeder and the associated equipment at wind farm units. The figure was taken from a paper on wind farm protective relaying [REIC2007].

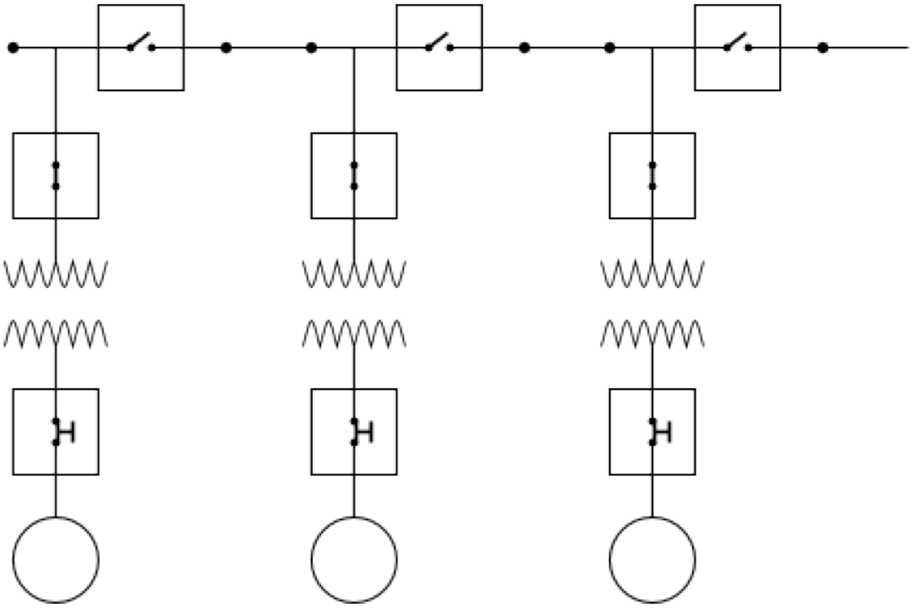

Figure 2-1
Example section of a wind farm feeder

Each turbine unit has the turbine, a protective breaker, a step-up transformer, and switches both between the unit and the feeder and along the feeder path allowing disconnect of feeder sections. The feeders themselves may be connected in either radial or looped configurations to a central point. The feeder will have one or more breakers providing protection at the central connection. The wind farm may have a substation-like facility providing VAR compensation, and a substation at which it connects to the Area Electric Power System (AEPS). In some examples, the substation has a ring bus configuration.

The resulting hierarchy should be as follows:

- Wind Farm
  - Feeder
    - Wind Unit
      - Voltage Level
- Substation
  - Voltage Level
    - Bay (if required)

A similar consideration likely applies to distribution.

Bay as Mandatory - The Bay level remains mandatory in 61850. Although North American utilities recognize bays in substation design, it is not their practice to name bays or to use devices such as bay controllers. Although workarounds are possible (and we discuss one below), 61850-

6 requires that the bay be named and that its name be at least one character. In the CIM, bay is an optional hardware level, supporting conformance to North American practice.

Workaround for Bay Naming

In 61850-6, Bay is a mandatory level, and the bay name is required to be at least one character. In our naming software, we include provision for an optional pre-specified name, and in the related examples the name is an underscore ("_"). Thus the single bay associated with the voltage level "ROANOKE_132KV" has the name "ROANOKE_132KV_", with the underscore serving both as the bay name and as a separator for the remainder of the equipment or connectivity node name.

Extension to Overall Power System

We went beyond the 61850-6 standard in using the overall power system as the root node of the SCL file. This has the effect of not limiting a single SCL file to a single substation. This simply requires making the individual substation SCL a child of the overall power system SCL. (Perhaps it also requires redefining the SCL acronym to be "System Configuration Language".)

This approach has the following advantages:

- It places the overall power system configuration in a single file. Extraction of individual substation files is straightforward, if necessary.
- It allows both ends of lines to be included in the SCL as two-terminal line (LIN) objects, rather than requiring each end of a line to be included separately in each endpoint substation as a one-terminal "infeeding line" (IFL). This provides advantages, including:
  - Providing information needed for determining overall topology
  - Providing information that relates the named line with its associated electrical equipment (breakers, switches, connectivity nodes) and monitoring/control equipment. As discussed below, this in turn provides information related to CIP reporting.
- It allows the SCL file to be used not only for individual IED configuration but also for SCADA master or control center configuration.

Focus on Design Patterns Rather than Individual Equipments

Rather than focusing on individual equipments in developing the substation section of an SCL file, we found it useful to focus on design patterns. We define a design pattern as a collection of equipment used together in a design. We initially used the substation designs described in the Rural Utility Service Substation Design Guide [RUS2001], that include breaker-and-a half, double-bus-double-breaker, main and transfer bus, segmented bus, single bus with bypass switch, and ring bus. The individual wind unit configurations shown in Figure 2-1 also form a design pattern.

In certain cases, such as main and transfer bus, we separated an individual design pattern into two patterns, a basic pattern and another pattern. For example, the transfer breaker configuration of the main and transfer bus pattern is treated separately.

Edition 2 draft appears focused on non-US practices

The latest draft of SCL (61850-6) for Edition 2 appears to be focused on non-US practices in facility acquisition. The document assumes that the IED configurator is a manufacturer-specific or IED-specific tool. It is certain that the operation of translating the SCL into IED internal information and loading that information into the IED will need to be manufacturer-specific or IED-specific. However, it is feasible for the tool used to configure and manage the SCL itself to be usable across multiple manufacturers and IEDs.

The non-US tendency is to acquire facilities from single manufacturers on a turnkey basis with maintenance included. This practice is fully supported in the Edition 2 draft. The US tendency is for the utility, in combination with a third-party integrator, to design, integrate, and maintain the facility, and for the facility components to be from multiple manufacturers. The Edition 2 draft does not clearly support this practice.

There may be multiple name versions needed for the same Logical Device (LD)

Although the IED is named in SCL, it is not included in the model of 61850-7-2. Only the server associated with the IED is included in 61850-7-2, and it is not explicitly named but is identified through its communications attributes/objects (addresses and associations). The first level that is named inside the IED is the logical device (LD). There is an attribute of the IED available in SCL indicating whether the LD names are configurable through SCL or if they are fixed and non-configurable. (There is also an attribute that indicates whether LN prefixes and instance numbers can be configured through SCL.) A list of LDs in an IED can be obtained by a GetServerDirectory request, and a list of LNs in an LD can be obtained by a GetLogicalDeviceDirectory request.

The full path name of a logical device is intended to be the concatenation of the LD name as prefixed by each parent in the device hierarchy. These parents include the IED and may include various levels of the equipment hierarchy. The full path name is capable of identifying the LD in the overall system. There is sufficient space defined in the object format to accommodate a full path name for an LD, which is also part of the object reference for every object in the LD. However, there are at least three names for the LD that may be applicable:

- The LD name as configured into the actual device. This name is the one that provides navigation within the device. It is also the one returned by a GetServerDirectory request. This is the only name that is meaningful to the actual device. If the LD name is not configurable through SCL, it will be the same for all IEDs of the same manufacturer and model.

- The LD name as known within the overall power system. This name must be unique within the power system. It can include the IED name, substation or other facility name, or other information. It may be configured into the IED or may only be known outside the IED.
- A temporary name identified in an SCL file and intended to be, but not yet, configured into the IED, assuming such configuration is allowed.

The IED and equipment parent names may be useful in setting up routing to the IED server, but with proper functioning of the message routing the system will work even if the LD name is not the full LD path name. However, a control center, maintenance center, or other facility must identify the LD by its full path name to avoid confusion with other instances of the same type of IED elsewhere in the system. Accordingly, unless there is a practice of acquiring only IEDs that allow LD name configuration and of loading every LD with its full path name, it is likely that there will be two name versions maintained in any overall system: the full path name as identified for the system, and the local device name as configured into the IED.

The use of IEC-61346 nomenclature is unhelpful

IEC-61346 is a standard for naming equipment in a power system (or in any system). It is not a part of IEC 61850 but falls under Industrial Systems generally, although it is used in most of the examples in IEC-61850-6, the SCL volume.. It has not been generally used in North America. The names are letter/number combinations such as E1Q1SB1. North American utilities tend to prefer more descriptive nomenclature. IEEE PSRC WG 10 recently began considering the use of the standard for naming IED's. However, the standard identifies equipment without providing the kinds of information that North American utilities have become accustomed to including in their equipment names. Limitation of examples in the standard to IED names conforming to IEC-61346 is unhelpful. We would recommend conducting a survey of North American utility naming practices and providing some examples in the 61850 documents based on those practices.

Proposed approach

Our proposed approach to accommodating wind power and other kinds of systems in 61850 SCL would be to change the tag for all facility levels to "Facility" and to add an attribute "type" to the "Facility" element using an enumeration of the kinds of facilities allowed. These could include the following:

- Substation
- Voltage Level
- Bay
- Wind Farm
- Wind Unit
- Feeder

- Power System

The only constraint on the hierarchy of facilities would be that Power System should be at the root. Header information could be placed at the highest and second highest levels of the hierarchy. Thus, both Power System and Substation could have headers, allowing the Substation section to be broken out for compatibility with present SCL in those cases where the present hierarchy is preserved. All levels would be optional and they could be mixed as appropriate for the power system involved. Backward compatibility with Edition 1 SCL could be accomplished by replacing the tag of "Facility" elements with the "type" attribute.

Issues Reported but not Satisfactorily Resolved

The following items reflect Technical Issues ("Tissues") that were posted to the Tissues web site (http://tissues.iec61850.com) as a result of Toolkit development activities but did not result in satisfactory changes to the standard. In each case the issue raised is described together with the proposed solution and response from the relevant working group. This may be followed by a comment reflecting our views on the response.

IED parameters not exposed in object models (Tissue 179)

Issue as posted: This expands the issue raised in Tissue 139. There are several parameters resident in the IEDs that are not exposed via the object models in Parts 7, 8, and 9, although they are managed by SCL in Part 6. These include the clients to which reports are to be addressed, the maxima of allowable data sets and reports, and identification of whether certain data values are settable by the client.

These parameters may be needed by clients. For example, in Part 10 there are tests specified to determine that service errors are issued in response to attempts to exceed the maximum numbers of data sets and reports. However, the only way a client can discover whether an attempt might exceed the maximum is to make the request and see if a service error results.

It would be better to expose such parameters to the client through the object models and the normal discovery process rather than forcing discovery by trial and service error.

Proposal as posted: Include the relevant parameters in the object models of Parts 7, 8, and 9.

Response: None

Status of "bay" in SCL (Tissue 286)

Issue as posted: “Bay” is a required element in SCL, although it is not required elsewhere in 61850. However, 61850-2 states that “The concept of a bay is not commonly used in North America” and bay is effectively an optional element of the CIM (because it allows "0..." bays). This complicates harmonization.

Proposal as posted: Make "bay" optional in SCL.

Response: "In contrast to CIM, where 'Bay' is an object, a bay in 61850 is just a level in the naming hierarchy. If this is not needed, then e.g. the last character of the voltage level name can be taken as name of one fictive bay. This means that although the bay level is mandatory, it does not need an own name. This has already been accepted world wide for the current IS."

Comment: As discussed above, the hierarchy needs to be changed to accommodate wind power and distribution. The CIM may also need to be changed for the same reasons. In both 61850 and CIM the hierarchy levels need to be more flexible and levels such as bay need to be optional.

Ambiguous treatment of FC (equivalent abstract syntax for FC) (Tissue 287)

Issue as posted: The document leaves to SCSM's the definition of concrete syntax for expressing the functional constraint in an FCD or FCDA. This effectively creates no abstract syntax for such expression. Some diagrams and other discussions in the document express it as "[FC]" inserted in the data reference, and this expression was also recently used in a conference presentation.

Proposal as posted: Define an abstract syntax for FC in FCD's and FCDA's or otherwise clarify its expression.

Response: "IEC 61850 does not specify concrete syntax. FCs in 61850 are listed; no abstract syntax is required."

Comment: The role of FC remains difficult to systematically include in discussion of 61850. FC is either part of the data reference or it is a separate attribute of the data and not part of the data reference. There needs to be a systematic, standard way to discuss data references and FC. This does not yet exist.

Presence Attribute (Tissue 295)

Issue as posted: What is the purpose of the "presence" attribute? It is defined in 7-2, but 8-1 does nothing with it, and it is not managed or supported in the SCL of Part 6.

Proposal as posted: Explain its purpose further (including why it is defined but not actually used), use/manage/support it, or delete it.

Response: "The meaning of the 'presence' attribute is explained in 7-2 clause 5.5.1. As it indicates if a data is optional or mandatory, it is not contained in SCL, because SCL types only describe existing (instantiable) attributes, not optional ones. If you want to extend the SCL usage to describe class definitions inclusive optional attributes, you can use the SCL extension defined in part 6 annex C.2, where the 'presence' attribute is called mop (mandatory / optional / private)"

Comment: The presence attribute is not the same as m/o/c or m/o/p. It is a Boolean. The abstract syntax implies that it is to be transmitted over the wire. The value of the Boolean to a client is unclear. If sent over the wire, it conveys the information that the data being sent is mandatory. The object is clearly present, because it is being sent. The only possible use of the Boolean would be that if set to "False" the client would know that processing of the data was not mandatory on the receiving side of the communications link. The value of such information is dubious.

Web Services in 61850

Both the OSECS Toolkit and the 61400-25 wind power standard include mappings of 61850 objects and services to W3C Web Services. The following paragraphs discuss the use and benefits of W3C Web Services in 61850.

W3C is an Open Standard

There appears to be some confusion in the IEC TC 57 community when discussing Web Services, which are on the IEC TC 57 roadmap for future development. When people in the IEC TC 57 community talk about web services, they often appear to assume that Web Services is synonymous with Object Linking and Embedding (OLE) for Process Control, also known as OPC. OLE is a Microsoft proprietary feature of the Windows operating system. For several years the OPC specification required a legal agreement prior to access. Recently, some aspects of the OPC specification have been moving toward publication as an IEC standard. However, it is highly likely that critical functions needed for implementing OPC are encumbered by Microsoft patents. It is unclear to what extent it would be possible for a third party to openly implement OPC without permission flowing from Microsoft through some organizational chain.

The web standards of the Internet are promulgated by the World Wide Web Consortium (W3C). Although W3C is a membership consortium of corporations, its standards are openly published, widely accepted, and unencumbered by enforced patents or royalties. The Web Services standards are W3C standards, including SOAP, XML, and others. There is a related organization known as the Web Services Interoperability Organization (WS-I) that promulgates standards and best practices that fill in certain gaps in the W3C Web Services standards.

As used in this report, Web Services refers to the W3C Web Services standards.

In addition to the standards themselves being openly published, there are open source implementations of the W3C Web Services standards for a variety of languages such as C/C++, Java, Python, and PHP.

W3C Web Services Mapping Included in 61400-25-4

The wind power extension to 61850, IEC-61400-25-4 provides a mapping of most of 61850 to W3C Web Services in its Annex A. A few services have been added, and a few (primarily related to GOOSE and SMV) are not included. OSECS developed its own alternative implementation of 61850 Web Services that differs from the 61400-25-4 Annex A version in the following ways:

- Web Services must be bound to a protocol for message transmission. The most common protocol for Web Services is HTTP, which is a request/response, client/server protocol. Only a client can initiate a request. For handling unsolicited reports, the 61400-25-4 client sends a request to be filled by the next unsolicited message and renews the request each time it receives a message. The OSECS implementation also optionally supports a client at the server and a server at the client for handling unsolicited messages.
- Each W3C Web Services message includes a header and a body, intended as support for a layered architecture. The header can be used for some functions defined under the W3C WS-Addressing standard, a companion to the Web Services standards. These purposes include providing a UUID to identify the message and a destination address identifying a final recipient (for systems in which there might be multiple recipients). The destination address allows switching of messages to the proper recipients at the application level. The OSECS implementation supports WS-Addressing. The 61400-25-4 Web Services places the same information in the message body, defeating the layering in the message structure. It is reasonably straightforward to use WS-Addressing until the final link to the device and then move the relevant header information to the message body. However, this is an extra processing step.

W3C has an Applicable XML Compression Standard

Web Services is a relatively verbose protocol, as is much of XML. This has created a barrier to adoption in applications having bandwidth or storage limitations.

As previously stated, the W3C has a draft XML compression standard called Efficient XML Interchange (EXI) moving toward adoption. The Last Call draft was issued in September 2008. An open source Java reference implementation has been initially released.

The EXI standard is based on existing technology for transmitting web pages to cell phones. The technology was provided on a royalty free basis to the W3C. As part of the development process for the EXI standard, performance tests were run and documented. The performance test document claims that EXI provides significant performance improvement over two alternatives, including gzipped XML and ASN.1 with Packed Encoding Rules. The implication is that EXI may possibly enable 61850 W3C Web Services to be used over communications lines having limited bandwidth.

Benefits of 61850 W3C Web Services

There are several benefits that would be provided by formally mapping 61850 to W3C Web Services (such as in a 61850-8-2):

- **Wide use and availability of software.** Web Services technology is widely used and readily available. The technology is available in both open source and proprietary products. Hardware modules are also being developed based on the open source Apache web server.

- **Broader base for support and improvement.** The other alternatives are mostly specialized protocols for electric power and process control SCADA. Web Services technology is more widely used and has a larger community interested in its support and improvement.
- **Increasing availability of suitable bandwidth telecommunications offerings.** Some of the other alternative communications methodologies are primarily designed for low speed (e.g., 2400 bit per second) multidrop communications lines. With increasing availability of broadband, and low-cost 56 kilobit modems available for use over voice-grade lines, it is becoming much easier to find suitable bandwidth for supporting Web Services technology. In addition, the EXI compression technology will eliminate the issues of bandwidth by enabling lower bandwidth Web Services.
- **Potentially easier enterprise integration.** The SOAP protocol and Web Services are XML-based technologies. CIM is an XML-based technology. Multispeak is also an XML-based technology and it specifies SOAP as a communication protocol.
- **Feasibility of avoiding use of routable protocols**. The "need" for avoiding routable protocols is based on a misunderstanding of the NERC CIP standards. CIP-002 requires that Critical Cyber-Assets use a routable protocol for the other CIP requirements to apply. Some misunderstand this to mean that routable protocols have been “outlawed” or that non-routable protocols are more secure. Based on FERC Order 706, that included an order for NERC to revisit this provision, the exclusion of non-routable protocols is likely to disappear or be significantly modified within a few years. However, the misunderstanding is common. Because the Web Services technology provides its own application-layer message switching support, it is feasible to operate a 61850 system in the client/server profile using a Web Services mapping and without using TCP/IP. This can be done by simply using an older point-to-point protocol that doesn't include routing capability, e.g., between a substation gateway and a control center, and using the WS-Addressing to direct the communications to the proper device association within the substation.
- **Eliminates dependence on OSI stack** - W3C Web Services use the Internet Protocol Suite and eliminate the need for using the ISO Open System Interconnection protocol stack. The electric power industry is one of the last users of the OSI technology, which was abandoned by most, if not all, other users in the 1990's. Only a few of the OSI-related technologies, such as ASN.1, are still being developed and maintained. A few documents referenced in 61850 are no longer available from the standards development organizations that created and standardized them.

A Proposal for future work on 61850 Web Services

We would propose that a 61850 Web Services mapping be formalized (e.g., as 61850-8-x) based on W3C Web Services. This suggestion can also be found in a report and briefing that resulted from the European Commission sponsored “Service Infrastructure for Real-time Embedded Networked Applications” (SIRENA) project [SIRE2005 and JAMM2005]. The mapping should offer EXI as optional compression functionality.

Security and NERC CIP Standards Compliance

Security and related NERC CIP standards compliance are facilitated in several ways by 61850. The following describe some of these approaches:

Identification of critical assets and critical cyber-assets (CIP-002)

As an ancillary part of the Toolkit, we developed an approach that appears to simplify identification of critical assets. The approach first requires the identification of critical lines, which can be done using power flow contingency analysis methods. Our focus on design patterns in developing SCL files then suggested that analysis of the design patterns associated with critical lines can then identify the critical equipment assets.

Once critical assets have been identified, the Substation section of a 61850 SCL file identifies the critical cyber assets. These are just the IED's containing the LN's that monitor or control the critical equipment assets.

Documentation and Enforcement of Access Control Policies (CIP-003 and 005)

IEC-61850 naming facilitates and simplifies the expression, enforcement, and documentation of access control policies required under CIP-003 and 005. It has the additional advantage that the files prepared to express the policies can be used for preparing the data used in enforcing the policies. This provides traceability between the articulation of the policies and their enforcement. The files used for expressing and enforcing the access control policies can also serve as the required CIP documentation.

The naming hierarchy in 61850 includes:

- IED/Server
  - Logical Device (LD)
    - Logical Node (LN)
      - Common Data Class (CDC)
        - Common Data Attribute (CDA)

Naming down to the level of LD, i.e., before the slash ("/"), is utility specified. Naming after the slash is standardized. The LN name can be preceded by an alphanumeric prefix and must be followed by a numeric suffix. The first letter of the LN name indicates a category of monitoring and control. For example, LN names beginning with P indicate protective relays, R indicates protection-related functions (such as event recorders), M indicates metering and measurement devices, and X indicates switchgear.

In addition to the LN name categories, the data categories found in the 7-4 tables, the functional constraints, and utility-determined characteristics of the utility-specified parts of the names can be used as elements in security policy rule construction.

The following table provides some examples of how this can be used.

Table 2-1
Examples of Access Control Rule Expression

Desired rule	Expression using 61850 naming
Only protection engineers are permitted to change settings on protective relays and protection-related devices	Only protection engineers have permission to write to settings for LNs having names beginning with P or R.
The only access permitted to Energy Accounting personnel is read access on metering devices.	Energy Accounting personnel are limited to read access on data from objects in LNs MMTR and MSTA.
Only personnel from a specified geographic division of the utility are permitted to change settings on equipment in certain substations.	Incorporate the substation name or geographic division name in the utility-defined part of the LD name and use that as the basis for expressing the rule.
Only personnel participating in a certain project are permitted to access certain data on certain devices.	Establish a role for the project personnel and provide a list of the data names.

Formalization of Categories in 61850-7-4

There are categories of data identified in 61850-7-4 that are useful in defining access control policy. These are the categories that are shown as headings such as Settings and Measurements, but are not treated in the standard as attributes of the objects. Several functional constraints can be found in the objects under the Settings category, so use of functional constraint as a selector is insufficient to cover everything identified as settings. There is some effort to formalize these categories in Edition 2 as attributes of the objects. These efforts should be encouraged and expanded.

Simplified Implementation of Role Based Access Control

IEC-61850 simplifies the implementation of Role Based Access Control (RBAC). The RBAC in the OSECS Toolkit is located in the part of our system where the message is XML format related to Web Services. The relevant object name can be located in the message and looked up in the access control database to determine permissions allowed for the object.

Although RBAC is currently a work item, we believe that by proper consideration of the underlying objects, most RBAC permissions can be reduced to “read” and “write”. The major change in viewpoint required is to think about directories as objects. A “create” function becomes a directory write. It may be necessary to expand the list of permissions slightly, but it can remain relatively small.

Defense in Depth (related to CIP-005)

IEC-61850 facilitates defense in depth, which is not currently in the CIP standards, but is required to be included in CIP-005 under FERC Order 706. Among the possible defenses are encryption, firewalls, role-based access control, surveillance of device settings, and intrusion detection. All of these defenses are facilitated by 61850.

In addition to the defenses facilitated by 61850, the Toolkit adds a operating system security through its implementation on two Linux platforms, one protected by Security-Enhanced Linux and the other protected by AppArmor. Security-Enhanced Linux was originally developed by the research division of the US National Security Agency, and was provided on Linux as a technology transfer project. AppArmor uses the same kernel interfaces as Security-Enhanced Linux but is easier to configure because it omits the file labeling functionality needed for military multi-level security (enforcement of rules related to hierarchical security designations such as Confidential, Secret, and Top Secret).

Simplified Surveillance of Device Settings

One approach to providing protection against device tampering is to periodically or randomly download selected device settings and compare their values to a database of approved and expected settings. Any change found would be cause for investigation. Performing this surveillance with 61850 only involves scheduling GetDataValues requests on the selected settings and performing comparisons against the database.

Comparison of Common Information Model (CIM) and Multispeak

The 61970/61968 Common Information Model (CIM) and Multispeak represent two common alternative views of enterprise integration and cross-enterprise interoperability in corporate information technology environments. The CIM is a top-down approach and Multispeak a more bottom-up approach. Each has important historical conceptual predecessors.

Harmonization of CIM and 61850 will require resolution of interface issues that arise because of differences in the design perspectives of their information models. These differences are based on the technical drivers in the requirements on which they are focused. CIM is focused on exchange of information models and related data between corporate information systems. The underlying requirement of 61850 is on exchange of data with field devices. Factors that are important in one context may be relatively unimportant in the other. For example, in exchanging power flow model data, the identity of the field device that produced a data value is of minor interest. This especially applies if the power flow processing has been front-ended by a state estimator that statistically consolidates the measurements from whatever field devices may be relevant to the particular data value, minimizing the effects of device failure. However, in collecting the data value from the device, the identity and health of the device are very important.

By contrast, harmonization of Multispeak and 61850 is relatively simple. Multispeak is fully capable of being extended to simply convey whatever 61850 objects need to be exchanged. The ongoing efforts to foster interoperation of CIM and Multispeak could provide insights that aid in harmonization of CIM and 61850.

Two alternative views of enterprise integration

The predecessors of the CIM are a three-layer database architecture concept circulated in the standards community in the late 1980's and the more recent Semantic Web. The three-layer database model is depicted in Figure 2-2. The physical layer contains the storage of the database, with all the detailed functions necessary to manage that storage. The enterprise layer contains an overall data model of the enterprise, encompassing all the data managed in the enterprise. The application layer contains views that are accessed by individual applications to perform their functions. The CIM essentially reflects the data model at the enterprise layer.

CIM grew out of efforts to enable third party applications to be added to control centers, hence the early name of Control Center Application Program Interface (CCAPI). The functionality needed to accomplish this interface turned out to be easily extended to numerous other interfaces in the utility enterprise.

CIM has a more recent predecessor in the Semantic Web and directly uses many of the concepts and tools developed for the Semantic Web. The underlying concept of the Semantic Web is to enable search of all knowledge in a particular domain and retrieval of all knowledge within the domain on some topic. Some concepts of the Semantic Web have their roots in Library Science, such as the Dublin Core, a generalization of the concepts in a library "card catalog." The historical roots of the Semantic Web are in library cataloging systems such as the Dewey Decimal System and the Library of Congress Numbering System.

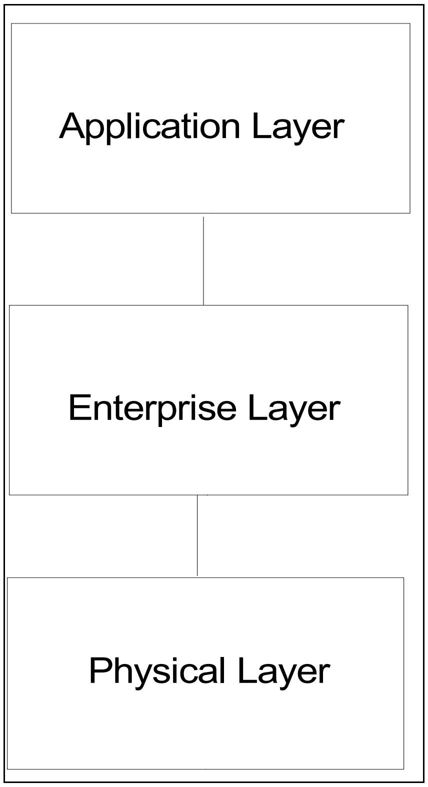

Figure 2-2
Three Layer Database Model

Another example application of the Semantic Web is an effort by the council of US Federal government agency Chief Information Officers to develop a common structure for all information held by US Federal agencies. This information can include items as diverse as moisture content of soil samples from Mars, number of private aircraft taking off and landing at the Van Nuys, California airport, rules for tax treatment of certain commercial transactions and employee benefits, revenue by state and county of businesses in industry classification code 311520 (Ice Cream and Frozen Dessert Manufacturing), and descriptions of exhibits at the Harry S. Truman Presidential Library. The concept underlying the Federal CIO Council application of the Semantic Web is to put information of this range of diversity into a common database structure and to enable searching of the entire database through a common portal. An electric power enterprise does not have the broad information diversity of Federal agency data holdings, but the underlying technology of CIM is focused on accommodating that level of diversity.

Multispeak is essentially an application of Electronic Data Interchange (EDI) within the electric power enterprise. The historical roots of EDI are in the commercial telegraph codes developed in the 1800's to express specific commercial transaction information in minimal characters. In the late 1960's the Transportation Data Coordinating Committee (TDCC) was formed to standardize business documents related to purchasing, shipping, and delivery of goods. The TDCC could not standardize the internal databases of businesses, that might span industries as diverse as grocery, construction, electric power, and automobiles, but they could standardize documents such as bills of lading that are used in shipping goods for those industries. The TDCC work became the ANSI X.12 series of standards, and later the concepts grew into a much more diverse and extensive collection of EDI standards promulgated by a variety of organizations.

The basic principal of EDI is to define the documents needed to accomplish specific information flows between entities without attempting to define the internal handling of those documents within the entities. Multispeak has identified several entities within the electric power enterprise, such as the SCADA, Outage Management System, Engineering Analysis, Customer Billing, and others. A Multispeak message is essentially a business document defining a specific exchange of information between a pair of these entities. The standard is relatively flexible, and new information exchanges can be added as the requirements arise.

Multispeak interface to 61850 can be relatively simple

Multispeak defines W3C Web Services as its communication methodology. The flexibility of Multispeak is such that selected 61850 data definitions, as expressed in the SOAP mapping of 61400-25-4, could be added directly to the Multispeak data exchanges for SCADA and other relevant electric power enterprise entities. The mapping could take place either at the SCADA or at its communicating partners. Alternatively, the 61850 data could be mapped into existing Multispeak messages.

Use of 61850 at the Customer Interface

Feasibility of Using 61850 for Advanced Metering Infrastructure (AMI)

Based on a status report at the 2008 Grid Week conference, the focus of AMI standardization activity is on use cases and other requirements. The communications technology currently being implemented tends to be proprietary, implying the use of proprietary data models as well. It is eminently feasible to model the data for AMI using 61850. It is also feasible to communicate the data using Web Services technology. The impending availability of EXI enhances the feasibility of efficient Web Services communication of AMI data.

Need for Customer Communications Integration with 61850

Many of the distributed resources intended to be controlled using 61850-7-420 are likely be in homes and commercial buildings. Unless two separate communications systems are built, one for customer communications and the other for distributed resources, it will be necessary to integrate customer communications and the distributed resources control. This combined technology is critical for development of the Smart Grid. Integration will also allow commonality of security technology throughout the grid.

Looking forward, it is likely that the requirements for both AMI and distributed resources will evolve. The most flexible technology available for handling evolving requirements is 61850.

Accordingly, 61850-7-420 is the best technology for future implementation of distributed resources and it should be integrated with a 61850-based collection of objects for AMI.

Relation of 61850 and BACnet

There is a historical relationship between 61850 and BACnet, the technology developed by ASHRAE for energy management in commercial buildings. The 61850 technology is derived from the EPRI-developed UCA. Some of the underlying concepts of UCA and BACnet are related. This makes it possible that a 61850-based AMI can be easily integrated with BACnet, to the extent such integration may be found useful during future evolution of the Smart Grid.

Standards Processes - IEC Versus IETF

The process followed by the standards developing organization (SDO) has a significant impact on ambiguity and interoperability. In many of the standards prepared by SDO's such as IEC and ISO, the technology is well known and the purpose of the standard is to gain the benefits of specifying a common set of practices. These practices include dimensions of parts that need to fit together, environmental conditions, measurement conditions, nomenclature, electrical characteristics, and a variety of other aspects where simple agreement on a common specification is very useful. These standards require little or no research/development to ensure that they are feasible, valid, and unambiguous.

By contrast, standards for information and communications more often involve development of new technology or system designs and require standardization to ensure interoperability. These standards often contain data structures, data representations, logic, and implied software functionality. Research and development are required to ensure that the data structures and representations, logic, and implied software functions are feasible, unambiguous, and meet the needs of the intended applications. Issues in such standards usually surface only during attempts to implement them for appropriate applications.

The processes followed by IEC and ISO are much more suitable for traditional standards than they are for standards involving information and communications. The effect is to have a process in which a standard is first developed and adopted, and is then followed by efforts to make the standard work.

One example was the ISO Open System Interconnection family of standards. After adopting the standards, ISO set up three OSI Implementers' Workshops in different parts of the world. One such Workshop was established at NIST. The Workshops prepared a variety of implementers' agreements and other memoranda addressing interoperability issues, ambiguities, and needed changes in the standards.

The comparable effort for 61850 is the Technical Issues (Tissues) web page. There are over 600 Tissues lodged against 61850. Although some of these are suggestions for future technical improvements, most involve errors, ambiguities, or interoperability issues in the adopted standard. Tissues lodged against 61850 Edition 1 are being considered in drafting Edition 2.

By comparison, the Internet Engineering Task Force (IETF) develops standards that are exclusively focused on information and communications. IETF requires that two reference implementations built on different code bases be demonstrated as interoperable before they will promote a proposed Internet standard to the status of a draft standard. They also take steps to ensure that the reference implementations are openly available and usable by implementers. Any functions or features of the proposed standard that do not interoperate must be removed from the proposed standard before it becomes an official draft.

An extract of the relevant provisions of IETF RFC-2026 is provided in Appendix B.

A reference implementation[DALC2003, CURR2003]:

- Is used as the definitive interpretation of the standard or specification
- Enables discovery of errors and ambiguities, and demonstrates the implementability of the standard
- Serves as the "gold standard" for testing other implementations and developing conformance test suites
- Helps to clarify the intent of the specification where conformance tests are inadequate

Reference implementations often accompany software specifications and standards, and are usually released under open source licenses.

Other Issues

Only Device Identification is Reported in Self-Discovery

Although 61850 provides a form of self-discovery, it does not provide complete information on the objects being discovered. In particular only the monitoring and control device identity is reported during self-discovery. For example, an MMXU logical node in an IED can be identified as reporting the magnitude of the Phase B voltage at some connectivity node. However, without further practices outside the 61850 standard itself, the identity of the connectivity node being monitored will not be available.

The SCL may contain information on what power system object is being monitored or controlled by each Logical Node. However, there is no standardized place in the device for that information to be provided. Each LN has an optional description object with sufficient space (255 characters) to provide the name of the corresponding power system object. It is possible for a vendor or a utility to establish a convention that the name of the related power system object be included in the LN description. However, there is neither a guarantee nor a reason to expect that the power system object identification will be supplied.

Need of a Fictitious Utility for Testing

OSECS found that to test the functionality of tools for 61850, it needed data from a fictitious utility. Data from a real utility could neither be requested nor used because it is now regarded as Critical Infrastructure Information. OSECS constructed a simplified version of such a fictitious utility by extending the IEEE 30-bus Power Flow Test Case. The test case provides names for its substations, and was extended to include details of substation configurations and example naming conventions for substation equipment. This allowed testing of tools that create names for substation equipment and monitoring/control objects based on utility-defined and 61850-standardized naming conventions.

Open Source Software

Open source software is substantially a product developed and maintained by voluntary communities. Some people have the impression that the main open source communities are composed of hobbyists. However, it is useful to understand the structure of the open source community, because there is major participation by commercial firms, academia, and government.

Some projects are initiated by an individual, others are developed and maintained by much larger and more organized groups. Many major open source projects are funded by commercial organizations or are organized to maintain and improve software that was formerly proprietary and has been released as open source. Commercial organizations that have made major commitments to supporting open source include IBM, Red Hat, Oracle, and Sun. The operating system security functions (Security Enhanced Linux) used in the Toolkit were originally developed by the National Security Agency of the U.S. Department of Defense, and NSA personnel continue to participate in its maintenance and improvement.

Projects generally have an infrastructure, often provided by sourceforge.net, and usually including:

- Packaged releases in formats such as tar.gz, rpm, deb, and others
- A software repository, usually based on a configuration management tool such as CVS, Subversion, or more recently GIT
- An email list for development and support discussions, often with web archiving
- A bug tracking tool, such as Bugzilla, for formal entry and tracking of bug reports and improvement requests
- Sometimes a chat room or web forum for development and support discussions
- Documentation

Lessons learned thus far in the project in the area of open source software include:

- Open source security software often ranks among the best-of-breed for various functions.

- There are numerous languages popular for programming in open source software, including C/C++, Python, Java, Perl, and others. The Toolkit uses C/C++ and Python (which has facilities for relatively easy integration of C and C++ code). Communities usually develop around languages. Within a language community there are sometimes multiple open source projects addressing a given area of technology.
- Each open source project has different goals, approaches, strengths, and weaknesses. Available software frequently has pitfalls. Functionality may be incomplete or erroneous. The original developers were "scratching an itch." Some functions and features important to a potential user looking at the software may not have been important to the original developer community. As in any community of volunteers (including IEEE itself) making a suggestion often results in an invitation to implement the suggestion. Identifying and evaluating each potentially-useful open source component project is a time-consuming but important activity in building a system using open source software.
- Selection of open source software requires particular care to avoid selecting dead-end software. It is especially important to assess the scope and activity in the community of users and maintainers, and to look at factors such as the activity on discussion lists in order to ensure that the software is still being actively maintained and improved.
- As described by Rosen [ROSE2005], there are two main kinds of Open Source licenses, the academic (with minimal conditions on use of the source code) and the reciprocal (requiring that derivative works be made available under the same terms as the original work). The major reciprocal license is the GNU General Public License (GPL), published by the Free Software Foundation (http://www.fsf.org). Under the terms of the GPL, if any significant GPL code is used in a program, all linked programs must be licensed under the GPL if they are distributed to others. However, this does not apply if a program is a "separate work," and is linked by interfaces used for separate programs. Thus a GPL program can only be interfaced to program that is not GPL or GPL-compatibly-licensed by means such as files, pipes, and messages, ordinarily used for interfacing separate programs. This creates a constraint on architecture that must be carefully managed. However, with care it is feasible to integrate GPL-licensed software applications into otherwise non-GPL systems.
- One alternative frequently found is "dual licensing." This is the practice of releasing software under a GPL license and also offering it under a commercial license without the GPL restrictions. The licensing of MySQL is an example. This approach requires careful management by the copyright holder, if contributions by others are considered for inclusion in the software.

3
ISSUES IN ADOPTION OF 61850

Although the 61850 technology was originally developed in North America by EPRI, the standard is far less popular in North America than it is elsewhere in the world. While over 55% of the world's utilities are planning near term implementations, only 17% of North American utilities are planning to do so (from data in [NEWT2007]).

Based on reports from North American pilot tests of 61850 [HOLB2007] and remarks by utility personnel at industry meetings, we believe the differences in adoption rates are attributable to differences in acquisition and maintenance policies between North American electric utilities and those elsewhere in the world. The utilities that are rapidly adopting 61850 tend to acquire substations as single-vendor turnkeys, including lifetime maintenance. The vendor who supplies and maintains the substation is usually the manufacturer of the substation equipment.

Utilities outside North America immediately capture the benefits of reduced costs in substation wiring and configuration. This reduces the initial acquisition costs of the facilities. There are no costs of transition to 61850, such as for personnel training, because the vendors perform the maintenance. They don't use 61850 for communications between the substation and control center, so there are no further impacts.

North American utilities tend to prefer to have more control over the design and maintenance of their facilities, and to avoid vendor lock-in. Although they may outsource portions of facility design and maintenance, they want to have their own people involved in those activities. They also tend to prefer having facility equipments supplied by multiple manufacturers. This leads to a need for tools that enable integration of heterogeneous equipments. Such tools have not been available for 61850.

For North American utilities, the initial savings in substation wiring and configuration are offset by transition costs such as training personnel to perform maintenance of 61850-based equipment. In the absence of tools for capturing the other benefits of 61850, North American utilities do not see the value of transition.

The potential benefits of 61850 are numerous and far-reaching. However, they require several actions to make them practically realizable:

- Tools must be provided to facilitate capture of the benefits. these begin with a need for tools to enable integration of heterogeneous equipments and extend to tools that enable capture of other benefits.
- Utility executives and regulators must be educated to understand the benefits of transition to 61850 and to consider the significant benefits that are either non-quantifiable or difficult to

quantify based on available models. Quantifiability is an issue because the regulators recognize that ratepayers will be charged for the costs of transition. They would like to have assurances that the transition will result in payback through reduced costs to ratepayers. They are willing to consider non-quantifiable benefits, but must be educated on the importance of these benefits.

- Adoption of 61850 needs to be placed in the context of compliance with the Smart Grid standards mandated under Title XIII of the Energy Independence and Security Act of 2007. Within this context, a potentially useful channel for educating regulators is the Smart Grid Collaborative established by FERC and the National Association of Regulatory Utility Commissioners (NARUC).

In approaching regulators, and to some extent management, it is important to explain the technology as simply and non-technically as possible. This is difficult with 61850, because it is a deeply technical standard.

The following sections provide descriptions of 61850, one from a management and regulatory perspective and the other from a technical perspective. They are intended as draft inputs to a white paper on 61850 to be provided to appropriate audiences.

Management and Regulatory Description of 61850

IEC-61850 basically applies modern computer technology to substation automation. It is intended to replace legacy technologies that -- one way or another -- are derivatives of decades old space telemetry technology.

The appendix provides an overview of the principles of both the legacy and modern technologies. The modern technology was developed to address the following deficiencies of the legacy technology:

- **Lack of modularity** - The older technology combines numerous functions together in a monolithic structure. If it is necessary to upgrade or replace any part of the technology, the entire system must be replaced.
- **Lack of layering** - An important modular attribute of modern technology is the principle of "layering", a structured separation of functions so that each layer interface can operate with only the information needed there. An analogy is sending a letter through the post office. The letter is placed in a nested sequence of containers -- envelope, mailbag, gurney, and vehicle -- and only the information for the outer container is needed at any time for moving the letter through the postal system. In the legacy technology, there is either no layering or only minimal layering. Both cases significantly increase the difficulty of upgrading the technology to accommodate new requirements.
- **Difficulty in documentation and maintenance** - Everything in the legacy technology is identified by a data point number. For human understanding, these data point numbers must be cross-referenced to the names by which they are known to the technical people that control and maintain the actual equipment and to the computer systems those people use. This can lead to mistakes in cross-referencing, confusion, and additional cost. The modern

technology uses names that are human understandable from the start, eliminating the need for cross-referencing and simplifying system documentation.

- **Expensive substation wiring** - In the legacy technology, each measurement, status, or control was individually wired from the sensor or control device to the communications equipment. This wiring is expensive to install, document, and maintain. Newer versions of the legacy technology have mitigated this issue, but they are not always used.
- **Expensive installation** - The issues associated with documentation and maintenance extend to make initial installation and configuration time consuming, error prone, and expensive.
- **Inflexibility in addressing new requirements** - The legacy technology has limited flexibility for addressing new requirements. This is exacerbated by the lack of modularity and layering.
- **Ad hoc data organization** - The data is organized for each system on an ad-hoc basis. Although systems from a particular vendor can be expected to have commonalities, every system is essentially an ad-hoc design for that particular system.

IEC-61850 replaces legacy technology with modern computer and communications technology. Specific advances include:

- **Standardized data organization** - Instead of starting with a communications concept and attempting to fit it to overall utility automation, 61850 starts with a data organization concept and attaches communications to it. The data organization concept is highly flexible, enabling new needs to be accommodated.
- **Layered communications** - The communications services are layered. This enables replacement of communications technology by newer or alternative communications technology without disturbing the organization of the data. It also allows mixing of communications technologies in a system, because the data is finally delivered according to the data organization and does not depend on the communications used for transmitting it.
- **Communications methods tailored to needs** - IEC-61850 currently supports three methods of communications that can be used for different purposes. In two of the methods devices directly talk to each other within a substation using common, high-speed networks. This helps get rid of a substantial amount of costly substation wiring. The remaining method can be used for a variety of purposes, including direct communication between devices as well as communication with control centers and maintenance facilities.
- **All data items are named** - The data items are named rather than numbered. In addition, half of the name is left for the utility and/or vendor to determine, and the other half is constructed in a standardized way. Some data items are mandatory and others are optional, but if two data items of the same kind exist in a system, the standardized parts of their names will be identical. This has several benefits:
  - Documentation is greatly simplified. There is no need for error-prone, expensive cross-referencing numbers and names as there is with the legacy technology.
  - Articulation, documentation, and enforcement of cyber security access control policies can be simplified by using the standardized data item names.

  - A much broader scope of information can be managed. This can eliminate the need for separate, vendor-proprietary access to equipment setup and configuration data. It also enables the greatly improved flexibility of the data organization.
  - Field devices can be self-describing, further simplifying documentation and maintenance. Devices have directories of their named data items. This enables some documentation to be collected directly from the devices. Some data items can be optionally filled with descriptive information, further enhancing the self-description of the devices and simplifying documentation.
  - New data items can be easily added to accommodate new requirements. It is easy to exhaust a limited set of numbers, but it is almost impossible to exhaust a flexible structure of names. Examples of new data needs that can be accommodated include condition monitoring (to detect equipment problems before they become failures) and specialized metering data to fulfill requirements for renewable portfolio reporting.

- **Greatly improved data management functionality** - The data organization concept also defines services that access, manage, and use the data. Many of the services can be provided by different communications methods. Additional services can be added, if they are found to be useful. An example of a service is "Get [a certain named item of] data".
- **Greater compatibility with other modern computer standards -** There are a number of modern computer standards that have been adopted by the information technology departments of businesses, including utilities. One major family of standards is based on something called eXtensible Markup Language (XML). This language is the basis of many standards for the Internet and business enterprise systems. IEC-61850 uses XML for some purposes and can use it for others. The Common Information Model (CIM), a standard used for integrating utility enterprise computing, is based on XML. This facilitates exchange of data -- interoperability -- between 61850 and CIM-based systems.

The resulting benefits of 61850 are summarized in Table 3-1.

An example of a previously unforeseen need in which the flexibility of 61850 and its related standards can serve an important role is the support of regulatory reporting requirements under state renewable portfolio mandates. These reporting requirements could include a wide range of metering data, measurement data, and especially statistics drawn from these data. The statistics could change as regulatory agencies gain experience with enforcement of the mandates. For example, relevant statistics could include averages, medians, quantiles, maxima, minima, moving averages, and a variety of other parameters relevant to describing the output of intermittent energy sources. There may be a need to collect the statistics over a variety of time frames.

As discussed in the technology appendix, the intelligent electronic devices that implement 61850 are essentially computers. In many cases it is possible to modify their software to perform additional computation not foreseen in their original designs. However, managing the data resulting from these computations can present a challenge.

With 61850, the management and communication of additional data is relatively simple. All that is needed is to define and name the data. The 61850 standard can easily accommodate new data definitions and names. (That is primarily what the wind power standard, 61400-25, and the distributed energy resources standard, 61850-7-420, provide.)

The 61850 communications capabilities and other functionality support any data definitions and names that comply with the 61850 standard. If needed, 61850 provides the capability for storing the data in logs and remotely retrieving it later. This functionality is all included in the standard.

Table 3-1
Summary of 61850 Benefits (Management/Regulatory Version)

61850 Benefit	Area(s)	Resulting from
Easier articulation and CIP documentation of security policies	Security Cost	Naming of data items
Compatibility with evolving standards for alternative energy	Operations	Use of 61850 as base standard for wind power and other alternative energy control standards
Simplified substation wiring	Cost	Layered communications
Significant increase in scope of available information	Operations	Naming of data items and the ability to add new data items to the standard
Significant increase in quality of available information; Easier investigation of events.	Operations	Inclusion of information such as data item time stamps, time clock accuracy, and data quality indicators as standardized components of data items
Simplified system management	Operations	Naming of data items
Better integration with corporate systems	Operations Cost	Support for increased use of XML technology commonly used in enterprise systems
Enabling defense-in-depth using conventional security tools	Security Cost	Modularity and layered communications allow use of existing security technology and tools.
Easier installation setup	Operations Cost	“Plug and play” self-description of devices because they can be pre-loaded with relevant information about their function in the power system
Easier upgrade	Operations Cost	Ability to add new data items to the standard Modularity.
Improved maintenance	Operations	Extensive inclusion of device health and maintenance information in device data
Easier accommodation of new requirements	Operations Cost	Flexible organization of the data, layered communications, and flexible/extensible structure of the standard

Technically-Oriented Overview and Benefits of 61850

IEC-61850 basically applies modern computer technology to substation automation. It is intended to replace legacy technologies that -- one way or another -- are derivatives of decades old, commutation frame based, data point numbered, telemetry technology.

The 61850 technology was developed to address the following deficiencies in the legacy technology:

- **Lack of modularity** - The older technology combines numerous functions together in a monolithic structure. If it is necessary to upgrade or replace any part of the technology, the entire system must be replaced.
- **Lack of layering** - An important modular attribute of modern technology is the principle of "layering", a structured separation of functions so that each layer interface can operate with only the information needed there. In modern communications protocols, each layer provides to the layer below an envelope consisting of a header and trailer that contain the information needed for supporting the functionality needed at that layer. As a message moves down the protocol stack, the envelopes are added, and as it moves up the stack the envelopes are processed and removed. At the top of a modern protocol stack the message consists of only the application information. In the legacy protocols, there is either no layering or only minimal layering. Both cases significantly increase the difficulty of upgrading the technology to accommodate new requirements.
- **Difficulty in documentation and maintenance** - Everything in the legacy technology is identified by a number. For human understanding, these numbers must be cross-referenced to the names by which they are known to the technical people that control and maintain the actual equipment and to the computer systems those people use. This can lead to mistakes in cross-referencing, confusion, and additional cost. The modern technology uses names that are human understandable from the start, eliminating the need for cross-referencing and simplifying system documentation.
- **Expensive substation wiring** - In the legacy technology, each measurement, status, or control was individually wired from the sensor or control device to the communications equipment. This wiring is expensive to install, document, and maintain. Newer versions of the legacy technology have mitigated this issue, but they are not always used.
- **Expensive installation** - The issues associated with documentation and maintenance extend to make initial installation and configuration time consuming, error prone, and expensive.
- **Inflexibility in addressing new requirements** - The legacy technology has limited flexibility for addressing new requirements. This is exacerbated by the lack of modularity and layering.
- **Ad hoc data organization** - The data is organized for each system on an ad-hoc basis. Although systems from a particular vendor can be expected to have commonalities, every system is essentially an ad-hoc design for that particular system.

The specific advances included in 61850 are based on two key concepts: named objects and layered communications. IEC-61850 differs from legacy technologies in that it defines and communicates named objects that are themselves hierarchical composites of other named objects, their named attributes, and the related attribute values. The named objects replace the numbered points used in legacy technologies. Power system equipment is modeled using standardized objects, and the object models are communicated using standard services (such as GetData and SetData) mapped onto modern, layered, network communications technologies. The layering of these communications technologies allows stack components to be modularly replaced with improved functionality as technology and related standards advance.

The named objects comprise an object model that describes substation monitoring and control devices, more commonly known as "Intelligent Electronic Devices (IEDs)". The object model includes all aspects of the devices -- analog and status values, settings, descriptive data, directories, logs, and control blocks for various functions. The data names are hierarchically organized, so a parent name implicitly includes its children, i.e., a request that names a bus voltage data object implicitly requests all phases and both magnitude and angle of each phase. The data object also includes data quality, time stamp and time quality for the values supplied.

Some components of the object model are mandatory under the standard. Others are either optional or conditional. (An example condition would be a requirement that an option selected for one phase must be applied to all phases.)

The naming hierarchy in 61850 includes:

IED/Server
- Logical Device (LD)
  - Logical Node (LN)
    - Common Data Class (CDC)
      - Common Data Attribute (CDA)

Each name in a 61850-based system consists of two parts. One part is a name assigned by the user. The remainder is the standardized name for the power system object. Naming down to the level of LD, i.e., before the slash ("/"), is utility specified. Naming after the slash is standardized. The LN name can be preceded by an alphanumeric prefix and must be followed by a numeric suffix. The first letter of the LN name indicates a category of monitoring and control. For example, LN names beginning with P indicate protective relays, R indicates protection-related functions (such as event recorders), M indicates metering and measurement devices, and X indicates switchgear. Figure 3-1 shows an example of 61850 naming.

```
Roanoke_238KV_LB99A_CTRL/MMXU1.PhV.phsB.CVal.mag.f”

Where:

"Roanoke_238KV_LB99A_CTRL” is a utility defined device name
MMXU1.PhV.phsB.CVal.mag.f is the 61850 standard name for the floating
point magnitude of the complex value that is the Phase B voltage
measured by measurement unit (MMXU) number 1 of the device
```

Figure 3-1
Example of 61850 naming

The standardized part of the power system object names can easily be extended to support new kinds of devices and additional relevant information. The 61400-25 wind power standard has some parts that extend the 61850 standardized objects to include equipment and information needed for defining wind power facilities. The wind power standard also takes advantage of the protocol layering to add two protocol stack standards not included in the 61850 standard itself.

Another advance provided in 61850 is use of XML for certain purposes that are expanded in related standards. One important purpose is configuration, for which 61850 provides an XML-based Substation Configuration Language (SCL). The XML capability of 61850 provides a means for harmonization with other XML-based standards, such as the Common Information Model (CIM) and Multispeak.

SCL is organized into four sections:

- Substation - defining and naming electrical objects
- IED – defining and initializing (where necessary) monitoring/control objects
- Communications - defining addresses and other communications parameters
- Data Type Templates – identifying named versions of objects with options selected

SCL has a variety of file types for different purposes:

- IED Capability Description (ICD), primarily including all sections but Substation
- Substation Specification Description (SSD), focused primarily on the Substation section
- Substation Configuration Description (SCD), having all four sections for a configured substation
- Others for additional aspects of tool linkages (e.g., design) and other specification needs

SCL also provides capabilities for supporting additional information, such as access control and graphics positioning.

The 61850 standard provides several functions and services that are not provided in the legacy technology. Identification of these functions is based on IEC-60870-5 services identified as not mappable to 61850. These include:

- Server, LD, and LN directories and data definitions
- Data sets
- Setting group management
- Report control blocks
- Logs
- Device-to-device messaging (GOOSE and Sampled value)
- File transfer
- Improved time stamping

The benefits of 61850 are summarized in Table 3-2.

Table 3-2
Summary of 61850 Benefits (Technically-oriented Version)

61850 Benefit	Area(s)	Resulting from
Easier articulation and CIP documentation of security policies	Security Cost	Named objects
Compatibility with evolving standards for alternative energy	Operations	Use of 61850 as base standard for wind power and other alternative energy control
Simple LAN connections replace complex point-to-point wiring in substations	Cost	Routable protocols
Significant increase in scope of available information	Operations	Extensible object models using named objects.
Significant increase in quality of available information; Easier investigation of events.	Operations	Time stamp, time quality, and data quality included in objects
Simplified system management	Operations	Named objects
Better integration with corporate systems	Operations Cost	Support for increased use of XML technology
Enabling defense-in-depth using conventional security tools	Security Cost	Routable protocols allow use of existing security technology and tools.
Easier installation setup	Operations Cost	“Plug and play” self-description
Easier upgrade	Operations Cost	Extensible object models. Modular structure of standards
Improved maintenance	Operations	Extensive health and maintenance attributes defined in device objects
Easier accommodation of new requirements	Operations Cost	Data structures, layered protocols, and flexible/extensible structure of the standard

4
RECOMMENDATIONS

The following sections provide recommendations for future work by EPRI.

Develop Use Cases for Tools

One issue identified in the adoption of 61850 is the need for tools. These include tools that allow utility personnel to manage integration and configuration of equipment from heterogeneous suppliers, and tools to capture the benefits of 61850. Examples of such tool functionality include:

- Assigning the utility-defined portion of names to IED's and managing the various IED and LD names in the power system.
- Assigning the names of electrical equipment
- Associating LN's with the electrical equipments they monitor or control
- Assigning line identifiers to the proper LIN or IFL "equipment" and locating them within the substation.
- Preparing NERC CIP documentation

Our recommendation in this area is to define the use cases for such tools.

Follow Up Proposals for SCL and Object Model Improvements

The improvements suggested above could be forwarded to appropriate IEC working groups and followed up with designs and implementations. Develop additional improvements as the editions of IEC-61850 evolve.

Develop AMI and customer communications approaches based on 61850

Study the feasibility of a 61850-based AMI and customer communications standards and the eventual need for integration of customer communications and 61850-7-420. Develop and provide to both IEC and the OpenAMI effort a 61850-based approach to AMI and customer communications.

Sponsor Needed Research, Development, and Demonstrations

The differences between the processes needed for many traditional standards and for most standards involving information and communications was previously discussed. The standards related to 61850 contain data structures and representations, logic, and implied software functions, and accordingly require research and development either during or subsequent to adoption to ensure that their provisions are feasible, unambiguous, and meet the needs of the intended applications. The IEC process does not require this research, development, and interoperability demonstration, as does the IETF process that focuses on information and communications standards similar to 61850.

During development of the Utility Communications Architecture, EPRI sponsored a set of demonstration pilots. As a result of those pilots, several utilities requested UCA technology in their procurement specifications. The requests did not successfully result in UCA technology being provided. Apparently, vendors were not prepared at that time to provide it.

Vendors are now prepared to provide 61850 technology, successor to the UCA technology. The process of expanding the use of a technology has been described in [MOOR1999]. The North American utilities that have planned to use 61850 can be described as “early adopters”. To go beyond early adopters requires convincing potential users who want to have recommendations from other users like themselves who are not early adopters. Experience from demonstration pilots can help create those recommendations. EPRI should consider restarting the kinds of demonstration pilot projects that were critical in development of the UCA.

Educate NARUC members and staffs

As stated earlier, educating utility regulators is a key requirement in moving forward the implementation of the Smart Grid. It is clear that 61850 is a core technology of the Smart Grid. Accordingly, educating regulators in the overall characteristics and benefits of 61850 will be a critical activity in moving the Smart Grid forward. It may be possible to formulate demonstration projects that produce the kinds of experience and data that regulators will need as reference material in approving recovery of Smart Grid expenditures. One good channel for both providing education and guiding the formulation of demonstration projects is the FERC/NARUC Smart Grid Collaborative established in the regulatory community.

Develop reference implementation(s)

As stated above, the resolution of ambiguities and interoperability issues is significantly helped by developing reference implementations as part of a standards process. The reference implementations become definitive interpretations of the standards text. EPRI should consider preparing such reference implementations.

Conduct a Survey of Member Utility Naming Conventions

In Section 2 it was recommended that IEC include examples in its documents based on North American utility equipment and device naming conventions. EPRI should consider conducting such a survey and providing the results as a contribution to the IEC.

Develop a Fictitious Utility to Serve as Data for Testing

In testing its tools, OSECS identified the need for a fictitious utility that included substation names, substation equipment configurations, and example utility naming conventions for equipment and devices. The definition of such a utility facilitates testing of 61850 tools and functionality. Such a fictitious utility is especially needed for 61850 because of the extent that 61850 explicitly names equipment, devices, and data objects.

Such a fictitious utility could be extended to include example security policies, access control policies, protection schemes, and other information for purposes such as testing tools for identifying critical assets and critical cyber-assets, serving as example data sets for reference implementations and interoperability tests, and a variety of other purposes. A fictitious utility could also serve as a reference example for software that assists in NERC CIP compliance.

A
APPENDIX: OVERVIEW OF THE OSECS TOOLKIT PROJECT

Open Secure Energy Control Systems, LLC (OSECS) has been developing an open-source Toolkit for constructing secure, next-generation systems that will control electric power transmission, distribution, and distributed generation. The Toolkit takes advantage of IEC-61850 protocols and related standards; and includes basic SCADA client and control center components, as well as tools for configuration and management of 61850-based systems.

The initial development was done under a Department of Homeland Security Phase II Small Business Innovation Research (SBIR) contract. OSECS initial intention was to address electric utility SCADA security issues by encouraging electric utilities and their equipment providers to migrate to the more easily secured IEC 61850 family of utility automation standards. IEC has developed and adopted a new standard for wind power (61400-25) that is based on 61850, and OSECS is currently expanding toolkit functionality to facilitate grid integration of wind power.

IEC-61850 is a core enabling technology for the Smart Grid. The Toolkit is focused on making the grid both smarter and more cyber-secure. It does so by:

- Providing 61850 protocol drivers for the Manufacturing Messaging Specification (MMS) and for Web Services
- Providing 61850 support tools, including management tools for 61850 Substation Configuration Language
- Supporting extensions for wind power and other alternative energy
- Enabling use of conventional security capabilities, such as encryption, firewalls, intrusion detection systems, and a secure operating system
- Supporting compliance with emerging security mandates, particularly NERC CIP 002-009
- Leveraging leading-edge open source technologies

Our solution makes available -- to utilities, equipment manufacturers and integrators, Distributed Resources owners, and the utility research community -- a highly versatile open-source toolkit for building SCADA and automation systems such as:

- System for secure remote non-real-time data access
- Control system for distributed generation facilities, including wind power
- Workstation for equipment maintenance or substation local Human Machine Interfaces

- Substation and control center security appliances (application firewalls and access control gateways)
- Starter or enhanced SCADA for small utilities

The solution is particularly focused on utilities, distributed resources owners, and their suppliers who need to be able to assess the benefits of 61850 before full scale deployment.

Figure A-1 shows an overview of our toolkit architecture. At its heart are a web service engine, an MMS protocol stack, and role based access control on messages passing through the engine. The web service engine operates within a SOAP server framework. The web service engine processes commands and information requests, expressed in XML, and either translates to MMS or converts to 61400-25 SOAP for communicating with 61400-25/61850 compatible substation equipment.

The engine refers to a database for the role-based security permissions of various objects and for looking up the addresses of individual substation equipments. There are two secure networks, one linking control center workstations, and possibly interfaces to corporate and other facilities, to the control center server on which the toolkit core engine is resident. The other secure network links the control center and the substation equipment.

Other functions can be added as building blocks, such as scheduled equipment polling or intrusion detection, and can operate by exchanging messages with the web service engine.

Various other functions are included in the Toolkit, such as management of role based access control (RBAC) policy data, management of Intelligent Electronic Device settings, security tools, and advanced applications such as power flow and contingency analysis.

The Toolkit goes well beyond IEC-61850, Edition 1 in its use of XML. It expresses the object models and access control privileges in XML, it defines 61850 services in XML-based WSDL, and it provides XML-based SOAP as a messaging method alternative to MMS. Use of XML and XML-related standards within the Toolkit can facilitate integration with Common Information Model (CIM) related standards for electric utility enterprise objects.

Although the Toolkit was a pioneer in its definition of 61850 SOAP messaging, a 61850-based SOAP messaging system is defined as an alternative communications method in 61400-25-4. the communications protocol mapping of the IEC wind power control standard. The wind power standard also uses 61850-style objects.

Open source components

OSECS has used freely-available open source components and tools to accelerate Toolkit implementation. A beneficial side effect of this approach is to ensure that the most recent security technology is always available for integration. As the security technology advances, improved components become available for incorporation in Toolkit based products.

Unfortunately, not all requisite infrastructure components are available through the open source community. Under the DHS Phase II SBIR, OSECS accomplished the development, design, or identification of open source tools to be configured for a number of components including:

- Open source 61850 MMS client stack
- Core 61850 SOAP server, MMS interface, and message RBAC
- Workstation 61850 SOAP messaging client
- Workstation 61850 SOAP object model and GUI
- RBAC security policy management
- SE-Linux platform and secure network environment
- Substation intelligent electronic device (IED) settings management and surveillance
- SCL management tool, including generation of object names to utility-specified naming patterns, that can be based on substation or wind farm design patterns
- Additional SCADA functions (polling, persistent database, topology)
- Interface to advanced application functions (e.g., power flow, contingency analysis)

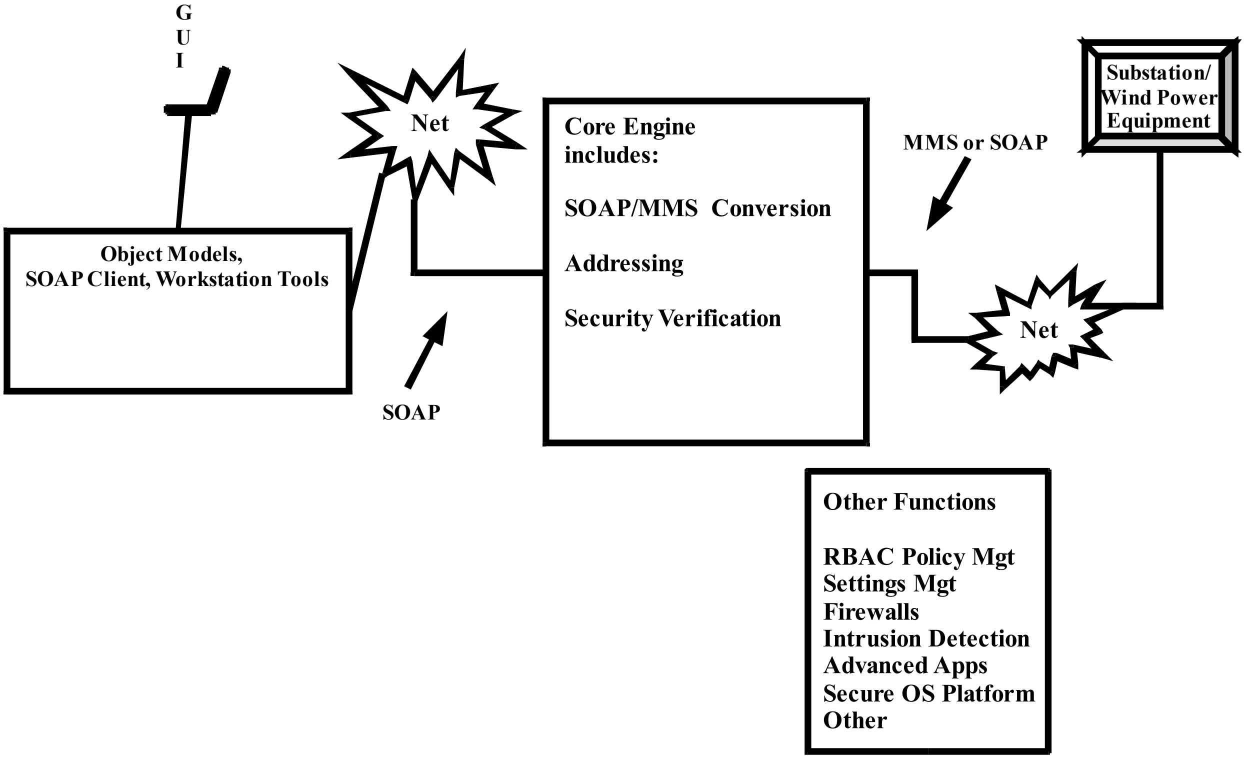

Figure A-1
Overview of Toolkit Architecture

The OSECS developed components are being released under dual licensing terms -- an open source license or a commercial license. Many equipment providers incorporate "secret sauce" technology into their products, and the commercial license is intended to enable those providers to avoid certain issues that can arise in open source licensing.

Key open-source COTS components include:

- gSOAP as the basis of the Core Engine.
- Python – for programming workstation client applications and ancillary tools
- GNU C/C++ - for programming server applications
- Enthought/wxWidgets/wxPython/GTK for the workstation GUI
- iptables (included in Linux) – for the platform firewall
- MySQL, PostgreSQL or other– for the persistent database
- ZSI for the workstation Web Services client
- PSAD, prelude, or other – for firewall log analysis
- Octave/PSAT – for advanced power system applications, such as power flow,
- and numerous others.

Figure A-2 shows the functionality of the workstation. The workstation contains two object models, one for electrical equipment and the other for monitoring/control equipment. The monitoring/control objects are linked to the electrical equipment they monitor and control.

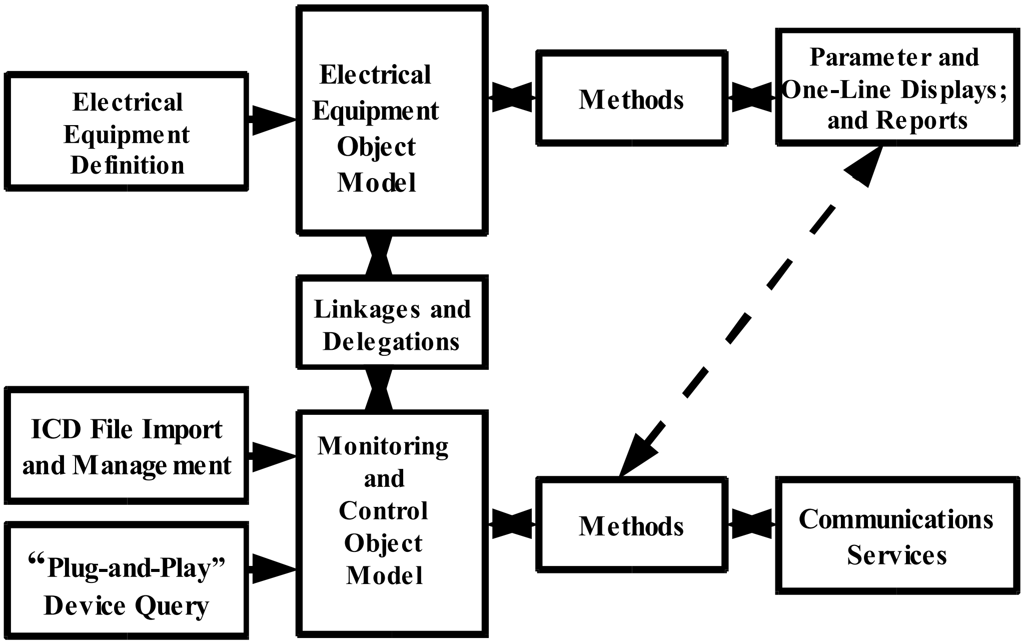
Electrical Equipment Definition
Electrical Equipment Object Model
Methods
Parameter and One-Line Displays; and Reports
Linkages and Delegations
ICD File Import and Management
"Plug-and-Play" Device Query
Monitoring and Control Object Model
Methods
Communications Services

Figure A-2
Workstation Functionality

The electrical object model is instantiated using files that describe:

- Design pattern structures (e.g., breaker-and-a-half) and name information for each item of equipment or connectivity node in the pattern
- Naming rules for devices and definition of counters for handling numeric parts of names
- Descriptions of substations or wind facilities in terms of the design patterns

The monitoring/control object model is instantiated either using manufacturer-supplied files that describe device capabilities or by querying the devices for their directory information.

Figure A-3 shows an example application of the Toolkit for application access control in a control center to substation environment. There are three networks shown, a secure network within the control center, a secure network between the control center and substation, and a network within the substation protected by a Toolkit-based security appliance.

At the conclusion of the DHS Phase II effort, the toolkit consisted of prototype components that had been individually developed and partially tested, but had not been integrated. As part of the DOE Phase I effort, additional development was performed and integration was initiated. Subsequent to completion of the DOE Phase I effort, there has been further development and integration.

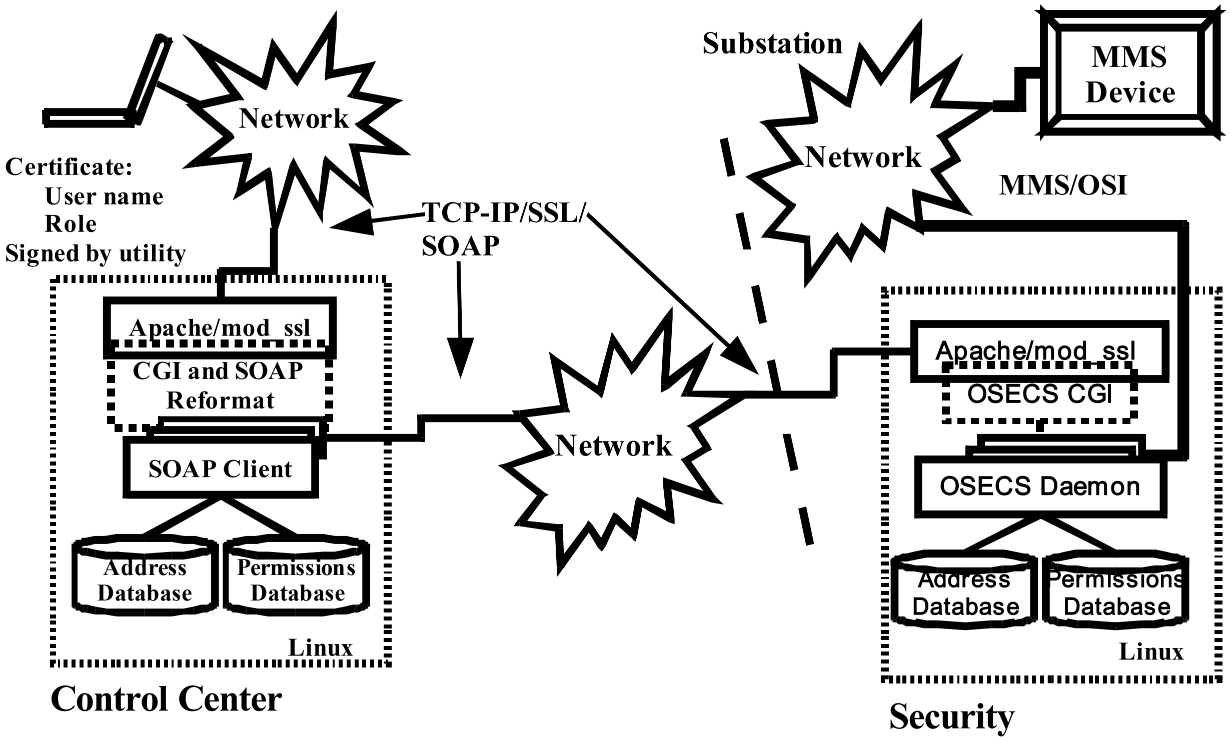

Figure A-3
Example Application of Toolkit for Access Control

B

APPENDIX: SELECTED MATERIAL EXTRACTED FROM IETF RFC 2026/BCP-9

4.1.2 Draft Standard

A specification from which at least two independent and interoperable implementations from different code bases have been developed, and for which sufficient successful operational experience has been obtained, may be elevated to the "Draft Standard" level. For the purposes of this section, "interoperable" means to be functionally equivalent or interchangeable components of the system or process in which they are used. If patented or otherwise controlled technology is required for implementation, the separate implementations must also have resulted from separate exercise of the licensing process. Elevation to Draft Standard is a major advance in status, indicating a strong belief that the specification is mature and will be useful.

The requirement for at least two independent and interoperable implementations applies to all of the options and features of the specification. In cases in which one or more options or features have not been demonstrated in at least two interoperable implementations, the specification may advance to the Draft Standard level only if those options or features are removed.

.....

10.3.2. Standards Track Documents

(A) Where any patents, patent applications, or other proprietary rights are known, or claimed, with respect to any specification on the standards track, and brought to the attention of the IESG, the IESG shall not advance the specification without including in the document a note indicating the existence of such rights, or claimed rights. Where implementations are required before advancement of a specification, only implementations that have, by statement of the implementers, taken adequate steps to comply with any such rights, or claimed rights, shall be considered for the purpose of showing the adequacy of the specification.

...

(C) Where the IESG knows of rights, or claimed rights under (A), the IETF Executive Director shall attempt to obtain from the claimant of such rights, a written assurance that upon approval by the IESG of the relevant Internet standards track specification(s), any party will be able to obtain the right to implement, use and distribute the technology or works when implementing, using or distributing technology based upon the specific specification(s) under openly specified, reasonable, non-discriminatory terms. The Working Group proposing the use of the technology with respect to which the proprietary rights are claimed may assist the IETF Executive Director in this effort. The results of this procedure shall not affect advancement of a specification along the standards track, except that the IESG may defer approval where a delay may facilitate the obtaining of such assurances. The results will, however, be recorded by the IETF Executive Director, and made available. The IESG may also direct that a summary of the results be included in any RFC published containing the specification.

C
APPENDIX: UNDERLYING TECHNICAL PRINCIPLES

This appendix provides simplified explanations of the underlying technical principles of the legacy technology and of 61850.

The legacy technology is derived from telemetry technology originally developed for the space program and other areas. This technology was developed in the 1950's, 60's, and 70's before computers could be made small enough to be embedded in equipment. However, it was possible then to electronically convert measurements to digital form and to process them in computers on the ground. The computers then filled large rooms and actually had much less computing capability than a modern cell phone.

Figure C-1 depicts the underlying concept of the legacy technology. There are a number of digitized measurements, known as "data points" attached to contacts on a commutator, conceptually similar to the commutators found in DC motors, although actually implemented in electronics. A conceptual arm rotates through the contacts, placing the data points in locations in a "data frame". Additional information needed for communications (such as the identity of the recipient and information to help ensure that the data has been communicated correctly) is added to the frame in the form of a header and trailer. The frame is sent and the process starts again.

Originally, this technology was implemented in electronics, but not computers. As computers became smaller and easier to embed in equipment, a computer was used, but the concept was not changed. The technology has advanced, but has retained the concept of numbered data points in a data frame. Dan Nordell in [CLEVE2003] has described the DNP-3 protocol as the "pinnacle of traditional SCADA protocols." However, retaining the concept of numbered measurements and data frames seriously limits the flexibility of the legacy technology in meeting new requirements.

The underlying concept of 61850 technology is that every monitoring, control, or metering device in a power system is a computer that includes a database, software, and communications capability. The computer may be very small, but it has these basic elements. For devices that take measurements, there is a measurement sensing device interfaced to the computer in a manner conceptually similar to the way a keyboard, mouse, microphone, speaker, or printer are interfaced to a personal computer. One peripheral that is required to be available in the substation is a precision digital clock, such as a GPS-based device. This enables data measurements to be accurately time stamped.

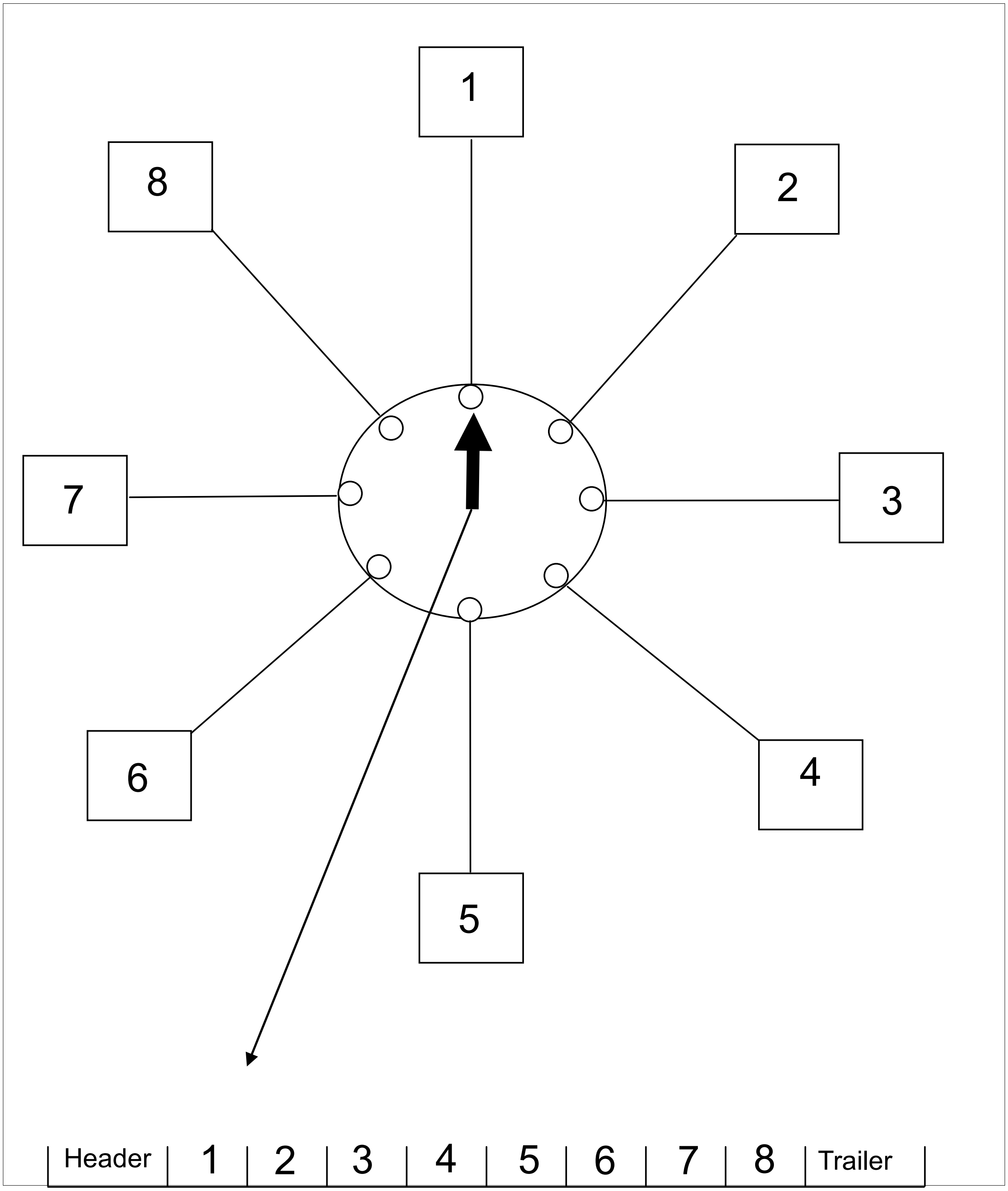

Figure C-1
Underlying concept of the legacy technology

The data items are placed in the computer database and are referenced by their names, assigned according to the 61850 standard and the practices of the using utility. The software can work on the data to perform functions required in the device. There are a few functions that are specified in 61850, such as having the computer check the data in the database and produce certain reports or store certain information in a log file if it detects certain changes. There are user-specified "control blocks" of data defined in 61850 to control the operation of these functions. Also, some data items are descriptive information loaded when the device is configured for installation.

Although there are significant differences in numerous detailed requirements and features of the standard, communicating 61850 data is conceptually the same as communicating information regarding a customer's account in a business system. The data items have names and values, and these are sent using communication methods based on commonly-used standards. The 61850 standard only identifies the other standards and tells how to use their features to support the data and data-related functions specified in 61850. IEC 61400-25, the wind power extension to 61850, identifies two additional communications standards beyond those already specified in 61850. Others can be added if they are found useful. Data items can be added, either by users or by companion standards. IEC 61400-25 is precisely such a companion for wind power. All it does is define the data needed for controlling wind power equipment. It, too, can be extended.

D
APPENDIX: REFERENCES

[CLEV2003] F. Cleveland, J. Newbury, M. Chaturvedi, D. Nordell, and S. Klein, *Developments in Power Communications Systems*, tutorial presented at 2003 IEEE Power Engineering Society General Meeting, July 2003

[CURR2003] P.Curran, *Conformance Testing: An Industry Perspective*, presented at NIST Symposium "Building Confidence and Trust in Voting Systems," December 2003

[DALC2003] E. Dalci, E. Fong, A. Goldfine, *Requirements for GSC-IS Reference Implementations*, NIST Information Technology Laboratory, 2003

[HOLB2007] J. Holbach, et al, "TVA Bradley: First IEC-61850 Multivendor Project in the USA", PacWorld (Protection, Automation, and Control Magazine) , Autumn 2007, pp 51-58

[JAMM2005] F. Jammes, *ITEA SIRENA industrial demonstration,* presentation, 4 July 2005

[NEWT2007] C. Newton, "2006-2008 Protection Relay Study: Summary and Highlights", PacWorld (Protection, Automation, and Control Magazine) , Autumn 2007, pp42-46

[MAC2006] R. Mackiewicz, Benefits of IEC61850 Networking, Presentation at UCA Users Group meeting, January 2006

[MOOR1999] G. Moore, *Crossing the Chasm*, Harper, 1999

[REIC2007] M.L. Reichard, D. Finney, J.T. Garrity (all of General Electric), "Windfarm System Protection Using Peer-to-Peer Communications, " Presented at 60th Annual Conference For Protective Relay Engineers College Station, Texas, March 27-29 2007

[ROSE2005] Lawrence Rosen, *Open Source Licensing: Software Freedom and Intellectual Property Law*, Prentice Hall, 2005.

[RUS 2001] United States Department of Agriculture, Rural Utilities Service, *Design Guide for Rural Substations*, RUS Bulletin 1724E-300, June 2001

[SIRE2005] SIRENA Partners, *WP4 – Software Components and Tools,* Service Infrastructure for Real-time Embedded Networked Applications (SIRENA), ITEA 02014 Project, 30 June 2005

[W3C2001] Web Services Description Language (WSDL) 1.1, W3C Note, posted at http://www.w3.org/TR/wsdl, March 2001

[W3C2003] SOAP Version 1.2 Part 1: Messaging Framework, W3C Recommendation, posted at http://www.w3.org/TR/soap/, June 2003

[W3C2004] Web Services Addressing (WS-Addressing), W3C Member Submission, posted at http://www.w3.org/Submission/ws-addressing/, 10 August 2004

Export Control Restrictions

Access to and use of EPRI Intellectual Property is granted with the specific understanding and requirement that responsibility for ensuring full compliance with all applicable U.S. and foreign export laws and regulations is being undertaken by you and your company. This includes an obligation to ensure that any individual receiving access hereunder who is not a U.S. citizen or permanent U.S. resident is permitted access under applicable U.S. and foreign export laws and regulations. In the event you are uncertain whether you or your company may lawfully obtain access to this EPRI Intellectual Property, you acknowledge that it is your obligation to consult with your company's legal counsel to determine whether this access is lawful. Although EPRI may make available on a case-by-case basis an informal assessment of the applicable U.S. export classification for specific EPRI Intellectual Property, you and your company acknowledge that this assessment is solely for informational purposes and not for reliance purposes. You and your company acknowledge that it is still the obligation of you and your company to make your own assessment of the applicable U.S. export classification and ensure compliance accordingly. You and your company understand and acknowledge your obligations to make a prompt report to EPRI and the appropriate authorities regarding any access to or use of EPRI Intellectual Property hereunder that may be in violation of applicable U.S. or foreign export laws or regulations.

The Electric Power Research Institute (EPRI), with major locations in Palo Alto, California; Charlotte, North Carolina; and Knoxville, Tennessee, was established in 1973 as an independent, nonprofit center for public interest energy and environmental research. EPRI brings together members, participants, the Institute's scientists and engineers, and other leading experts to work collaboratively on solutions to the challenges of electric power. These solutions span nearly every area of electricity generation, delivery, and use, including health, safety, and environment. EPRI's members represent over 90% of the electricity generated in the United States. International participation represents nearly 15% of EPRI's total research, development, and demonstration program.

Together...Shaping the Future of Electricity

Program:

Substations

Printed on recycled paper in the United States of America

1015962

Electric Power Research Institute
3420 Hillview Avenue, Palo Alto, California 94304-1338 • PO Box 10412, Palo Alto, California 94303-0813 USA
800.313.3774 • 650.855.2121 • askepri@epri.com • www.epri.com