Award: **DE-FC26-04NT42213**

Title: Advanced Communication and Control for Distributed Energy Resource Integration: Phase 2 Scientific Report

Report Date: February 13, 2009
Project Dates: 10/1/2004 - 9/30/2008
Report Type: Final Scientific/Technical Report

Recipient: BPL Global, Ltd.
(Acquired Connected Energy Corp. in 2008)
Four Commercial Street
Suite 400
Rochester, NY 14614
Tel: 585-697-3800
Fax: 585-697-3880
www.bplglobal.net

DISCLAIMER

1. Project Title

Cooperative Research and Development for Advanced Communication and Control Solutions

2. Report Author

David W. Sheehan, Technical Lead
BPL Global Ltd., 4 Commercial Street, Rochester, NY 14614
E-Mail: dsheehan@bplglobal.net
Office Phone: 585-697-3815
Office Fax: 585-697-3880

3. Project Team

Organization	Role Description
BPL Global (Connected Energy Corp.)	Principal Investigator Software and Protocol Developer, Site Data Acquisition and Control Provider.
Southern California Edison	Electric Utility Partner Owner and Operator of Phase II test site at Pebbly Beach Generation Station on Catalina Island, CA.
Long Island Power Authority	Electric Utility Partner Owner and Operator of Phase II test sites located on the following Long Island campuses: SUNY Farmingdale, Good Samaritan Hospital, and Winthrop Hospital.
Sandia National Laboratory	National Laboratory Partner IT and SCADA security experts, project lead security policy developer, and principal security design reviewer.
New York State Energy Research and Development Authority	State Energy Commission Partner Co-Sponsor of Phase II test sites at Rochester International Airport (Rochester, NY) and Greenpark Care Facility (Brooklyn, NY).
New York Independent System Operator	New York State ISO Partner Advisor of DER use-cases for demand-response, real-time market, and control area operation uses.
California Independent System Operator	California ISO Partner Advisor of DER use-cases for demand-response, real-time market, and control area operation uses.
California Energy Commission	State Energy Commission Partner Sponsor of related project using this project's communication architecture for ancillary services.
Mykotronx (SafeNet)	Security Consultant Consultant on best practices for communication security and cryptography technologies.

4. Subcontractors

Organization	Deliverables
Southern California Edison	Project management, site engineering, and site installation for 3 DER installations for Phase II demonstration sites. Engineering to establish communication with the Capstone C60 microturbine at the Pebbly Beach Generating Station. Administrative and engineering work associated with the maintenance of the DER installations for the duration of the Phase II demonstration.
Long Island Power Authority	Project management, site engineering, construction, equipment, and administrative costs to provision and maintain remote monitoring and control for three Phase II demonstration sites.
Sandia National Labs	Assessment of the Phase II security levels and how the design meets the recommended policy practices. Assist in outreaches involving security policy and recommended practices.
Mykotronx (SafeNet)	Define the security requirements for a hardened onsite gateway device for DER OEMs. Identify strategies for managing hardware based authentication tokens and infrastructure. Definition of security boundaries in the architecture and the requirements for crossing them.

5. Other Partners

Organization	Role Description
Los Angeles County Sanitation District	Owner of three Phase II test sites: Calabasas Landfill, Lancaster Landfill, and Palmdale Water Reclamation Plant.
Monroe County Department of Environmental Services	Coordinator of the Rochester International Airport Phase II test site. Owner and operator of the Irondequoit Pumping Station Phase II test site located in Rochester, NY.
Gas Technology Institute	Security consultation on gas utility SCADA systems and the American Gas Association's Security Standard (AGA-12).
Alternative Energy Systems Consulting, Inc.	Provided expertise and smart agent technology for use at the Calabasas Landfill demonstration site.
Infotility, Inc.	Provided real-time energy pricing data for use at the Calabasas Landfill demonstration site.

Table of Contents

6. Glossary

The following acronyms and terms used throughout the document are described in the table below.

Term	Definition
DER	Distributed energy resource. This term typically refers to a range of smaller-scale devices designed to provide electricity and (in some cases) also thermal energy in locations close to consumers. These devices include a variety of fossil fuel and renewable distributed generation (DG) technologies, energy storage (e.g. batteries and flywheels) and combined heat and power systems.
DNS	Domain name system. This system is used on the Internet and computer networks to associate human understandable textual names with a numerical address on the Internet that computers need to use. As an example, when a user navigates to www.bplglobal.net, the computer uses the domain name system to lookup an IP address that it then uses to connect to the appropriate server to fulfill the request.
DSA	Digital Signature Algorithm. This is a computer algorithm developed to implement digital signatures used to verify the identity of the sender of a message.
HTTP	Hypertext transfer protocol. This is a request/response protocol commonly used by a web browser to load a web page hosted on a remote server.
HTTPS	Hypertext transfer protocol secure. This is the HTTP protocol that runs over a secure SSL connection that protects the data being exchanged as it passes over networks such as the Internet.
ICCP	Inter-Control Center Communications Protocol. This is a protocol that can be used to exchange SCADA data over wide area networks.
IP	Internet protocol. This is a common protocol that is used to exchange information between computers. As an example, the Internet protocol is used between a web browser on a computer and a web server when accessing a web page.
IPSEC	Internet protocol security. This is a technology used to provide communication security through the use of data encryption and user authentication.
PIN	Personal identification number. This is a numeric identifier that is typically used in conjunction with a physical security token such as a key or card. It is used to minimize the risk of the hardware token being lost by requiring that the user also know this short identifier to be able to prove that they are the owner of the hardware token.

Term	Definition
PLC	Programmable logic controller. This is a piece of specialized hardware that is commonly found in commercial and industrial control systems. It interfaces with a variety of other systems and is able to run small automated programs that act upon these inputs.
RTU	Remote terminal unit. This is the packaged hardware that is installed on-site near the DER that is responsible for communicating with the equipment and interfacing it with the remote data center.
SCADA	Supervisory control and data acquisition. This term is used to describe the commercial and industrial control systems that interface with processes and equipment such as power generators.
SSH	Secure shell. This is a mechanism that is used to securely access a remote computer system over an insecure network. It is commonly used to securely obtain a terminal session on a remote computer but can also be used to exchange data or run commands on a remote system.
SSL	Secure Sockets Layer. This is a set of protocols that are used to provide data encryption, data integrity, and user authentication capabilities to software used over insecure networks such as the Internet. It is commonly used to protect the data exchanged with certain web pages over the Internet.
TCP	Transmission Control Protocol. This is a protocol that is used to exchange data between two computer systems in a fashion that guarantees that messages (packets) sent are received intact and in the proper order by the receiver.
USB	Universal Serial Bus. This is a physical communication system used to attach hardware peripherals to a computer system. It supports plugging and un-plugging devices without powering down the computer system and multiple devices can be attached to a single physical port using a hub.
VPN	Virtual private network. A VPN is used to take a device and allow it to communicate on a remote computer network as if it were directly connected to that network. Virtual private networks typically utilize data encryption to protect data in transit and have user authentication and authorization services. One use of a VPN is to allow an RTU to communicate with a remote data center securely by simply placing the RTU and data center on the Internet instead of running a dedicated network link between the two entities.
XML	Extensible markup language. This is a specification allowing for the creation of structured data representations in a human readable textual format.
XSD	XML schema. This is an XML document that describes the structure for another XML file. An XSD file can be used to programmatically validate that an XML file is correct.

7. Project Objectives

The objective of this research project is to demonstrate sensing, communication, information and control technologies to achieve a seamless integration of multi-vendor distributed energy resource (DER) units at aggregation levels that meet individual user requirements for facility operations (residential, commercial, industrial, manufacturing, etc.) and further serve as resource options for electric and natural gas utilities. The fully demonstrated DER aggregation system with embodiment of communication and control technologies will lead to real-time, interactive, customer-managed service networks to achieve greater customer value.

Work on this Advanced Communication and Control Project (ACCP) consists of a two-phase approach for an integrated demonstration of communication and control technologies to achieve a seamless integration of DER units to reach progressive levels of aggregated power output. Phase I involved design and proof-of-design, and Phase II involves real-world demonstration of the Phase I design architecture.

8. Project Description

The scope of work for Phase II of this ACCP involves demonstrating the Phase I design architecture in large scale real-world settings while integrating with the operations of one or more electricity supplier feeder lines. The communication and control architectures for integrated demonstration shall encompass combinations of software and hardware components, including: sensors, data acquisition and communication systems, remote monitoring systems, metering (interval revenue, real-time), local and wide area networks, Web-based systems, smart controls, energy management/information systems with control and automation of building energy loads, and demand-response management with integration of real-time market pricing.

For Phase II, BPL Global shall demonstrate the Phase I design for integrating and controlling the operation of more than 10 DER units, dispersed at various locations in one or more Independent System Operator (ISO) Control Areas, at an aggregated scale of more than 1 MW, to provide grid support. Actual performance data with respect to each specified function above is to be collected during the Phase II field demonstration. At a minimum, the Phase II demonstration shall span one year of field operations. The demonstration performance will need to be validated by the target customer(s) for acceptance and subsequent implementation. An ISO must be involved in demonstration planning and execution.

As part of the Phase II work, BPL Global shall develop a roadmap to commercialization that identifies and quantifies the potential markets for the integrated, aggregated DER systems and for the communication and control technologies demonstrated in Phase I. In addition, the roadmap must identify

strategies and actions, as well as the regional and national markets where the aggregated DER systems with communication and control solutions will be introduced, along with a timeline projected for introduction into each identified market.

9. Project Results

In Phase I of this project, we developed a proof-of-concept ACCP system and architecture and began to test its functionality at real-world sites. These sites had just over 10 MW of DERs and allowed us to identify what needed to be done to commercialize this concept.

As a result, we started Phase II by looking at our existing platform and identified its strengths and weaknesses as well as how it would need to evolve for commercialization. During this process, we worked with different stakeholders in the market including: Independent System Operators, DER owners and operators, and electric utility companies to fully understand the issues from all of the different perspectives.

Once we had an understanding of the commercialized ACCP system, we began to document and prepare detailed designs of the different system components. The components of the system with the most significant design improvements were: the on-site remote terminal unit, the communication technology between the remote site and the data center, and the scalability and reliability of the data center application.

As we began to implement the Phase II ACCP system, we upgraded the real-world demonstration sites from Phase I of the project as well as added additional sites to broaden the types of DER the platform was tested with. We worked with the owners and operators of these sites to understand how the system was meeting their needs and made modifications throughout the project as needed. This also included an effort to continue to understand the barriers to commercial adoption of the ACCP architecture and standardized communication protocols.

The final aspect of this phase of the project was to prepare resources to aid in the commercial adoption of the ACCP architecture and standardized communication protocols. This entailed: presentations at conferences, published articles and papers, and web-based technical resources to provide tools to aid in the design and implementation of ACCP systems.

ACCP System Overview

The Advanced Communication and Control Platform has two key pieces:

- **Remote Component** - System components installed at the site physically connected to the DER. The hardware components are typically installed in a Remote Terminal Unit (RTU) that contains the *CENTRY*wcc® (WCC) intelligent controller and other input/output modules that may be required for the site. The WCC communicates securely over the Internet to the data center using a proprietary VPN technology known as ener*TIE*™.
- **Data Center Component** - This component provides the majority of the data aggregation capabilities and the advanced data analysis, display, reporting, and alarm functionality. This component contains the servers used to present the web application to the end user. A deployment typically has a single data center.

The platform encompasses all of the hardware and software in both of these pieces as well as the bi-directional interactions and communications. A functional diagram of the system is shown below with the data center in the upper half of the diagram and the hardware installed at the site on the bottom:

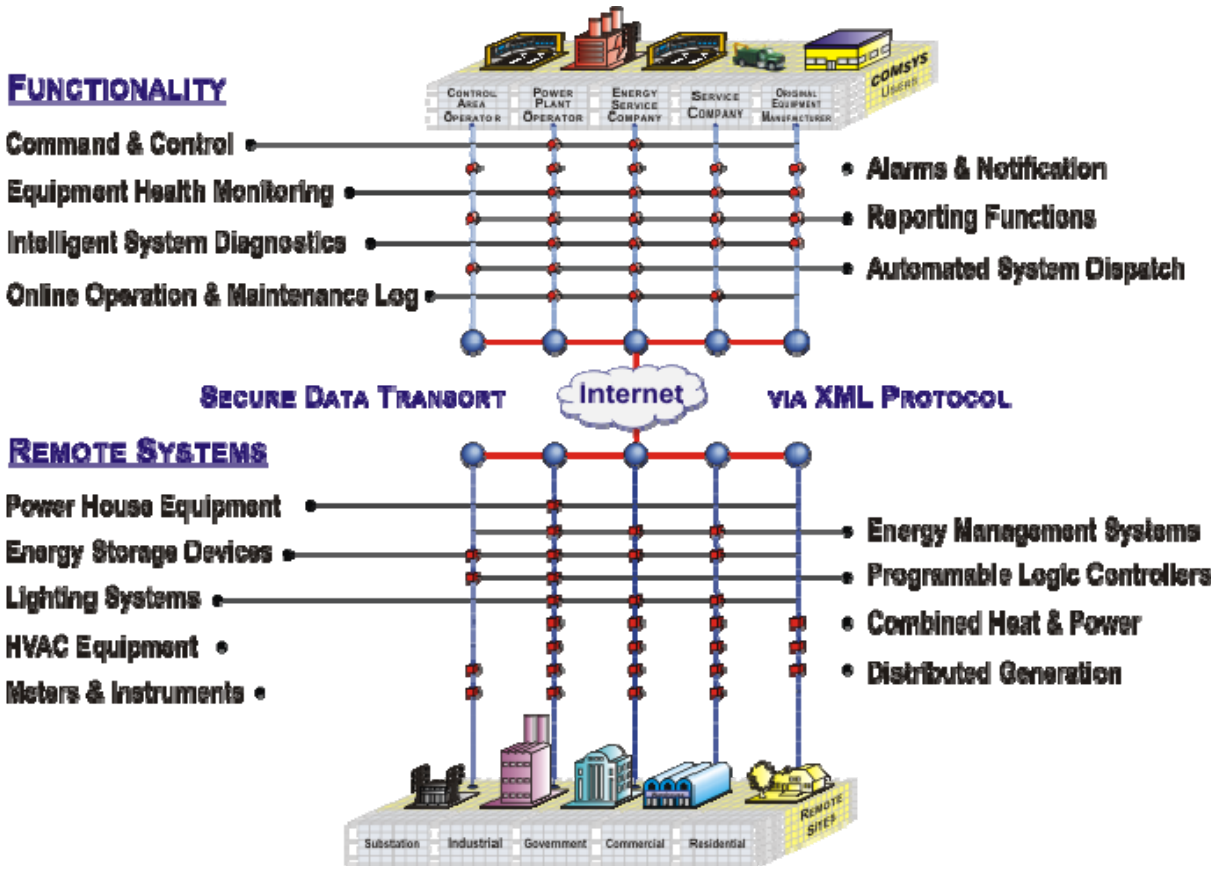

Figure 1: ACCP Functional Diagram

Figure 2 below depicts the high-level architecture of the Phase II ACCP system. The top portion of the diagram depicts various types of DER and shows the bi-directional communications between the physical DER equipment and the data center. This communication utilizes the standard ener*TALK*™ protocol. In addition to DER, other data sources are shown and integrate with the system in the same way as the DERs. The possibilities for these data sources are endless but may include: weather data feeds, pricing data, or SCADA data.

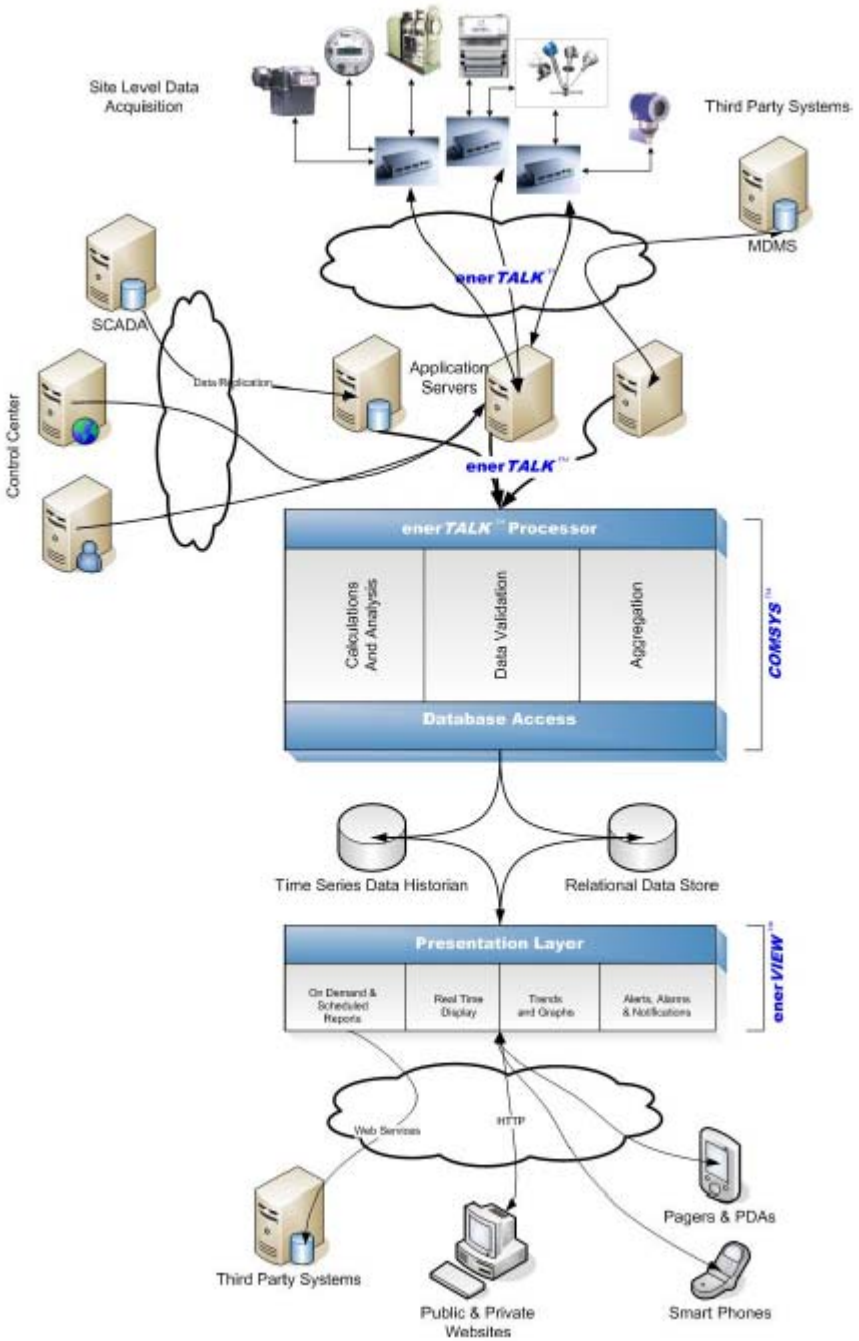

Figure 2: High-Level ACCP Architecture

Below the DERs and data sources is the core data center application. This is split into three pieces. The COMSYS™ layer which processes the ener*TALK*™ messages and provides data services such as: validation, aggregation, calculations, and other analyses. Once the data has been fully processed, it is sent to the second layer which archives the data in either a time series historian or a relational data store depending on the type of data. Data automatically flows from the DERs and data sources into the database regardless of any users who may currently be accessing the system.

The final piece of the system is the presentation layer. This is known as ener*VIEW*™ and is responsible for providing: the web based data display, alarming, reporting, and other related services. In some applications, it is necessary to export the archived data to third party systems which also occurs through this layer.

Authentication and authorization mechanisms are in place at all external touch points of the system. This includes both the presentation layer as well as the devices that communicate with the ener*TALK*™ processor. In addition, encryption technologies are utilized at both ends of the system to protect all data exchanged over the Internet.

ACCP Security

One of the key deliverables of this phase of the project was a Security Protection Profile (SPP) developed by Sandia National Laboratories. This profile sets security standards for advanced communication and control platforms and sets the baseline for the security requirements of the Phase II commercialized implementation of this system.

The diagram below was prepared by Sandia National Laboratories and is contained in the Security Protection Profile. This shows a high-level diagram of the ACCP system identifying the areas included in the security profile by the cyan ellipses.

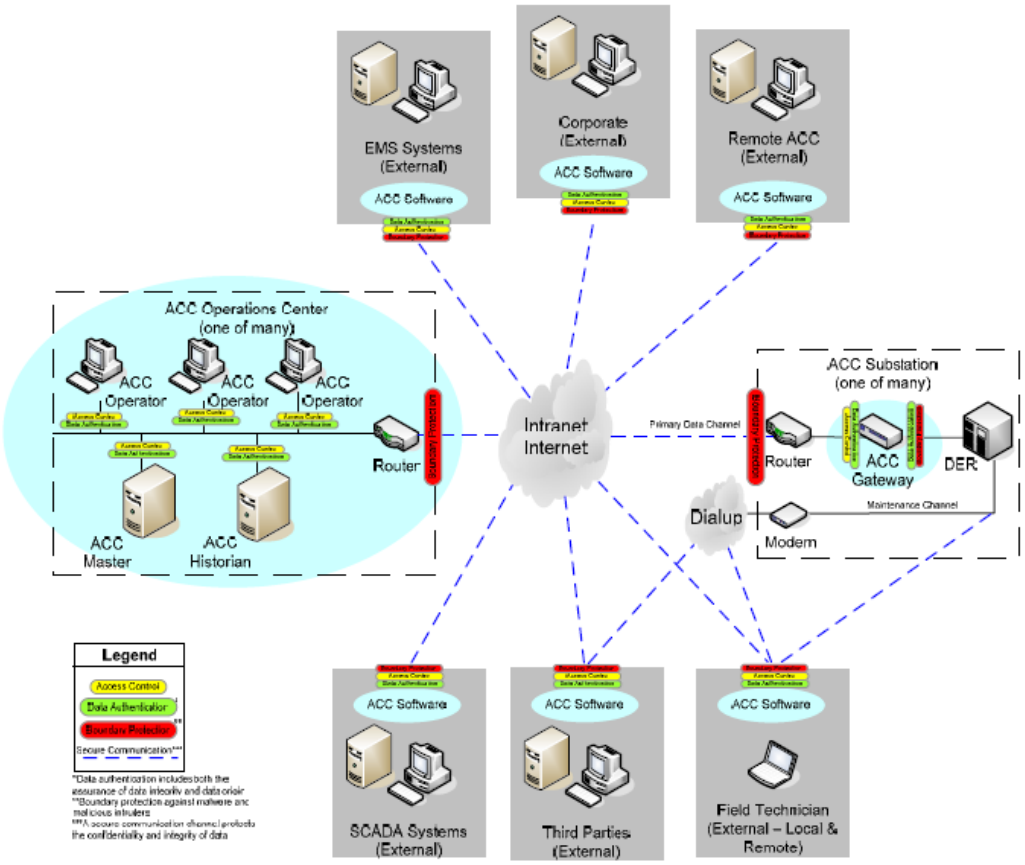

Figure 3: High-Level ACCP Architecture Covered in SPP

Results

The current implementation of the ACCP system meets the security criteria outlined in this Security Protection Profile. However, one possibility for further improving the security in a future release of the platform would be to use application layer authentication and authorization in the backend data center systems as well as within the WCC. This change would not create any noticeable difference to users of the system but would enforce security constraints on each component trying to access other parts of the system. The system should also be

extended to cryptographically sign each software component allowing the system to verify the authenticity of the code. This would help protect against the insertion of rogue processes masking themselves as valid system modules.

CENTRYwcc® - Premise Remote Monitoring Terminal

Overview

The *CENTRY*WCC® is an intelligent controller that is located in each of the Remote Terminal Units (RTU) installed physically at the site near the DERs. This controller is responsible for communicating with DERs and related metering at the site using the native, proprietary protocols utilized by these devices. It takes these protocols and translates them bi-directionally to a standardized protocol (ener*TALK*™) used to communicate with remote system nodes. The most common remote system node is a data center hosting an application allowing an operator to remotely interact with their DERs.

The WCC communicates with the data center and other remote nodes through a standard Internet connection. Due to the insecure nature of this type of network link, all of the data exchanged with remote nodes needs to be protected. Prior to Phase II of this project, a hardware virtual private network (VPN) appliance was installed in the RTU that provided authentication, authorization, and data protection services for the WCC. The WCC is connected to this appliance using a standard Ethernet link. This was one of the areas significantly enhanced during this phase of the project.

In addition, the WCC provides local data buffering and advanced aggregation and calculation capabilities. The local data buffering allows the WCC to protect against network outages between the RTU and the remote system node thereby improving the reliability of the entire system. Without this capability, the WCC would not be able to utilize an inherently un-reliable network such as the Internet for its communication with the data center.

The data aggregation and calculation capability allows the WCC to locally compute values based on the data being monitored from the DERs in real-time. This is an important capability for the system as it provides the following benefits:

- Distributes computing load allowing the data center to support a greater number of DERs
- Allows the WCC to support mode advanced local control that requires more complex input data versus the raw data values read from the DER
- Simplifies installation of the RTU by allowing the technician to more completely validate the data before leaving the site

Phase II Improvements

During Phase I of this project, we identified the need for improving the security of the WCC in several areas. This was a priority requirement for Phase II of the project as a result of input from stakeholders and the vision of the Department of Energy. While the original WCC provided some protections against attacks,

assumptions were made around how the WCC was deployed that would not necessarily hold for all commercial deployments.

The primary focus of these security improvements was on the communication uplink channel between the WCC and the remote data center. However, we also addressed security weaknesses in three other areas:

1. WCC Physical Input/Output (I/O) Port Access By External Devices
2. Authentication and Authorization of Users Permitted to Administer the WCC
3. General Hardening of the WCC Software Operating System

In addition to security improvements, the WCC was upgraded to support the new version of ener*TALK*™ also developed under this phase of the project. These enhancements allowed for: an additional layer of security, greater flexibility around the types of control and messages that can be dispatched to the WCC, and improvements to the type of data that can be exchanged with remote nodes. We identified the need for these changes based on the specific types of DER deployed in Phase I and those planned for Phase II.

We also made numerous improvements to help reduce the time requirements to deploy and maintain the WCC. These improvements were largely in the form of enhancements to the automated health monitoring capabilities of the WCC as well as streamlining the configuration process. In Phase I, we discovered that in certain situations, it was time intensive to manage WCC deployments and thus needed to improve this for commercialization of the component.

Finally, modifications were made to further improve the performance of the data monitoring capabilities of the WCC. In Phase I, we were able to acquire data from DERs and transmit the data to the network operation center in less than one minute. Through improvements made in this phase of the project, we were able to increase the number of data points that can be monitored by the WCC as well as reduce the processing latency in the WCC by several seconds. As a result, the average time for the WCC to process the data collected from the devices and begin to send it to the data center is now 5 seconds.

Security - Communication with the Remote Data Center

As one of the first tasks completed under this phase of the project, we designed, implemented, and tested an embedded secure virtual private network software client for the WCC. This application replaces the hardware VPN appliance installed at the Phase I demonstration sites and is focused on additional security in the authentication and authorization aspects of the remote communication. It was also designed to provide flexibility around the encryption technologies utilized to allow the application to easily adapt to ever changing cyber security requirements.

This embedded virtual private network software client provides additional protections to ensure that WCCs are only permitted to communicate with data center services applicable for their provisioning. It also protects against non-

authentic or non-configured WCCs from opening up a connection to the data center.

In addition, the Phase I sites utilized a non-secure communication link between the WCC and hardware VPN appliance. This created the possibility for someone with local site access to insert hardware on the internal RTU network to access the remote data center as well as view the data being exchanged between the WCC and data center. With the embedded VPN client approach in Phase II, this security threat is eliminated as the end point for the secure communication resides within the software on the WCC.

The removal of the hardware VPN appliance also substantially reduces the cost of the RTU and simplifies deployment. In Phase I, we identified that while the hardware and installation costs were generally fixed regardless of the size of the DER being integrated into the system, the cost was prohibitively high for small DER resources. For a site with 15 kW of DER, this modification results in a cost reduction of roughly $35 per kW while enhancing the security at the same time.

The embedded virtual private network client and server application is discussed in additional detail in a subsequent section.

Security - Physical I/O Access

The Phase I proof of concept WCC product had no protections on any of its input/output (I/O) communication ports. Due to the fact that most of the security that can be applied to these I/O ports is specific to the protocols being utilized, there are limited options for generic improvements in this area. However, we identified this as a risk that needed to be addressed as it provided an unsecured entry point for an adversary to attack the system or attempt to inject invalid data.

As a result, in Phase II, we focused on the second Ethernet port on the WCC hardware and added an intelligent firewall that manages access to ensure that only connections required for proper WCC operation are permitted. The firewall operates in as much of a stealth mode as possible meaning that it does not send any responses whatsoever to connection attempts to blocked ports.

As part of limiting access to only essential services, we also exposed services such as HTTP or SSH to specific static IP addresses versus allowing access from any device on the network. The intent is that a site technician could access these services to configure and administer the WCC while at the same time reducing the likelihood of a user not familiar with the system to be able to connect. In addition, this in conjunction with the highly granular firewall reduces the risk of a local denial of service (DoS) attack by preventing local adversaries from attempting to break into services running on the WCC.

Security - Authentication/Authorization of Administrative Users

The Phase I WCC only utilized a single user account for access to the system for administrative purposes. This account had no access limitations allowing anyone who was able to gain access to this account the ability to have full control of the WCC. While protections were in place to limit who could attempt to login, enhancements were made to the login process for the Phase II WCC.

In the design phase, we considered the use of a two-factor authentication system for administrative access to the WCC. However, using any kind of hardware based token introduced significant usability and business process implications. As a result, the strategies discussed below were employed to resolve this problem.

1. Modified the deployment, configuration, and maintenance processes to reduce the need for highly-privileged login accounts in day to day operations on the WCC
2. Imposed restrictions on the length and quality of the passwords utilized for login accounts on the WCC
3. Created several login tiers and only permitted full access to the system by first logging in as a less privileged user
4. Added protections to log all access to the system and to detect attempted malicious use of the system

We found that the implementation of these strategies adequately protected the system. Due to the fact that multiple passwords needed to be cracked in order to gain full access to the system and due to the password quality constraints, the time to break into the unit using currently viable attacks would not be feasible. In addition, the time it would take to execute such attacks would cause the WCC to detect the attempted malicious access triggering action by an administrator of the system.

While no password change procedures were enforced by the system, the Phase II WCC allowed for greater flexibility of password management allowing for such a procedure to be supported with greater ease.

Security - General Hardening

While identifying and designing the changes to the WCC for Phase II of the project, an effort was made to carefully inspect the entire WCC and operating system configuration to identify areas for additional hardening. As a result of this work, several configuration changes were made that further improved the overall security of the system, specifically surrounding the underlying operating system.

Results

The updated WCC met its objectives during the demonstration site testing. We were able to demonstrate that with the significant architectural changes made to support the improved security policy, the WCC was still able to satisfy its functional requirements. We also did not identify any reliability implications as a result of the modifications.

One of the initial concerns raised in the design phase of the project was the potential performance impact of the additional processing overhead required for the encryption of data. As a result, we performed extensive load and scenario testing of the performance characteristics of the WCC utilizing the embedded virtual private network client in our test lab. We found no significant performance impact to the system during normal operation. The encryption overhead is apparent when the data throughput on the data center uplink starts to exceed several megabits per second, although it is still low enough that it does not impact the normal operation of the WCC.

In our test lab, we also performed numerous security attacks on the system in an attempt to validate that the security goals were achieved by the enhancements. We were not able to maliciously attain access to the system or compromise any component of the WCC during this testing.

As a result, the WCC developed during Phase II of this project was deemed ready for commercial adoption for use in monitoring and controlling DER. However, future improvements should be made to further simplify the deployment process. It is expected that this work would primarily take the form of a set of tools that would assist a technician with preparing, validating, and installing a configuration on the WCC. Also, future work should include additional tools for the management of a fleet of installed WCCs. These tools would further reduce the fixed and variable deployment costs associated with this solution.

While not a barrier for immediate commercial adoption, it is recommended that physical security mechanisms be explored to protect the WCC and related hardware components installed at the site. One of the mechanisms specifically discussed was an anti-tamper sensor that could be used to detect and potentially disable the operation of the WCC if the unit was physically tampered with. Similarly, protections or sensors installed within the RTU itself could also be valuable for the same purposes. A physical security policy and standard should be established such that DER manufacturers and ACCP implementers can more easily convey the physical security features and risks associated with their equipment.

In addition, using an encrypted file system on the WCC and other hardware appliances within the RTU should be investigated further. This would continue to reduce the risks of physical attacks if implemented correctly. However, since this solution could have serious performance implications, hardware based solutions embedded within the WCC and other appliances should also be included in the analysis process. A policy and set of standards should be established that define how this type of solution should be implemented possibly providing for several levels of security based on the specific needs of the DER.

enerTALK™ - Protocol Standard for DER Interoperability

Overview

ener*TALK*™ is a standard XML-based open protocol designed to integrate and promote interoperability between DERs. It is an asynchronous request/response protocol and is designed to be flexible and expandable to support all types of DER. ener*TALK*™ is used to exchange data between nodes in a network of DERs that typically involves reporting data collected from equipment at a site to a remote data center as well as dispatching remote control requests and service invocations.

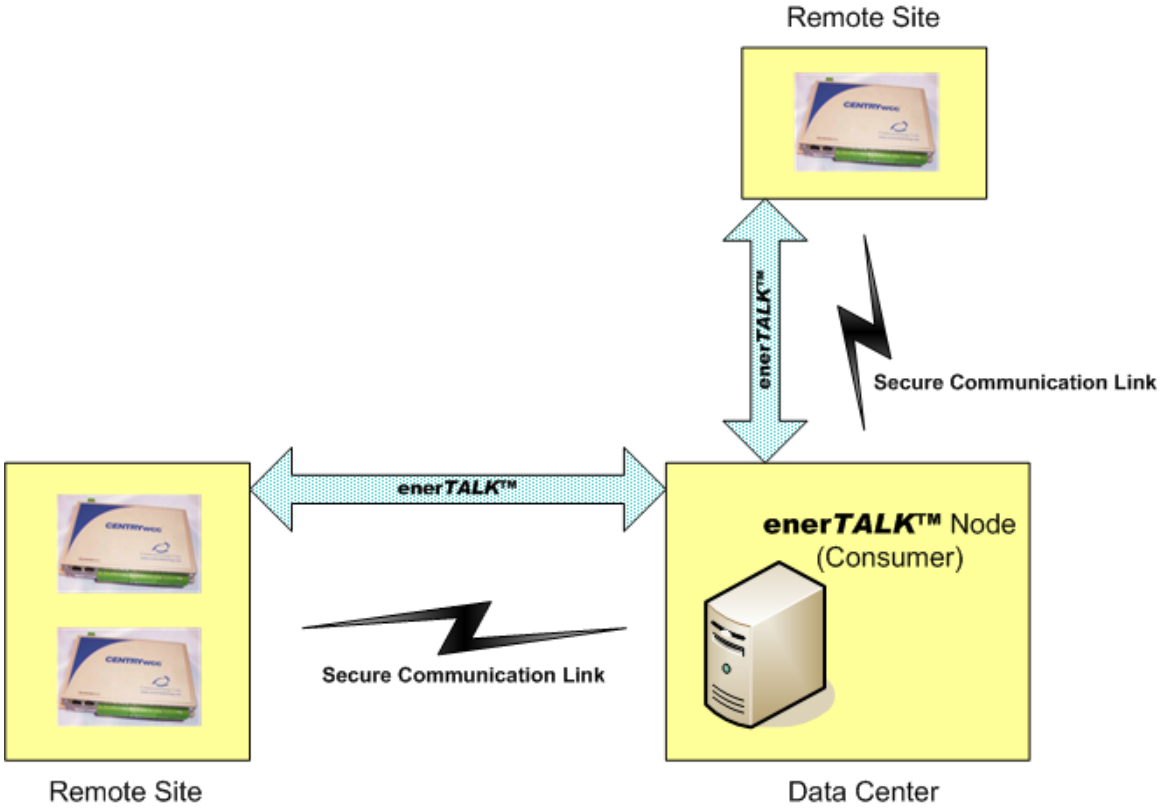

Figure 4: enerTALK™ High-Level Network Diagram

Figure 4 depicts a typical ener*TALK*™ system showing the communication between remote sites and a data center. The ener*TALK*™ protocol provides authentication and authorization capabilities as well as the ability to ensure data integrity. However, it does not provide data protection such as encryption. As a result, a secure communication link is typically used when ener*TALK*™ is exchanged over non-secure networks such as the Internet.

In Phase I of the project, initial versions of the ener*TALK*™ protocol were developed that supported basic service invocations and the transmission of time-series data. The service invocations that initially were supported allowed an ener*TALK*™ node to send a start, stop, reset, or setPoint command to a device connected to a remote ener*TALK*™ node. It supported running these commands either immediately or at some time in the future.

Based on what was learned early in Phase I, a major new version of ener*TALK*™ was conceptualized to include built in authentication and authorization capabilities, message signing, and additional flexibility in the representation of data values and control dispatches in the message. This version of ener*TALK*™ was not fully designed or documented during Phase I of the project and is known as ener*TALK*™ 3.0.

Phase II Improvements

During Phase I of the project, several key weaknesses were identified in the initial version of the ener*TALK*™ protocol:

- Limited Flexibility for Control/Command Requests
- Lack of Support for Relational (Non time-series) Data
- Limited Error Reporting Capabilities

These limitations introduced problems in supporting the Phase II demonstration sites as well as served as a barrier to commercial adoption of the protocol.

In addition, the ener*TALK*™ message routing capability initially conceived in Phase I needed to be implemented to support the upgrades to the demonstration sites. While designing the structure of this capability, it was decided that a mechanism to add metadata to an ener*TALK*™ message would be required. This metadata capability (known as ener*TALK*™ directives) not only aids message routing but also provides an extensible way to add any metadata to the message.

During Phase II, additional design work occurred on the node authentication and authorization capabilities of ener*TALK*™ 3.0. However, due to staff and scheduling constraints imposed by other ener*TALK*™ implementation tasks, nodes that fully supported these features were not implemented or deployed as part of this phase of the project.

Control Request Flexibility (Properties Interface)

One of the big weaknesses identified in the Phase I version of the ener*TALK*™ protocol was the lack of flexibility in representing control requests in the messages. The initial representation was extremely rigid and made assumptions about the types of operations that could be performed on the remote equipment. While this set of operations covered control applicable to a wide variety of DERs, it

did not easily expand to support the richer set of commands supported by other pieces of equipment.

As a result, the ener*TALK*™ Properties Interface was developed. This interface provides a common framework for issuing requests on a remote node. A remote node utilizing the properties interface has one or more components that can process these requests. These components are known as entities.

Each entity has a set of properties that it is responsible for servicing. These properties are extremely flexible and are based on the type of entity. As an example, a small generator may have the following properties:

- **Engine Switch** - turns the engine on or off
- **Target Power Output** - specifies the desired output of the generator

Through the properties interface, a remote node can issue a "getProperty" request to query the value for either of these properties resulting in the entity responding with an ener*TALK*™ message containing the current value. Alternatively, a remote node can issue a "setProperty" request to change the value of either property such as turning the engine on or off or changing the desired power output.

Figure 5 below shows how an ener*TALK*™ message issuing a request to the properties interface gets processed by an ener*TALK*™ node. The implementation of this interface on the WCC first provides a component that parses the message, validates and authorizes its contents, and then routes it based on the entity to an appropriate handler. This handler is then responsible for servicing the request sending a response message to the requesting node.

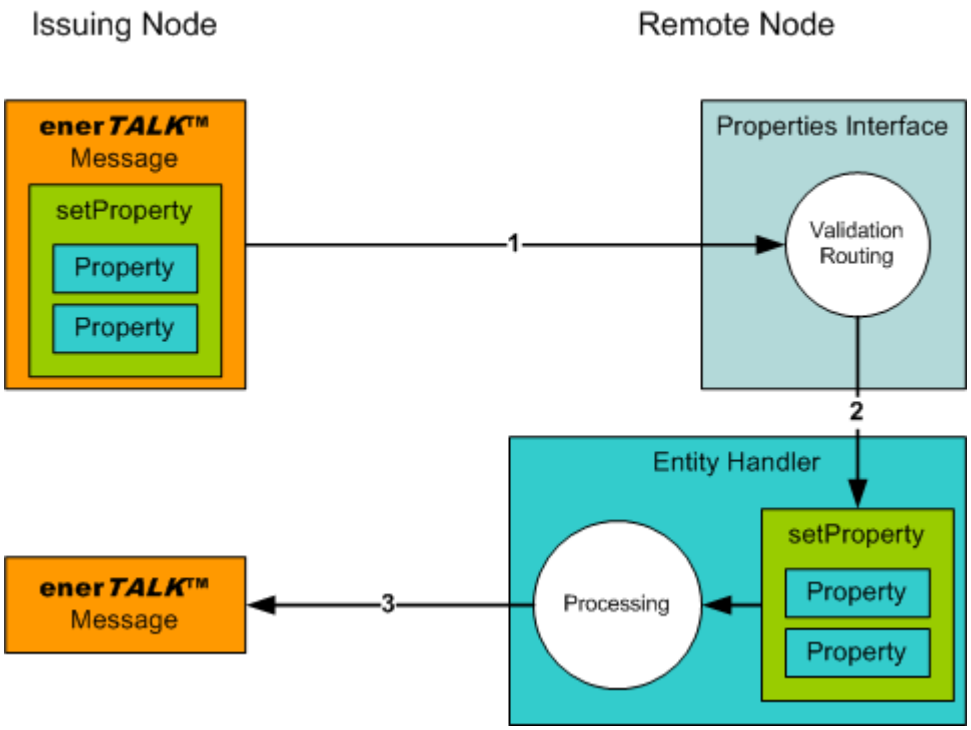

Figure 5: enerTALK™ Properties Interface Message Processing

Non Time Series Data

The Phase I version of the ener*TALK*™ protocol only supported time-series data as that typically is the format of data collected from DER and related metering. However, we quickly saw this as a limitation as we began to explore more advanced functionality in the WCC appliance and the data center that required acting on different types of data.

Specifically, as we began to plan for the LACSD Calabasas Phase II demonstration site, we identified the need to be able to represent relational data in ener*TALK*™ messages. The smart agent technology deployed at the site utilized weather forecasts that needed to be sent to the WCC from the data center. Using the Phase I version of ener*TALK*™, it was not possible to naturally represent this data in the constructs of the old message schema.

As a result, we added the capability to ener*TALK*™ to support non time series data. Due to the nature of this type of data coupled with the self-describing attribute of the ener*TALK*™ protocol, additional metadata is needed to aid in the parsing of the message. This metadata is configured on the consuming ener*TALK*™ node and is known as a template. When the issuing node prepares an ener*TALK*™ message containing this type of data, the name of the template that the consumer should use is specified as a textual string.

Utilizing metadata to aid in the parsing of non time series data allows the schema to be more flexible in how data is represented in the message. Typically, this type of data is represented by having a single XML element that contains an instance of relational data (equivalent to a row in a relational database table). Within this single XML element is zero or more additional elements that contain the specific data for that instance (the columns in a database table).

Sample ener*TALK*™ messages are provided in the appendix that shows one possibility for representing relational data.

Error Reporting

As a commercialization plan was being developed for ener*TALK*™, it became evident that a richer set of common errors needed to be supported as well as a mechanism that allows a specific implementer to define their own error codes. This capability did not require any changes to the ener*TALK*™ message but did establish a set of standardized error codes that are common among many types of DER. These error codes are split into several categories allowing for an easy classification of errors by the consuming node.

enerTALK Directives

In the design phase for the new features of ener*TALK*™, it became evident that a mechanism was needed to add metadata to the messages to aid in processing and routing. Support for metadata was implemented in ener*TALK*™ 2.7 and is known as ener*TALK*™ Directives. These directives are simple name-value pairs that occur outside of the main XML element in the messages. The table below shows common directives and their descriptions although implementers of ener*TALK*™ can add other directives as needed.

Directive Name	Directive Value	Description
archiveUntil	ISO 8601 Timestamp	The time the message should be removed from any archive.
dataSource	String	The source of the data contained in the message.
dateCreated	ISO 8601 Timestamp	The time the message was generated.
generatedBy	String	A string indicating which service generated the message.
messageExpires	ISO 8601 Timestamp	The time the message expires.
msgid	Unique ID	A unique ID for the ener*TALK*™ message.
postTo	Network Address	An address of the node the message should be sent to.

enerTALK Message Routing

In Phase I of the project, initial planning began for the structure of ener*TALK*™ networks and the concept of ener*TALK*™ message routing came to life. There are three typical roles of an ener*TALK*™ node in a deployed system:

- **Producer** - a node that generates an ener*TALK*™ message
- **Consumer** - a node that receives and processes an ener*TALK*™ message
- **Conduit** - a node that relays a message but does not process it

The diagram below depicts an example ener*TALK*™ network showing the interactions between these types of nodes:

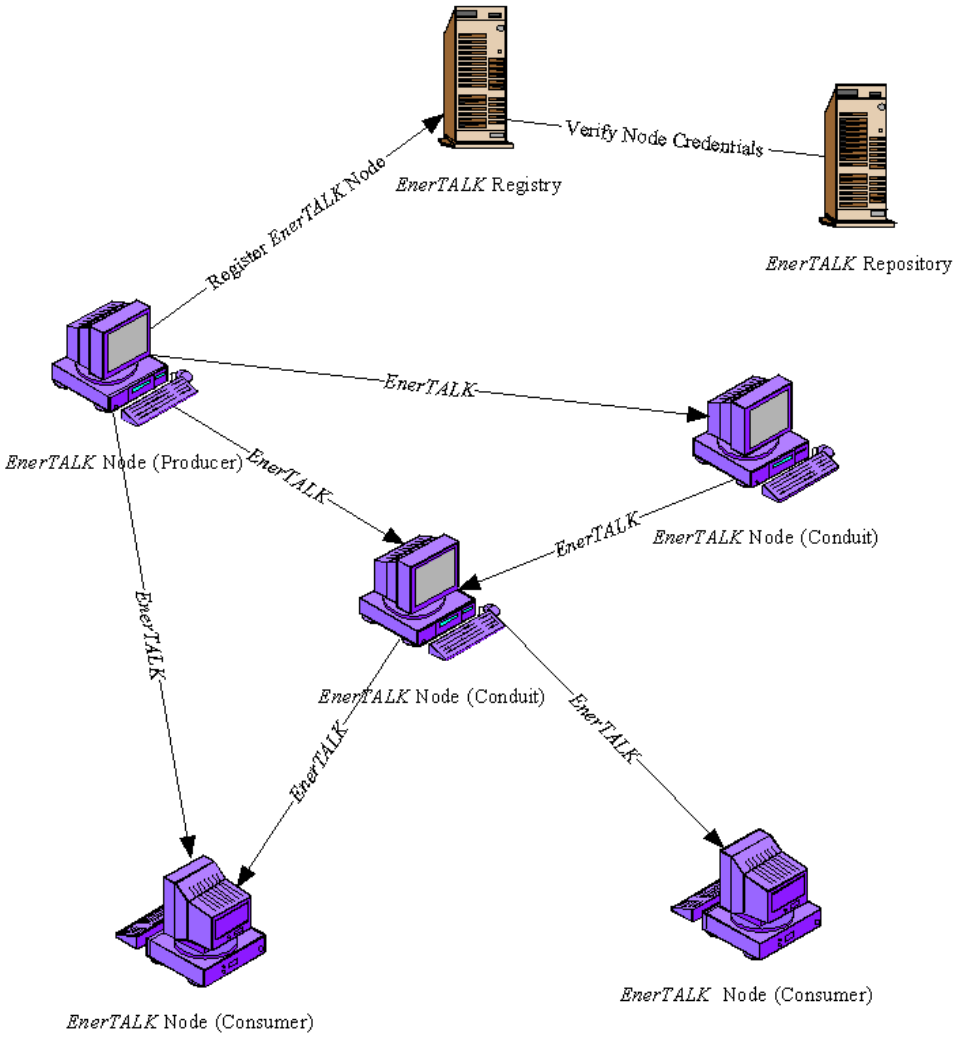

Figure 6: enerTALK™ Network Diagram

At any given time, an ener*TALK*™ node can only act in one of the different roles. However, it is typical for a single node to be able to act in different roles at different times. As an example, a WCC is both a consumer and a producer of ener*TALK*™ messages and can be a conduit in certain applications.

Role of enerTALK™ in DER Networks

As we designed the new version of ener*TALK*™, we looked at characteristics of other common DER communication protocols. A comparison of these protocols in relation to ener*TALK*™ 3.0 is presented in the table below.

The majority of DER equipment utilizes protocols that are fairly low-level and are designed to present the devices being monitored in a very specific way. The

rationale behind this structure is that it maps very closely with the role that DER plays in the overall network. On the other hand, ener*TALK*™ is higher-level and seeks to put this low-level DER data in context of the entire DER network and the associated business processes.

	ener*TALK*™ 3.0	Modbus, Canbus, DNP3	Equipment
Protocol Type	• High-Level Protocol • Application Level abstractions	• Interface Protocol	• Application Semantics (models of devices and applications)
Protocol Focus	• Aggregation Centric	• Interface Centric	• Data/Transaction Centric
Design Rule	• Enable Interoperability and aggregation	• Optimize use of bandwidth and hardware	• Simplify device engineering; Reuse Models
Transaction Paradigm	• Exchange of domain specific messages	• Exchange of numbered lists of sample data	• Modeling of application objects
Service Level	• Service activation	• N/A	• Models exchange of I/O and metadata for services
Security	• Integrated, multi-layer • AAA services	• N/A	• N/A

As a result, ener*TALK*™ serves a different role in the entire DER network than many of these other protocols were designed to do. Rather than taking a design approach of adopting these low-level protocols into a standardized protocol suitable for inter-DER communication, ener*TALK*™ instead was designed from the other direction and builds a protocol around the true requirements for an interoperable DER network communication protocol. As a result, ener*TALK*™ is strongly positioned to meet the needs required for such a protocol.

The primary design goals of ener*TALK*™ are as follows:

- Shared Services
- Shared Information Models
- Shared Protocols
- Integrated Security

Results

The implementation of the ener*TALK*™ Properties Interface and the support for non time-series data worked well to support the Phase II demonstration sites. The current version of ener*TALK*™ supports the majority of scenarios expected to be seen in creating networks with DERs.

However, one of the key features that need to be included in a future version of ener*TALK*™ is the ability to automatically validate the message using a technology such as XSD. With the current ener*TALK*™ schema, it is not possible to fully validate the message due to the dynamic XML element names that change based on the identifier for the data value being exchanged. In addition, the current implementation of the non time-series data also suffers from the same weakness, although it may be alleviated somewhat through the use of the template metadata files.

Automatic message validation is critical as ener*TALK*™ is adopted among equipment manufacturers. When consuming messages prepared by other nodes, it will become more important to validate the message to ensure data types are properly enforced, the message is properly structured, all required elements are present, etc. If ener*TALK*™ implementers are expected to develop their own validation techniques, it is inevitable that numerous problems will arise as a result of vendors rejecting valid messages or attempting to process invalid messages. Although utilizing a standardized technology (such as XSD validation) to resolve such issues, it will not guarantee that these problems do not arise. However, it will simplify supporting validation and result in a more standardized approach to message acceptance and rejection. This ultimately will increase the overall reliability and interoperability of networked DER.

In addition, the naming hierarchy used to identify data values for time-series and non time-series data is rigid and makes assumptions about the topology of the DER. Each DER or piece of equipment is associated with exactly one site. A site has zero or more pieces of equipment and is part of exactly one organization. An organization may have zero or more sites that are part of it. These constraints simplify the representation of DER in the system by imposing a constraints on how it is organized and presented. The diagram below depicts this hierarchy.

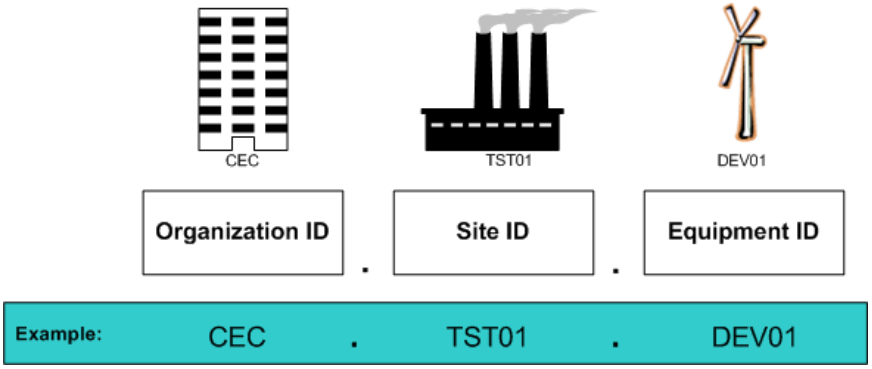

Figure 7: enerTALK™ Data Point Naming Hierarchy

For the Phase I and II demonstration sites, this naming hierarchy worked well although it may need to have greater flexibility to accommodate adoption of ener*TALK*™ by more equipment manufacturers.

Finally, ener*TALK*™ should be expanded to have a common, standardized way to extend the protocol. As an example, some equipment manufacturers could benefit from using ener*TALK*™ nodes and infrastructure to route opaque messages or data such as updates or binary data to a remote node. In these situations, there is no clearly defined way of utilizing ener*TALK*™ to exchange this data. By developing a standard before vendors begin finding their own solution to this problem, compatibility issues between one implementation of ener*TALK*™ and another will be avoided.

enerTIE™ - Remote Terminal Unit Secure Connectivity

ener*TIE*™ is a client/server secure virtual private network software application developed to secure the communication uplink between the remote DER and the data center. It uses a multi-tier authentication process, has a user authorization component, and is encryption algorithm agnostic allowing for maximum flexibility in deployments.

In Phase I, communication security was obtained by deploying a hardware virtual private network appliance at the site. While this protected the communication occurring over the Internet, it had the following problems:

- Limited flexibility around user authentication and authorization
- Lack of two factor authentication
- Limited flexibility around encryption algorithms used
- Time consuming to administer and deploy new sites
- Not compatible with all Internet connections due to its use of IPSEC
- Expensive hardware device required in each RTU
- Gap in the security between the hardware VPN appliance and the WCC. This link was not protected in any way.

As a result, several alternatives for this hardware based VPN approach were considered. Due to the deployment costs of a second piece of hardware solely responsible for encrypting network traffic, software based solutions that could be embedded within the WCC were the only viable options. In the end, it was determined that developing a proprietary client and server application was the best way to support the required features as well as have the security capabilities required for DER communication networks.

The high-level required feature set of this virtual private network application are as follows:

- Two-factor user authentication.
- Ability for the client to verify the authenticity of the remote server.
- Authorization policies on the server that can be applied to user accounts and groups. These policies are applied to fully authenticated users to grant them access to the required network resources for the site.
- Transparent encryption of all data exchanged between the client and server utilizing strong symmetric encryption algorithms.
- Complete logging and audit trail of connections from clients as well as administration of the server.
- Ability to route IP traffic over the secure connection to and from the WCC.
- The WCC must establish the connections to the server and not require a public IP address on the Internet to work correctly.
- Underlying network traffic must utilize TCP to allow for data traversal of encrypted network packets without the modification of corporate firewalls and routers.
- Load balancing and fault tolerance support allowing a WCC to automatically connect to one of several different servers based on server availability and load.

- Flexibility to utilize different encryption algorithms and key-sizes as applicable to allow the application to adapt to changing security requirements or site/customer specific needs.
- Utilization of encryption algorithm implementations that is well supported and tested such as OpenSSL.
- Keys utilized for the encryption of exchange data must be generated for each connection by the application. These keys must be able to be regenerated periodically after a certain amount of data has been transferred or a certain amount of time has elapsed.
- Dynamic firewalling on both the client and the server to modify the firewall as needed to only permit required traffic to traverse the filters.

In addition, the application must provide protections against common security problems including but not limited to the following:

- Man in the middle attacks
- IP address spoofing
- DNS spoofing

Figure 8 on the following page shows the topology of the client and server application as well as the connection sequence going from a non-authenticated user to a fully authenticated user who can access the system. From the time a client connects, they have 2-minutes to successfully complete both authentications otherwise they will be disconnected. The failure of either authentication or if the user account has been disabled will cause the account to be disconnected immediately.

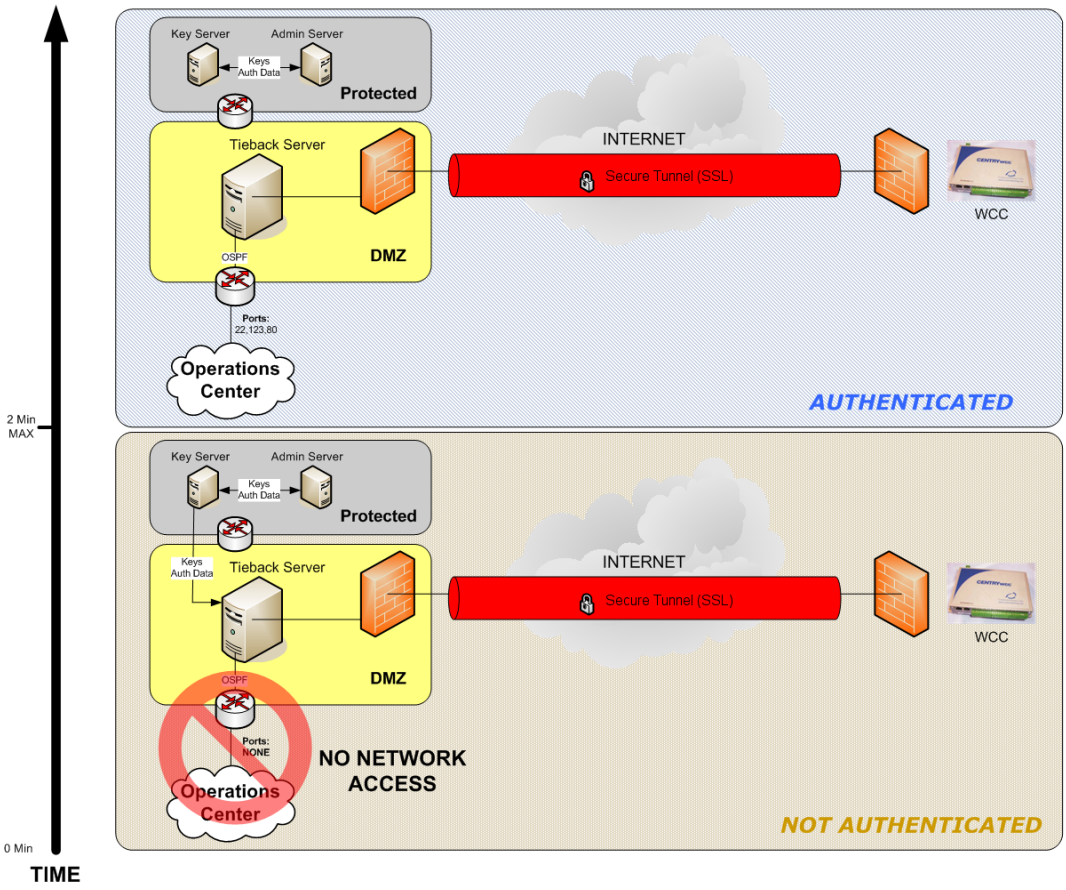

Figure 8: enerTIE™ Overview

In the diagram, the firewall and secure tunnel terminate within the WCC and the ener*TIE*™ server on each side. This means that no traffic traversing the secure tunnel ever leaves either piece of hardware unencrypted. Since the application protects against man-in-the-middle attacks, the attempt to place a rogue node in between the client and the server will not allow the adversary to access any protected data or compromise the system.

Lab Testing

After the initial version of ener*TIE*™ was developed, it underwent extensive security, reliability, and performance testing prior to deployment at any Phase II demonstration sites. The goal of this process was to ensure the satisfaction of the high-level requirements previously discussed.

In addition, Sandia National Laboratories reviewed the detailed architecture and underlying technologies utilized in this product from a security perspective. The results of this analysis are presented in their report “High-Level Assessment of CE DER ACC Security Architecture” prepared under the scope of this project.

Phase II Demonstration Site Testing

After the ener*T/E*™ security product had been tested and reviewed, it was deployed to three of the Phase II demonstration sites. This was only deployed to a subset of the sites due to the need to have a technician visit the site to migrate it from the hardware VPN solution to the software based ener*T/E*™ solution. The following demonstration sites were upgraded:

- LACSD Calabasas Landfill
- LACSD Palmdale Water Reclamation Plant
- NYSERDA Greater Rochester International Airport

Based on the testing performed at these sites, ener*T/E*™ was found to be a reliable, secure, and a manageable security component. In addition, the two LACSD sites utilized a cellular modem for Internet connectivity resulting in higher communication latencies which were found to be reliable and compatible with ener*T/E*™.

All of the testing at the Phase II demonstration sites utilized 2048-bit DSA keys for one of the two authentication tiers. In addition, 128-bit Blowfish keys were utilized as the symmetric algorithm used to protect the data exchanged over the secure tunnel. Among other algorithms, ener*T/E*™ currently supports the Advanced Encryption Standard (AES) algorithm using keys from 128 to 256 bits. Due to the flexibility of the design, different sites can utilize different algorithms and new algorithms can be easily supported.

Results

The Phase II testing of ener*T/E*™ was successful and the product was found to meet all of the security and functional requirements. In addition, we worked with a variety of information technology (IT) personnel to explore the compatibility of the ener*T/E*™ product with their networks. We found virtually all networks to be compatible with the technology as a result of it utilizing standard TCP packets and since the WCC establishes a connection to the server instead of requiring an inbound connection from the Internet to the WCC. The only network incompatibilities were from corporations that filtered outbound traffic from their networks and in these situations, most were amenable to permitting ener*T/E*™ traffic as approved outbound communications.

While ener*T/E*™ provides many built-in security protections not currently available in typical virtual private network hardware appliances, it may be worth considering further enhancements in the future to improve its inherent security. Specifically, the automatic re-generation of authentication credentials (pre-shared keys used in the authentication process) should be considered as a way to more actively protect against potential attackers.

In addition, the presentation of additional login credentials or data during the second-tier authentication could be an easy way to further secure the system. In

particular, if a hardware serial number or value unique to each WCC is available and secure from spoofing, this could be used as a mechanism to ensure that the physical hardware is not swapped out. This would help protect against an attack where a malicious user replaces the WCC hardware with a similar appliance with backdoors built into the hardware to allow access to the system.

enerVIEW™ Web Application

ener*VIEW*™ is the web based remote monitoring and control application used by site operators and various stakeholders to interact with their remote DER. The application is accessible using a standard web browser over a secure HTTP connection (HTTPS). In order to access the application, a valid username and password must be specified which also determines the permissions the user has once they are logged in.

Overview

ener*VIEW*™ is structured as a hierarchal collection of data screens that visually depicts data being collected from the DER in real-time. Data boxes are placed on the screen and update automatically as new data becomes available in the system.

Typically, the first screen that is visible after logging in shows an overview of the entire site. This screen usually contains aggregations and balance of plant data such as the total power output from the DER at the site or the power being used by the facility.

From the site overview screen, the user can navigate to all of the other screens that they have access to. This usually includes equipment overview and detail screens that show high-level data for a single piece of equipment and detailed data, respectively.

The figure below shows several screenshots from ener*VIEW*™:

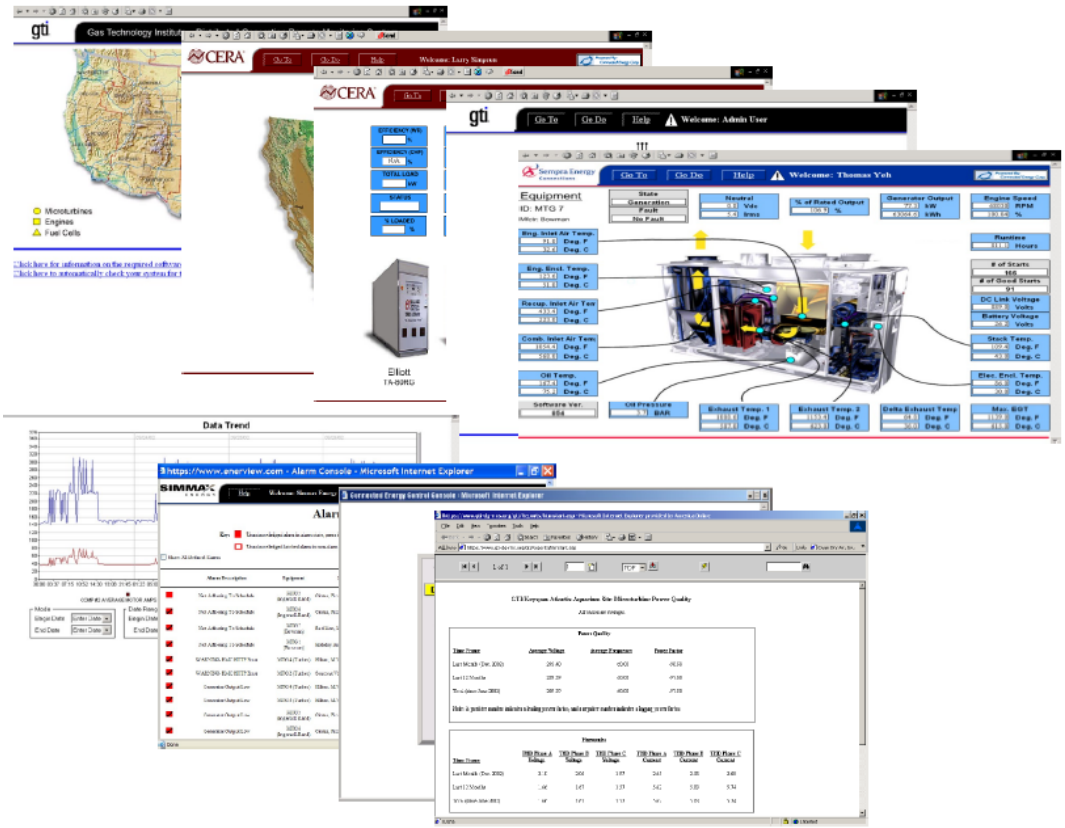

Figure 9: Sample enerVIEW™ Screenshots

ener*VIEW*™ also supports the following features:

- Reporting
- Data Trending
- Multivariable Trending
- Equipment Control
- Alarming

Phase II Enhancements

The majority of the Phase II enhancements were changes made behind the scenes to the services that feed ener*VIEW*™ with processed data. These changes commercialized the proof of concept implementation demonstrated in Phase I. The architecture was migrated to a three-tiered system utilizing a modular approach to the functionality.

The multi-tiered approach improved the security of the system by creating common interfaces to interact with core components of the system such as the database. By using common interfaces, security protections can be more easily enforced and additional options are available to secure the system.

The modular approach to the components makes the system more agile and able to adapt simply by updating, installing, or removing different components. This also aids in the testing of the system as modules can typically be tested individually allowing for more complete testing before an update is applied to a production system. In addition, the system is more scalable and reliable as certain redundant components can be running either to process more requests or more rapidly transfer to a backup module should a component fail.

Improvements were also made to the permissions model and user authorization component during Phase II. These changes increased the flexibility of the user permissions as well as improved the security of these critical system components.

Enhancements were also made to: support non time-series data, process the newer versions of ener*TALK*™, integrate weather and electricity pricing data into the system, improve the alarming subsystem, and enhance the reporting subsystem. These improvements were made as a result of limitations and problems identified in these areas during Phase I of the project.

Two-Factor Authentication

One of the big improvements that was started in Phase I but completed and enhanced in Phase II was the use of two-factor authentication to control access to ener*VIEW*™. This second level of authentication utilized a special hardware security token that needed to be inserted in the clients' computer in order to access the system. This hardware token in conjunction with a PIN number allowed ener*VIEW*™ to authenticate the user.

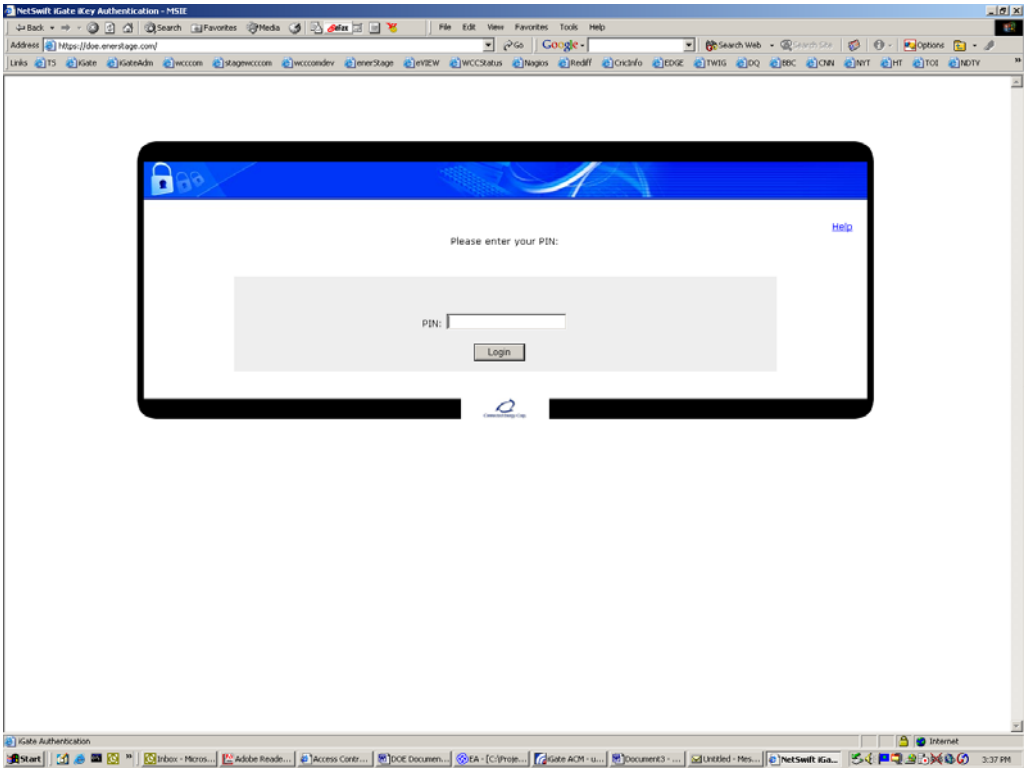

Figure 10: enerVIEW™ Login Screen Using Two-Factor Authentication

To implement this two-factor authentication system, a SafeNet iGate server was deployed in the data center that was responsible for processing the authentication requests. In order to access the system, the client would insert a SafeNet iKey USB hardware token into their computer. On the ener*VIEW*™ login screen, they would enter their corresponding PIN number which would cause a secure authentication to occur with the iGate server in the data center. If the user had a valid iKey and used a valid PIN number, they were granted access to the system based on their permissions.

Phase II Demonstration Sites

During Phase II of this project, ten sites were commissioned to demonstrate the commercialized advanced communication and control architecture. A remote terminal unit was deployed at each site with one or more WCC controllers to communicate with the DER.

Phase II Demonstration Site Details

Four of the ten demonstration sites had existing Phase I hardware and were upgraded under the scope of this project. The table below summarizes each of the sites including the type and size of the DER that was integrated:

Site	Sponsor	Total Size	Equipment	Start Date
SUNY Farmingdale (Long Island, NY)	LIPA	15 kW	3 Plug Power Fuel Cells	2003-June-05
Pebbly Beach Generating Station (Catalina Island, CA)	SCE	8.9 MW	6 Engines	2003-Oct-08
Green Park Care Center (Brooklyn, NY)	NYSERDA	150 kW	2 TECOGEN Engines	2003-Oct-14
Greater Rochester International Airport (Rochester, NY)	NYSERDA	1.5 MW	2 Wakashau Engines	2004-Jan-19
Good Samaritan Hospital (Long Island, NY)	LIPA	15 kW	3 Plug Power Fuel Cells	2004-Oct-19
Winthrop Hospital (Long Island, NY)	LIPA	35 kW	7 Plug Power Fuel Cells	2005-Jan-31
Irondequoit Pumping Station (Rochester, NY)	Monroe County		This site never came online as no DERs were identified in time.	
Lancaster Landfill (Lancaster, CA)	LACSD/SCE	250 kW	IR Microturbine	2005-June-17
Calabasas Landfill (Calabasas, CA)	LACSD/SCE	300 kW	10 Capstone Microturbines	2006-Jan-24
Palmdale Water Reclamation Plant (Palmdale, CA)	LACSD/SCE	500 kW	2 Fuel Cell Energy Fuel Cells	2006-Jan-25

Total DER Monitored Under Phase II: 11.67 MW

Figure 11: Map Depicting Locations of Phase II Demonstration Sites

Calabasas Landfill Site

Most of the Phase II demonstration sites were very similar in terms of the type of high-level functionality that was implemented. All of the sites provided remote data monitoring and had the ability to send control commands if supported by the equipment at the site. However, the Calabasas Landfill site was chosen to demonstrate the interoperability of the ACCP system with smart agent technology for DER scheduling based on a pricing signal from the utility.

The Alternative Energy Systems Consulting (AESC) Smart*DER agent technology was deployed at the site and connected to the WCC using the local site Ethernet network. The WCC and the Smart*DER agent communicated bi-directionally using ener*TALK*™. The WCC was responsible for sending real-time electricity pricing data as well as weather forecast data and the smart agent utilized the WCC to interact with the DER.

The pricing signal and weather data was integrated into the remote data center and sent to the WCC in real-time using the ener*TALK*™ protocol. The WCC utilized the ener*TALK*™ conduit routing capability to send the messages from the data center to the smart agent.

The data center received the critical peak pricing signal from Infotility via ener*TALK*™ utilizing a web service interface. This showcased the use of ener*TALK*™ as an easy way to interconnect with other energy data systems. The

weather forecast data was collected by the ACCP data center from the National Weather Service also using a web service.

Site Survey Procedure

After each demonstration site had been identified and permission had been obtained from the site owner and operator, a detailed site survey needed to take place. These surveys involve a project engineer traveling to the site and working with the customer to identify the equipment that will be interfaced with for the deployment. At this point, discussions also occur as to what data points will be monitored, what aspects of the system will be controlled, what changes if any are required to the equipment at the site, and logistical issues of the deployment are explored.

The key outcome of the site survey is a detailed understanding of how the control center can best communicate with the equipment at the site. This includes what types of physical connections will be required as well as the protocols that need to be used. As this is being worked out, other aspects of the deployment are investigated such as: where the best place for the RTU enclosure is, what types of cable runs need to be installed, and Internet connectivity options for uplink to the remote data center. This investigation also seeks to identify potential problems such as interference from other equipment installed at the site or weather or environmental considerations. Digital photographs and measurements are also taken as necessary.

After the project engineer completes the site survey, documentation is created making recommendations as to how the RTU should be installed at the site and creating a task list of other installation dependencies such as cable runs. Once this is complete, the engineer discusses the proposed solution with the customer and arrangements are made to complete each of the dependencies.

Site Commissioning Procedure

After the site survey was completed, a project engineer designed a hardware and software Remote Terminal Unit package to communicate with all of the customer equipment. Every RTU contained at least one WCC product which serves as the intelligent gateway bridging the site equipment with the data center running ener*VIEW*™. In addition to the WCC, many sites also had other I/O products such as a *CENTRY*PIA™ which is used to expand the number of inputs that can be aggregated by the WCC.

Once the hardware and software package has been designed, the project engineer completes a high-level provisioning diagram for the site. This diagram contains all of the high-level pieces of RTU hardware as well as the external DER assets and communication hardware that the RTU will be connected with at the site. All of the interconnections between each of these components are shown listing the relevant communication protocols and technologies used for each one.

After the provisioning diagram is complete, the deployment team reviews the document for approval. Once approved, work begins on configuring and creating the ener*VIEW*™ screens as well as the design and construction of the actual RTU panel. This provisioning diagram is also used at the time of deployment by the on-site technician as a guide to all of the external interconnections of the system.

Next, the project engineer produces a detailed RTU panel layout which is required for the actual assembly of the RTU. The panel layout diagram includes all of the wiring between the meters and the WCC as well as any communication equipment required for the site. This panel layout is documented and once approved, sent to the panel assembly shop for construction and preliminary testing. After the panel has been constructed and tested, it is shipped to the site for installation. This panel layout document is analogous to the blue prints for a building whereas the site provisioning diagram is more similar to a high-level site plan for a building.

As the project engineer works on the panel layout, other members of the deployment team work on: designing, developing, and creating the ener*VIEW*™ remote monitoring screens, control faceplates, alarms, and reports. These engineers also configure the initial user accounts and corresponding security permissions. As this work is going on, the customer does not have access to login to the application or view the screens due to the fact that the site needs to be enabled before they have access to login. Once this work is completed, each configured ener*VIEW*™ component is tested so that it will be ready when the RTU is installed at the site.

Once the RTU is assembled and tested, a technician travels to the site installing the RTU enclosure and making all of the external interconnections. While they are on-site, communication with each piece of equipment is verified as well as connectivity back to the data center. This typically involves an interaction with a technical site contact that is familiar with the equipment being integrated.

Once all of the on-site installation and testing is complete, the site is enabled which causes data to become available to the customer. At this point, the site enters the hosting phase since no further configuration or installation work is required after this point.

Phase II Demonstration Site Testing

After the site installations were completed, a technician at the operations center remotely looked at the values being read from the DER equipment and verified that the data values were appropriate for what was being monitored. An end-to-end test was then performed to ensure that this data was properly being recorded in the data center and available for viewing on the remote monitoring screens.

The control aspects of the demonstration sites were tested by triggering each of the control actions through the faceplates on the ener*VIEW*™ web portal. These tests also included verification of the safety measures such as ensuring that only a single user could control the equipment at any one time.

In addition, after some data had been collected at each demonstration site, the reports were examined to ensure that all calculations were being performed correctly and that the reports were being run at the right times.

Once the internal tests were completed and each site was fully commissioned, project engineers worked with the site owners or operators to verify that the remote monitoring and control pages were working correctly. As an outcome of these tests, slight modifications were made to some of the remote monitoring screens to enhance the clarity of the data being displayed.

10. Issues Encountered

Lack of bump in the wire security solutions

While looking for a solution to enhance the security of the communication between the WCC and the data center and while also removing the hardware VPN appliance, possibilities for software based data security solutions were evaluated.

While many products exist that serve this purpose, they all substantially impact the way that the network connection is utilized and many effect the protocol used to exchange data. None of the solutions (with transparent data protection) had the right mix of other features such as a high level of security and the utilization of standard TCP network packets for the underlying transport.

As a result, the best option for the purposes of protecting the uplink in the ACCP platform was to design and implement our own custom solution with the exact feature set we were looking for.

Many diverse protocols at the premise level

There are many different types of DERs in active service using many different communication protocols to interface with external control systems. This diverse set of protocols has grown around specific feature requirements and advantages that some protocols offer over others as well as the evolution of control systems.

As a result, in order to integrate all of these different devices into a common DER network, an extensive set of protocol adapters needs to be developed. While dedicated hardware converters exist for this purpose, this can quickly become expensive to deploy, manage, and configure. As an alternative, we designed the WCC premise controller to be able to use protocol software plug-ins to allow this single piece of hardware to interface with a wide array of field equipment.

Lack of extensible but simple to implement standard communication protocol to use between the premise and data center

Although many standardized protocols exist for exchanging data in industrial and commercial control systems, no protocols existed that provided the level of business intelligence related to energy resource integration and aggregation. In order to meet high levels of interoperability these rich protocols are required. As a result, we designed and implemented ener*TALK*™ to serve in this role.

11. Commercial Viability Assessment

Strengths

Flexibility

Recently, there has been a growth in the markets for energy efficiency and performance management as a result of higher energy costs and increased concern over the environment. The growth in this market has led to numerous products being targeted for residential, commercial, and industrial customers seeking to manage their energy use more efficaciously. They also help users better understand how they utilize energy. Many of these products seek to meter energy consumption assets such as HVAC systems or lighting systems.

Due to the nature of these products, many provide a simple user interface to the end user allowing them to view data on their energy use or in some cases, control and interact with these loads. Because of this, a single user may have multiple applications each containing a small slice of their energy assets. This creates an opportunity for products that seek to integrate all of this data into a single, unified management console.

As a result, the flexibility and standardization of the ACCP system is a key strength as it allows the application to be agile by adapting to integrate and aggregate data from the ever growing types of assets that can be monitored. By providing a single interface that the user can use to access all of their energy assets, it provides a strong business case for replacing many of the extremely specialized products currently in the market.

Security

In addition, the ACCP system has been designed and built with strong security practices and policies in place from the beginning. A key aspect is the clearly articulated and standardized security protection profile that allows stakeholders to understand what is meant by the platform being secure. This is a critical deliverable of the project as it reduces ambiguity around security and defines a set of criteria that the system can be tested against. Further, it allows market stakeholders to quickly assess how the security of the system relates to their requirements and what exposures, if any, are opened through using this platform.

During the design and implementation of the ACCP system utilizing this security protection profile, it was determined that it would be best to provide as much flexibility as possible to allow the system to easily adapt to changing security requirements. This also is a huge strength of the system as it becomes a simple task to utilize different technologies as older ones lose their strength due to other technological advancements. As an example, ener*TIE*™ can easily be configured to use larger keys or a different encryption algorithm if one of the ones currently being used is found to be insecure.

DER Network Communication

The specification of an open and standardized DER communication protocol is also a big strength of the system. As implementers are performing analyses investigating the deployment of an ACCP system, the future expansion and support of the system is a key consideration due to the amount of the initial investment. By utilizing an open and documented communication standard, these implementers can be more comfortable knowing that other systems can be integrated with the platform in the future.

Depending on the needs of the DER owner, this standardized protocol also allows for independent use of the premise solution or the data center solution separately from one another. While doing this, the full functionality of both sides of the system can be realized. Since most other systems closely couple these two components, this capability is not typically an option with other DER integration packages.

Data Center Communication

The design of the ACCP ener*TIE*™ technology and the ener*TALK*™ protocol allow the system to be utilized with any Internet connection to securely exchange data between the RTU at the site and the remote data center. This allows significant flexibility to utilize whatever communication technology is available at the site. In addition, Internet connection links tend to be significantly less expensive than any kind of leased, dedicated network link thereby minimizing ongoing costs to keep the site operational.

The Phase II demonstration sites utilized the following types of Internet connections for data center connectivity:

- Existing Local Area Network Connection (Corporate Network)
- Cellular Modem
- Analog Dial-Up Modem
- Broadband Digital Subscriber Line (DSL) Service

In addition, the local data buffering on the WCC allows for the use of intermittent and/or unreliable Internet connections. Data compression can also be enabled to reduce the amount of data being exchanged over the connection.

Network connections can also be scheduled allowing the WCC to connect with the remote data center only at certain times of the day. While this option is not recommended (as it does not allow the remote application to update data in real-time nor control the equipment in real-time) it provides an affordable option if the only available Internet connection requires the use of a communication channel with per minute charges.

Documentation

Unlike some of the other solutions available to integrate DER, the ACCP platform provides documentation around the technologies and protocols it utilizes. This documentation helps promote the adoption of this particular platform as it provides visibility into how the system operates.

Weaknesses/Limitations

Configuration

Due to the diverse nature of distributed generation assets and their associated control systems, site-level configuration, testing, and deployment can be an arduous and time consuming task to complete.

Utilizing a high-level, standardized, open protocol such as ener*TALK*™ alleviates this to some degree by allowing DER manufacturers to directly implement a protocol that can be easily integrated with the system. However, it is inevitable that the system will frequently need to integrate DER using non-standard protocols and in these situations, customization and elaborate configurations are typically needed to convert these protocols to ener*TALK*™.

In the current implementation of the ACCP system, there is only a limited set of tools to aid in this configuration and deployment process. This results in the entire process being time consuming, error prone, and fairly manual. Because of this, it typically needs to be performed by an engineer with a detailed knowledge of the system as well.

Level of Customization Required for Simple Deployments

Although somewhat related to the configuration, one of the big issues of the current implementation is the amount of customization that is needed for all deployments regardless of their complexity. As an example, while all of the remote terminal units utilized at the demonstration sites were similar, no two were identical and all had to be custom designed for the specific site being deployed.

Beyond the RTU customization, the web presentation of the data and control aspects also varied from site to site causing no two to be the same. While this is a harder portion of the system to fully standardize, having some basic templates for different types of DER will streamline the process substantially.

This level of customization is desirable for sites with a substantial amount of DER such as the Pebbly Beach Generating Station at Catalina Island. However, some of the smaller sites would be better off with a standard RTU and standard data

presentation screens. As an example, a site such as Good Samaritan Hospital with only 15 kW of generation would probably suffice having a basic screen showing parameters that are very typical of a fuel cell. If the particular site required additional data specific to the model of fuel cell, that could be a level of customization added on top of a standard offering.

Most of this customization can be attributed to the fact that existing control and energy management systems are typically custom built and that different DERs have different physical interfaces for connectivity. As a result, it is not feasible to create a single RTU that would be applicable for all sites but it would be possible to prepare a set of ten RTUs that would allow for the interconnection of a large percentage of sites. In conjunction with standard web presentation screens for different types of DER such as a Plug Power Fuel Cell, Capstone MicroTurbine, etc., the entire logistical process of deploying an ACCP site will be more seamless and far less expensive.

In addition to the potential cost savings associated with some level of basic standardization, vendors would be able to stock some of the hardware components and common products reducing the lead time required for the deployment of additional DER.

It is important to note, however, that this should not replace the flexibility and advanced customization currently made available by the system. This should instead supplement the current system allowing the customization to be used when applicable.

Barriers and Economics Surrounding Commercial Adoption

Conflict of Interest with System Integrators

Many of the dominant players providing integration solutions for distributed energy resources have their own proprietary protocols and end-to-end systems that are utilized in their solutions. These protocols and systems tend to be extremely closed and do not typically integrate easily or completely with third-party solutions. The reason for this is that it is in the best interest of these integrators to sell their complete package instead of using a third-party system for part or all of the solution.

As a result, these firms will be less likely to adopt a standardized communication technology (such as ener*TALK*™) or utilize an open platform such as the one constructed during this phase of the project. However, it is in the best interest for the end-users to utilize standardized open protocols in their DER networks as it makes the entire solution less coupled to a single vendor.

Platform Adoption Costs - Initial

Although some reference designs and documentation were prepared for various aspects of the system, initial platform adoption cost is a major investment to implement a complete end-to-end ACCP system even with such items in place.

There are typically two levels of platform adoption depending on the product line and goals of the system implementer:

1. Data Center Application Adoption
2. ener*TALK*™ Adoption for Standardized DER Integration

Most original equipment manufacturers (OEMs) will only seek to add ener*TALK*™ support to their DER products. In these cases, providing the data center application environment is the responsibility of the customer, or a preferred partner of the manufacturer.

On the other hand, a large entity deploying a vast DER network would likely only need to build out the data center application and, (with presumed adoption of ener*TALK*™ by the OEMs) would be able to expect that ener*TALK*™ is already integrated into the equipment that they purchase.

As an alternative to an entity building out their own data center, the ACCP system can easily be a hosted solution as was done in this phase of the project for the demonstration sites. In this case, an external firm provides the data center and the company deploying the DER network pays for use of this environment.

Data Center Application Adoption

The provisioning of a data center supporting an ACCP system typically is very expensive initially. As a result, a substantial number of monitored DERs need to be deployed in order to obtain a positive return on the investment.

enerTALK™ Adoption

The cost to adopt ener*TALK*™ natively on a DER tends to be high as well. This is a result of the design, implementation, and testing work that is required by the manufacturer. Although ener*TALK*™ was designed to be a lightweight protocol, in some cases the hardware configuration needs to be changed to accommodate the creation of XML documents.

Platform Adoption Costs - Support, Maintenance, and Operation

Once an ACCP architecture is built out, the majority of the operational costs are associated with the data center infrastructure. There are also support and maintenance costs associated with the RTUs that tend to scale based on the amount of DER being integrated.

Based on our experience deploying the Phase II data center environment and supporting the demonstration sites, we found that these costs are comparable to hosting a typical server side data driven application with remote clients. However, these costs tend to be tied very closely to: the exact way in which the data center is built, the types of RTUs and DERs that are integrated, and any service level or maintenance agreements established. Because of this, each implementer will need to assess these costs and accept the risk for underestimating their scope.

Concerns Surrounding Suitability of Solution for the Specific Need

As discussed previously, the ACCP system is designed to be flexible and generic to allow the integration and aggregation of any DER. Because of this, the system can be configured and implemented to support virtually any system that needs to remotely interact with energy assets. Since many implementers will have specific requirements they are trying to support, they need to be able to assess how well the platform will meet their needs.

In some cases, implementers will be able to perform this analysis based on the available documentation and reference designs. However, in certain cases, this will not be possible or will not allow the implementer to fully understand the scope of work. The large size of the system and its complexity makes it expensive and typically unreasonable to construct an evaluation system for this purpose.

Lack of Current Market Adoption

Currently, the market is flooded with a variety of different communication protocols, DERs, energy management systems, and other related technologies. In many cases, customers have existing systems deployed and have found a way to make their current system meet their needs. There is also a wide range of different sized customers. The larger users of DER typically have these existing systems that have been customized and built to their specification by a system integrator. On the other end of the spectrum, the smaller users typically do not have enough DERs to make an entire management system feasible.

Because of this fragmentation, there is no current large customer taking the initiative of adopting this standardized communication technology. From a system integrator perspective, standardization does not add substantial value to their system since they provide complete solutions. Meanwhile, from a customer's view, the costs tend to outweigh the benefits.

However, if this architecture can gain traction among DER manufacturers, the economics of deployments for smaller user's changes and it now becomes a reality for them. In addition, large users can benefit from being able to more easily: maintain their existing system, install new DERs, add DERs already installed at their site but not currently monitored, and pick up features allowing for the streamlined operation of their DERs. Utilities will also see more value in utilizing the technology as there will be other first movers in the market.

Essentially, the risk of adopting this technology is substantially reduced as other entities demonstrate its value and functionality.

Efficiency and Reliability

As the Phase II platform was developed, each component was extensively tested individually to ensure that it operated correctly in both normal situations and when common errors occurred. These components were also tested to gauge the approximate level of overall performance to ensure that the final application would meet performance requirements. This initial testing was performed in a lab environment prior to deployment at the demonstration sites.

Once each individual component was tested and passed the basic tests, it was deployed for testing at the Phase II demonstration sites. At this point, additional reliability and efficiency testing was performed as follows:

1. Stress/Load Testing of Components - Lab Environment
2. Real-World Testing - Demonstration Sites

During the stress/load testing phase, each aspect of the system was tested by repeating common scenarios many times in an automated testing environment. During these tests, data was collected on the performance and behavior of the system. Although many different scenarios were tested in this fashion, the following list highlights the key tests:

- Remote Terminal Unit/WCC
  - Equipment Communication Problems
  - Corrupt Data Being Received from the Equipment
  - Internet Connectivity Issues
  - Secure Tunnel (VPN) Connectivity Issues
  - Normal Operation
  - High Data Loads, No Errors
  - Database Performance Statistics
- Data Center
  - Invalid ener*TALK*™ Messages from the WCC
  - Invalid Data Values in Messages
  - System Load Based Upon Number of Concurrent ener*VIEW*™ Users
  - System Load Based Upon Number of Concurrent Connected WCCs
  - Data Point Throughput

The real-world testing at the demonstration sites continued from the time the software was deployed at the site to the completion of Phase II of this project. During this time, we worked with the relevant stakeholders and operators for each site to assess how the system met their specific needs. In addition, we examined logs and collected performance data on the data center environment to assess how well the system was operating.

Results - Efficiency

Through our performance testing, we found that the WCC takes an average of 5-seconds to process a data point and begin to send the message to the data center. The communication between the WCC and the data center is highly dependent on the Internet connection but typically is less than one second for high-speed links. Once the data arrives at the data center, it takes roughly 30-seconds to process and archive. As a result, the total system latency is consistently well under 1-minute and typically around 45-seconds.

The control latency is much faster as the messages are prioritized by the system. Our testing showed that typically, the messages were sent to the WCC and processed in under 10-seconds.

Results - Reliability

During reliability testing, there were no outages identified in either the core data center applications or any of the supporting services. However, over a several month test period, a few brief outages occurred in some of the modules, typically the data reporting service. Each incident was analyzed, the root causes for these outages were identified, and changes were made to the system to improve reliability. As a result, overall uptime of the entire system is extremely high.

The system also performed very well in the scenario stress testing by consistently responding to situations in accordance with design parameters.

Interoperability

The selection of Phase II demonstration sites was based partially on the types of DERs available for monitoring and control. The ACCP system refined during this phase of the project was deployed at ten test sites, and interconnected with the following types of DER:

- Fuel Cells
- Microturbines
- Large internal combustion engines
- Combined heat and power (CHP) systems

At each of the test sites, the WCC appliance was able to monitor data and as applicable, dispatch control messages to the equipment. For each of these devices, the data was able to be normalized and aggregated and marked up using the ener*TALK*™ protocol in its intended fashion.

At the LACSD Calabasas Landfill site, we also integrated with an Alternative Energy Systems Consulting, Inc. (AESC) Smart*DER intelligent agent. Communication with this agent utilized the ener*TALK*™ protocol and also

required the WCC to consume weather forecast data from the data center. The ability to represent non time-series data in ener*TALK*™ allowed us to cleanly integrate this appliance with the DER network.

Results

Based on our testing at the Phase II demonstration sites, the current design and implementation of the ACCP architecture is suitable for use to interconnect distributed energy resources with the power grid. The reliability, performance, interoperability, and security aspects of the architecture all met the objectives set forth in the design phase to satisfy the project goal of seamless grid interconnection.

First, the reliability testing found that the core components of the overall system were available at almost all times. In addition, the stress test scenarios demonstrated that the system consistently behaved as expected.

The performance testing shows that the Phase II demonstration system performed marginally better than the proof of concept design built in Phase I. This translates to real-time data acquisition latency of roughly 45-seconds between the data collection time and processing by the data center (dependent on the Internet connection). The data center systems were able to easily handle the entire load created by the demonstration sites and the performance testing showed acceptable performance as we simulated additional DERs in a testing environment.

While it is expected that the performance characteristics of the system are acceptable for a commercial deployment of the system, enhancements are currently underway to substantially reduce the data acquisition latency and increase the number of simultaneous data streams that can be processed from DERs. These improvements will allow the platform to be suitable for additional applications such as managing spinning reserves.

During the security testing, we did not find any vulnerabilities or execute any attacks on the system. Also, we were able to verify that it satisfied the parameters outlined in the Security Protection Profile. It therefore meets the requirements for use as a platform to interconnect DERs. The flexibility of the security technologies allow this requirement to be maintained over time as security needs evolve.

The system also provided enough flexibility to easily integrate with all of the different DERs at the demonstration sites and cleanly present a high-level representation of the data. While some improvements in this area will aid in the deployment aspects of the system, the current version provides the interoperability required to support various types of DERs.

Deploying the data center and modifying DERs to natively support ener*TALK*™ have high initial costs but are very comparable to implementing and deploying other similar solutions. The variable costs to maintain and operate these items are also on par with similar solutions. Economically, this aspect of the system is

viable so long as the data center infrastructure is capable of supporting a large number of DERs. In order to achieve this, owners that operate small numbers of DERs will likely need to utilize an infrastructure provided by an external service provider.

It is recommended that a market analysis be performed in the future to assess the demand for a lightweight version of the data center application that could support a smaller number of DERs. However, this analysis is outside of the scope of this project and this type of lightweight data center application is not technically viable or relevant for a solution to integrate DER with the power grid.

The costs of the RTU may be prohibitively high for smaller DERs. The Phase II RTUs cost $5000 regardless of the size of the equipment being integrated. At a site such as Catalina Island, this resulted in a unit cost of $1.78 per kW. The Good Samaritan Hospital site, however, had a unit cost of over $300 per kW due to its smaller size.

This can be addressed by natively supporting a protocol such as ener*TALK*™ within the DER. As an example, the unit cost at the Good Samaritan Hospital would have been substantially lower if the fuel cells natively utilized ener*TALK*™. However, for larger generation assets such as the engines on Catalina Island or the Microturbines at the Calabasas Landfill, the RTU costs are clearly viable.

As a result, for grid interoperability, the overall cost of building and supporting an ACCP platform makes the system economically viable. However, other applications of the architecture may require changes to reduce the costs. As ener*TALK*™ and other standardized technologies see wider commercial adoption, these costs will naturally begin to decline.

12. Competitive Products and Architectures

The table below provides a high-level overview of similar competitive products and compares these with the ACCP platform developed during this phase of the project. Both the Siemens and Comverge products are targeting slightly different markets and thus were not designed with several of the ACCP requirements. As a result, they each have some weaknesses that exist only if they are to be used for DER integration although both are viable contenders in this space.

	ACCP Platform	Siemens Spectrum Power	Comverge Virtual SCADA
Standardized Protocols	Yes; enerTALK™	Yes; ICCP	No
Secure Communication Uplink	Integrated	Only between control centers. Non-integrated within control center	Yes
Real-Time Data Monitoring	Yes, 45 sec	Yes	Yes
Real-Time Control	Yes, 10 sec	Yes	Yes
Application Type	Web Application	Web Application	Web Application
Two-Factor User Authentication	Yes		
Integrates All DER	Yes	Yes	Yes
Remote DER Connectivity Options	Internet; Any Type	Ethernet LAN/WAN	IP Based; Ethernet, Cellular, Dial-Up

Siemens Spectrum Power

The Spectrum Power product by Siemens Energy is fully commercialized and provides a remote SCADA solution. This type of solution seeks to serve a different role than the ACCP system although provides similar functionality for integrated DERs.

Strengths for DER Integration

The Spectrum Power system utilizes standard communication protocols between the RTU and data center as well as for inter-data center communication. The system provides analysis and reporting tools as well as other advanced capabilities designed for a utility such as: generation frequency control, load forecasting, and economic dispatching. The application is well supported and provides a set of tools and interfaces for configuring the deployments.

Weaknesses for DER Integration

The communication between the RTU and data center occurs over a local area network (LAN) and thus would require special considerations for distributed energy assets. Local area networks tend to be secure entities so utilizing a remote network link in place of the LAN would also require a hardware based security solution such as a VPN appliance.

Although standardized protocols are used throughout the Spectrum Power system, ICCP is designed for the exchange of SCADA data and is thus a lower-level protocol than ener*TALK*™. As a result, other systems could likely be integrated with this platform although the interoperability would be less flexible.

Comverge Virtual SCADA

Like the Siemens Spectrum Power solution, the Comverge Virtual SCADA system is another remote SCADA solution. For DER integration, this would utilize the Comverge Maingate Embedded Site Server (ESS) as the premise controller coupled with a remote data center application.

Strengths for DER Integration

The Maingate ESS is a controller well suited for connectivity with DERs. It has several built-in options for establishing a connection to the remote data center such as: Ethernet, cellular modem (GSM/GPRS and CDMA), and analog dial-up

modem. This flexibility reduces the hardware needed at certain sites and may reduce costs as well.

The Maingate ESS controller can integrate with the DERs using a variety of protocols and provides protections such as guaranteed data delivery that are also included as part of the ACCP platform.

The data center application provides a web portal exposing the user to the same type of functionality as is available with ener*VIEW*™. In addition, like the ACCP platform, a variety of different data center modules can be utilized allowing flexible data center integration with other systems.

Weaknesses for DER Integration

The communication protocol between the RTU and the data center is secured but does not utilize a standardized high-level protocol such as ener*TALK*™. This reduces the interoperability with other types of DER that may not be able to be easily integrated with the Maingate ESS controller. In addition, it ties the premise solution with the data center solution.

13. Market Potential

While integrating any energy resource into the power grid, it is critical to have real-time visibility into the resource and the ability to control and modify its interaction with the grid. For distributed energy resources, this becomes more complicated as the grid operators do not typically have the ability to view data and manage how these resources interact with the grid. As a result, giving the market operators the ability to see data from these resources as well as influence their interactions with the power grid is critical if distributed generation (DG) is to operate in a grid-connected fashion.

Although some DG is not connected to the power grid, in many cases it makes sense for the operator to do so because of the imbalance between the fluctuating power demand of the site and the power output of the generation. In some cases, the operator is utilizing the DG for heat and taking the electricity as a by-product such that they may have even less control of the power output. These situations make it even more logical to connect the DG to the power grid. As a result, there likely is a correlation between the demand for DG and the need for a communication platform to integrate these resources with the grid.

According to projections in a report from the Energy Information Administration (EIA) by Robert T. Eynon[1], distributed generation use by utility operators in the United States is expected to grow to 19.1 GW in 2020 from 0.9 in 2005. Outside of utilities, natural gas fired DG in 2020 is expected to be over 5 times higher than levels from 2000.

In addition, the EIA projects that renewable energy production will increase in the United States from 8.4% of the electricity generation in 2007 to 12.5% in 2030[2].

Distributed generation owned and operated by utilities is intended entirely for operation in a grid-connected mode. Most renewable energy resources are also operated in a grid connected mode. Therefore, it is expected that there will be strong market demand for the DG integration platforms such as ACCP in the coming years.

Beyond these projections by the EIA, as more distributed generation is successfully integrated with the grid and solutions such as the ACCP system begin to develop additional credibility in the industry, it is likely that the demand will increase further for DG resources and thus these technologies as well. This will be compounded as DG technology drops in cost and improvements in electrical efficiency are obtained. This will further make the economic case for combined heat and power systems which again will likely lead to an increase in DG available to be interconnected with the grid.

[1] Energy Information Administration, "The Role of Distributed Generation in U.S. Energy Markets". Eynon, Robert. Accessed 12-February-2009. http://www.eia.doe.gov/oiaf/speeches/dist_generation.html
[2] Energy Information Administration, "Annual Energy Outlook 2008". June-2008. Page 131.

14. Commercialization Roadmap

Commercialization Strategy

The ultimate goal of the commercialization process will be to put numerous resources in place to address the barriers for adoption. Specifically, it will be important to clearly articulate how the ACCP system and technologies can provide solutions to common problems in the industry. In addition, the commercialization process should focus on getting a commitment from several OEMs to support ener*TALK*™ in their products. These resources will not only help market stakeholders see how ACCP will be useful for them but will also begin to build confidence that these are technologies that are being actively supported and will continue to be in the future.

The entire commercialization process is expected to take roughly 1-year to complete. However, interim progress will be made that will cause the technologies to begin to gain traction in the markets during the second half of the roadmap.

Activities Required for Commercialization

Development of Deployment Tools

Time Horizon: Months 0-3

In order to ease the adoption of the ACCP platform, additional tools need to be developed to streamline the deployment of the system. These tools would be split into two categories:

1. RTU Configuration Tools
2. ener*VIEW*™ Presentation Configuration Tools

The RTU tools are used by a technician to configure the WCC to communicate with the DERs. It allows for the specification of: any communication parameters with the equipment, the data points being collected, and configuration of the control capabilities of the system. These tools will allow for a reduction in deployment costs thereby enabling the ACCP technology to be commercially viable for smaller sizes of DER.

The ener*VIEW*™ presentation tools are used to configure the web application for a particular customer. During this activity, standard templates would be created for common types of DER that would simplify this aspect of the deployment. Once the templates and tools have been created, the process would be to select a relevant template and customize it based around the specific site needs. Like the RTU tools, this will help reduce the deployment costs of the system.

Preparation of Case Studies

Time Horizon: Months 2-3

A set of case studies need to be prepared highlighting how the ACCP platform can be utilized as a solution to common problems in the industry. These case studies should focus on initiatives backed by public energy groups such as NYSERDA or the California Energy Commission.

The output of this activity is a set of documents that could be made available on a public web page designed to promote the adoption of this platform and related technologies.

Preparation of Business Cases and Financial Benefits

Time Horizon: Months 3-6

To aid in the decision making and planning process by potential adopters of the ACCP system, it will be important to provide resources that allows business cases and financial benefits to be seen and estimated, respectively, for common uses of the technologies.

The output of the business cases would be several documents tailored to specific applications of the technology. For each of these applications, spreadsheets would also be provided to allow the: net present value, cash flows, and/or estimated time until return to be calculated given the input of various parameters by the user. These deliverables would be made available on the same web page used for the case studies. As applicable, these business cases and financial benefits should be referenced to corresponding case studies.

Development of Process for Security Certification of ACCP Component Implementations

Time Horizon: Months 3-12

As organizations consider utilizing the ACCP system and technologies for their applications, it will be important for them to easily identify which products actually adhere to the Security Protection Profile. Rather than relying on the vendors themselves to indicate that their product is compliant, having a process as well as an organization certify a product will result in greater uniformity and adherence to the policy. This will help in alleviating security concerns by market stakeholders as well.

Partnerships/Adoption of enerTALK by OEM Manufacturers

Time Horizon: Months 3-9

As the business cases and case studies are being prepared, it will be important to begin engaging with DER manufacturers to seek their adoption of ener*TALK*™ as a natively supported protocol. The target output would be the commitment from two to three OEMs that they will adopt ener*TALK*™ in their equipment.

This activity addresses the core need of beginning to build market adoption of the technology. As the ACCP system and communication protocols begin to develop a presence in the markets, it is expected that it will be easier to grow the use of the technology.

Initial Regional and National Market Focus

Initially, the ACCP platform and technologies will be promoted in southern California and the New York City area. The intent is to utilize existing relationships with customers who (as a result of participation in this project) have seen the value of these technologies to serve as marquee showcases of the business cases surrounding the use of ACCP work. In addition, these areas have favorable market incentives for grid participation of DER and are active in promoting innovations and inventions in the industry.

15. Publications, Presentations, and Outreaches

Gridwise Initiative

Date: July 2003

Thomas Yeh participated as a consultant advising the grid interoperability framework for the future vision of the electric power system in the United States. The outcome of this work was the "Grid 2030" report outlining the key issues facing the electric power system in the United States and providing an initial plan to prepare the system for the future.

DER Aggregation: A reference design

Date: September 30th, 2004

Arup Barat participated as a panelist at a Peak Load Management Alliance conference in Orlando, Florida.

California Energy Commission Demand Response R&D Symposium

Date: November 30th, 2004

Thomas Yeh presented "Communication Architecture for Dispatching Demand Response" at the symposium in Sacramento, California.

Paper: A Comparison of IEC-61850 and enerTALK™

Title:
A comparison of IEC-61850 and enerTALK™ as advanced communication protocols for Distributed Energy Resources.

Date: September 30th, 2005
Author: Arup Barat

This document aims to describe, classify and contrast the approaches taken by IEC-61850 and enerTALK™ in enabling interoperability among Distributed Energy Resources (DER) via commonly available communication infrastructures. It analyzes the design approaches as well as feature sets of each protocol to evaluate their suitability for DER communication. Finally it provides possible integration scenarios for the two protocols to create best of breed and reusable solutions.

Report: System Protection Profile

Title:
System Protection Profile: Distributed Energy Resource Advanced Communication and Control Systems

Date: October 11th, 2005
Prepared By: Mary Young, Sandia National Laboratories

This document was prepared by Sandia National Laboratories as a deliverable for this project and specifies the minimum security requirements for DER communication and control systems. Its scope is limited to systems that utilize the Internet to communicate between DER sites, system stake holders, and central control rooms.

Distributed Energy Peer Review Poster Presentation

Date: December 13-15, 2005

Arup Barat made a poster presentation at the DOE sponsored peer review meeting in Arlington, VA.

6th Annual Microturbine Applications Workshop

Date: January 17-19, 2006

Arup Barat made a poster presentation "Seamless aggregation of microturbines: a framework approach" at the workshop in San Francisco, CA.

Grid-Interop Conference Presentation

Date: November 7-9, 2007

Arup Barat presented "Interoperability in the ACCP Reference Implementation" in the Information Modeling track. This presentation explores the issues and challenges in grid interoperability and discusses the solutions provided by the ACCP Phase II architecture.

IEEE 1547.3 Working Group

Date: November 2007

Arup Barat and Thomas Yeh served on the working group helping to define the standards for interoperability of distributed energy resources. In 2007, the official IEEE standard was released.

Transmission & Distribution World: Battery Storage Paper

Date: December 1, 2008

Stephanie Hamilton of Southern California Edison (SCE) published a paper entitled "Batteries are Key to Wind Integration" in T&D World. This paper discussed the use of battery storage to address the intermittent and non-dispatchable nature of wind generation when integrating it with the power grid. The analytic work for this paper was performed under this ACCP project.

16. Resulting Collaborations

Alternative Energy Systems Consulting, Inc. (AESC)
Smart Agents: Integration for Renewable Generation

This project is currently in progress and is using AESC Smart Agent technology in conjunction with the BPL Global intelligent data acquisition and control platform. The goal of the project is to demonstrate the use of this technology to synchronize the energy production and transmission from wind generation resources with the rest of the electric grid.

Consortium for Electric Reliability Technology Solutions (CERTS)
Demand Response Spinning Reserve Demonstration

This project was a demonstration of the use of existing utility load (residential and commercial air-conditioners) as a resource to the spinning reserve markets. The demonstration sought to determine the key issues surrounding the use of such load for demand response purposes.

Alternative Energy Systems Consulting, Inc. (AESC)
Smart Agents: Calabasas Landfill

This served as an extension to the initial scope of work at the Calabasas Landfill Phase II demonstration site. We integrated Southern California Edison's Critical Peak Pricing (CPP) Signal received from Infotility into the ACCP platform to allow intelligent DER scheduling of the equipment at the site. The AESC Smart Agent technology was used to act on the pricing signal and schedule the generation.

17. Budget Data

A complete Cash Transaction Report (Long Form) will be provided separately.

	Planned	Actual
Phase 2 DOE Funding	$597,198	$501,870
Phase 2 Total Budget	$2,865,233	$2,195,283

The primary reason for the actual project cost falling below the budgeted cost was a result of the cost sharing portion of the project costing less than initially projected. This was largely related to a modification of security hardware purchased for the project and the subcontractor costs associated with bringing some of the demonstration sites online.

18. Inventions and Patents

No patent applications have been filed for work performed under this project.

19. Appendices

Appendix 1: Sample enerTALK™ Documents

Example 1: enerTALK™ 2.7 Time-Series Data

```
<?xml version=”1.0”>
<enerTalk version=”2.7”>
  <momAction type=”postData” orgID=”CEC” siteID=”TST01”>
         <data equipID=”DEV01”>
                <ET-500 timestamp=”2005-11-21T22:56:32Z”>224</ET-500>
                <IT-650 timestamp=”2005-11-21T22:56:32Z”>334</IT-650>
         </data>
  </momAction>
  </enerTalk>
```

Example 2: enerTALK™ 2.7 Non-Time-Series Data

```
<?xml version=”1.0”>
<enerTalk version=”2.7”>
  <momAction type=”postData” orgID=”CEC” siteID=”TST01”>
         <data equipID=”DEV01” type=”non time series data” template=”weatherData”>
                <WeatherForecast>
                       <time>2005-11-21 20:19:05</time>
                       <max_temp>55</max_temp>
                       <dew_point>51</dew_point>
                       <liquid_precip_amnt>0.02</liquid_precip_amnt>
                </WeatherForecast>
         </data>
  </momAction>
</enerTalk>
```