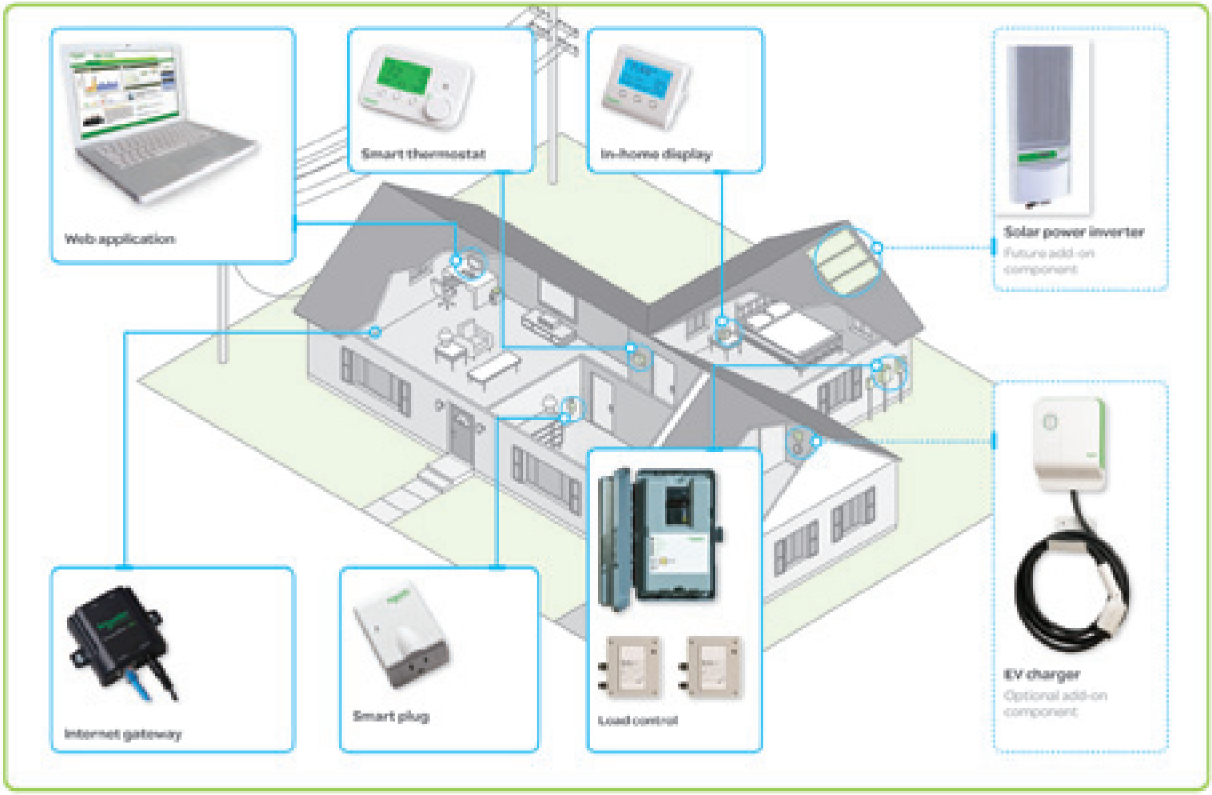
PP40010082
www.electricenergyonline.com

Electric Energy T&D MAGAZINE

NOVEMBER-DECEMBER 2011 Issue 8 • Volume 15

Avista's Pullman Smart Grid Demonstration Project

The Wiser way is a smarter way



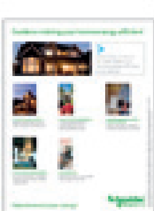
The Schneider Electric Wiser energy management system (EMS) enables innovative energy conservation that helps your home use less power while significantly lowering your utility bill.

Wiser™ EMS is the **complete home energy solution** that monitors, communicates, and manages residential energy use through wireless interconnectivity and real-time communication between homeowners and their local utility.

Simple to understand and manage, Wiser lets homeowners control how much electricity they use, and when they use it. And they **conserve energy and save money without sacrificing comfort and convenience.**

Through the Wiser system's in-home energy displays, **users receive important rate-reducing information throughout the day** that allows them to better control and optimize their home energy use by automatically turning appliances, devices, or heating/cooling systems down, or off.

The Wiser EMS also lets users **easily monitor and manage their electric vehicle charging** when integrated with Schneider Electric™ EVlink™ indoor/outdoor charging stations. Available in wall or pedestal mount models, the 240 volt EVlink provides a **50 percent faster charge** than typical 120 volt charging stations.



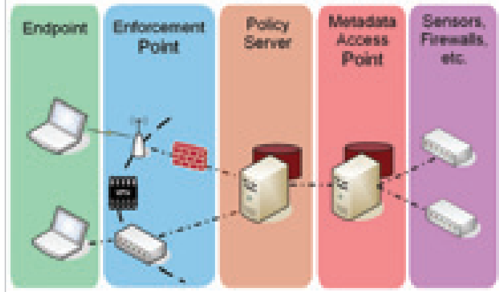
Download our FREE "How to make your home energy efficient and reliable" brochure

Visit www.SEreply.com and enter key code h729v

Schneider Electric

Circle **13** on Reader Service Card

Electric Energy T&D MAGAZINE



page 33

Publisher:
Steven Desrochers: steven@electricenergyonline.com

Editor in Chief:
Mike Marullo: mam@electricenergyonline.com

Contributing Editors:
William T. (Tim) Shaw, PhD, CISSP
tim@electricenergyonline.com

Account Executives:
Eva Nemeth: eva@electricenergyonline.com
John Baker: john@electricenergyonline.com

Art Designers:
Anick Langlois: alanglois@jaguar-media.com

Internet Programmers:
Johanne Labonte: jlabonte@jaguar-media.com
Sebastien Knap: sknap@jaguar-media.com

Electric Energy Magazine is published 6 times a year by: Jaguar Media Inc.
1160 Levis, Suite 100,
Terrebonne, QC Canada J6W 5S6
Tel.: 888.332.3749 • Fax: 888.243.4562
E-mail: jaguar@jaguar-media.com
Web: www.electricenergyonline.com

Electric Energy T&D Magazine Serves the fields of electric utilities, investor owned, rural and other electric cooperatives, municipal electric utilities, independent power producers, electric contractors, wholesalers and distributors of electric utility equipment, manufacturers, major power consuming industries, consulting engineers, state and federal regulatory agencies and commissions, industry associations, communication companies, oil & gas companies, universities and libraries.

Post Publication mail agreement #40010982
Account #1899244

COVER PAGE IMAGE:
Avista Utilities
J. Craig Sweat, Photograph

National Rural Electric Cooperative Association
ASSOCIATE MEMBER

Electric Energy T&D is proud to be a member of these associations

gita
GEOSPATIAL INFORMATION & TECHNOLOGY ASSOCIATION

Circle **11** on Reader Service Card

Powerful Software for Power System Professionals

• Electric T&D Modeling & Analysis • Interactive Voice Response • Electric Utility GIS & Field Engineering • Outage Management

Smart meters are central to Smart Grid technologies which are revolutionizing the electric utility industry. As smart meters make more and better data available, powerful software is required to take full advantage of that data. A Smart Grid makes Milsoft software even more powerful and Milsoft software makes a Smart Grid even more valuable. Get the most out of your Smart Meter investment with Milsoft software.

Scan this into a QR code app on your phone to read more about Milsoft Utility Solutions.

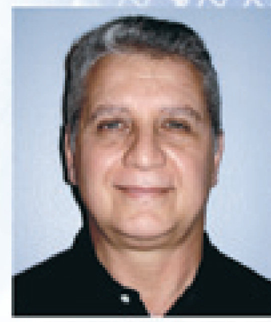
www.milsoft.com • 800.344.5647 • info@milsoft.com

MILSOFT
Utility Solutions

facebook twitter linkedin

GridLines

Michael A. Marullo,
Editor in chief



You can't do that online!

A few weeks ago, just before returning from our Fall Smart Grid RoadShow Conference in Corpus Christi, Texas, a somewhat disturbing bit of news hit my Inbox. It was the results of a survey we (meaning the Jaguar Expo business unit of Jaguar Media, the latter of which is the publisher of this magazine) had co-sponsored with several other 'Smart Grid' event developers. The purpose of the study – carried out by the widely respected McDonnell Group (Atlanta, GA) – was designed to gather some perspective on the scores (and still growing, by the way!) of conferences that at least claim to address Smart Grid topics in one way or another.

The survey went out to a large cross section of utilities of all types, sizes and locations across the United States and Canada. In the end, TMG managed to secure 100 qualified respondents from across the target market set of the roughly 3,000 electric utilities serving North America, which is a very respectable sample for a study of this type. While I cannot even begin to address all of the results of that effort here, there were a few things that I think are worthy of note.

First of all – and probably the most disturbing finding of that research – is that many of the utilities surveyed are planning to further reduce their conference attendance in the coming year. That this comes now is not a big surprise; after all, we're just coming out of the worst recession in history, and utilities are understandably concerned about costs associated with what they deem – correctly or incorrectly – as 'non-essential' expenses. And this comes on the heels of conferences getting demoted years ago from a separate budget to an agglomeration of all things educational.

'Nothing wrong with that,' one might say. How could being lumped in an educational activity possibly be a bad thing? Well, of course, it isn't a bad thing at all – at least not from a philosophical standpoint. But it does have an important financial component that simply can't be ignored. The downside is that dollars once dedicated exclusively to trade shows, conferences and symposia are now being shared with things like short courses, seminars, webinars and other pure-play educational endeavors. Again, there's nothing wrong with being cast in an educational light, but the fact remains that the money is being spread over wider set of choices, and that usually means that somebody isn't getting as much as they wanted or expected or, in some cases, really needed.

What really disturbs me, however, is that I feel like this is going to be an irreversible trend. It reminds me of when a drought in Marin County, California in the 1970s caused restaurants to stop serving water to patrons. After a few months the drought ended, but the moratorium on restaurant water didn't. (I should point out here that like being associated with education, being a part of conserving natural resources isn't a bad thing either, since it saves both water and energy in very large amounts; and over time, makes a huge difference!)

If you're wondering why I'm so concerned about this, I assure you that my role as a conference chairman – though professionally quite gratifying – is really incidental to the larger issue. That larger issue is the growing sentiment that conference participation is a relic whose time ended with the 20th century. My problem with that notion is very simple; we didn't stop being human when the last century ended, and we didn't stop needing human interaction when the Internet was invented.

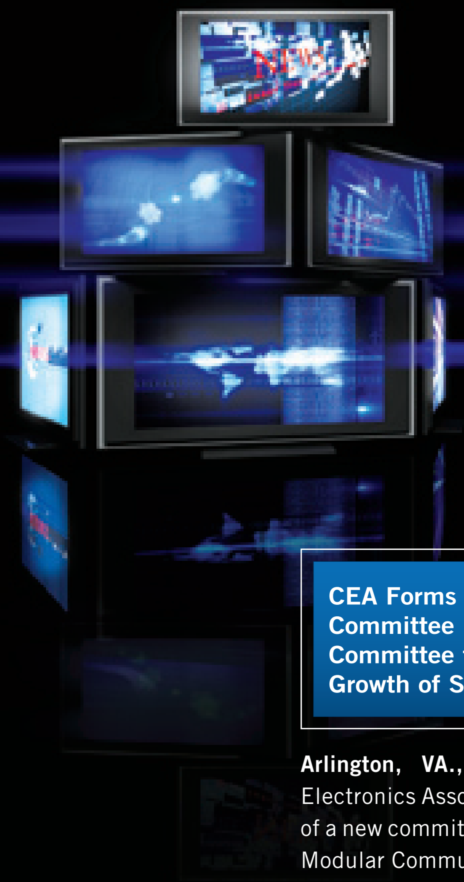
I think most people would agree that communicating has gotten a lot easier in the past decade. Despite all of the email issues we endure, slow Web pages, dropped calls, and more recently, those Tweets of "I had a tuna sandwich for lunch today!" most everyone appreciates the positive side of being able to get news, exchange information, and yes – even pause for a bit of humor now and then – at the speed of light (unless, of course, you're still using a dial-up connection!). Yet I have to admit that it's a little disturbing to watch kids text each other when they're sitting three feet apart on the sofa.

But kidding aside, that's where my concern really begins. That concern is about our ability to understand that there are many kinds of communicating – it's not a one-size-fits-all proposition. Instead, some forms of communication fit nicely into a 140-character Tweet, while others may require a more explanatory text message (albeit in some nearly incomprehensible dialect of what you can only loosely call a language), and still others may deserve a full email – the medium that most younger folks have now relegated to the communications medium of 'old' people.

Then there's a whole different class of communicating that is seemingly in danger of extinction. That involves an actual conversation between two or more human beings, ideally in person for the maximum (and most gratifying) experience. And in case you don't remember the 20th century, this kind of communication between humans has often been observed taking place at trade shows, conferences, symposia and other such gatherings with common interests.

Frankly, I'm distressed by how many people I hear making comments like, "*Why should I go to a conference? It's just a bunch of vendors anyway. And besides, I can get anything I need on the Web for free.*" It would take me many more pages to even scratch the surface of all the ways I disagree with those views, but let me sum up with this…

Before you decide whether conferences are a necessary part of your budget, ask yourself a few simple questions like: Which websites let you determine whether the keyboard on your next system has the right tactile feedback? Which ones allow you to meet the people that will be supporting your system? And, which ones will help you resolve those thorny technical problems? The reality is, you can't do that online! – ***Ed***.



INDUSTRY NEWS

CEA Forms Smart Grid Interface Standards Committee

Committee to Accelerate Adoption and Growth of Smart Grid Products

Arlington, VA., November, 2011 - The Consumer Electronics Association (CEA)® announced the formation of a new committee to advance the standardization of the Modular Communications Interface (MCI) specification. The new standard will benefit manufactures, utilities, service providers and consumers as it creates a path to Smart Grid ready products.

The MCI specification, created by the Universal Smart Network Access Port (USNAP)

Alliance and based on research from the Electric Power Research Institute (EPRI), will allow manufacturers of consumer products to build Smart Grid ready products that can obtain energy information from digital meters and energy system interfaces regardless of the communication technology used.

The USNAP Alliance will work with the CEA committee, CEA R7.8 Modular Communication Interface for Energy Management, to support the industry adoption of the MCI standard through certification and test programs. EPRI continues to provide valuable research, conducting interoperability workshops through which prototype devices and demand response programs can be evaluated.

“This committee is designed to accelerate the adoption and growth of Smart Grid ready products,” said Brian Markwalter, senior vice president of research and standards for the Consumer Electronics Association. “We’re eager to build on the significant efforts of USNAP and EPRI to create this standard by further addressing the needs of manufacturers, utilities, service providers and consumers alike.”

At the request of the National Institute of Standards and Technology (NIST), independent modular interface initiatives from the USNAP Alliance and EPRI were merged into a unified specification that identifies the interface between a Universal Communication Module (UCM) and a Smart Grid Device (SGD). A NIST working group completed the MCI specification, and it was formally submitted to CEA to facilitate creation of the standards development project.

“This new specification addresses a significant gap in the Smart Grid for a unifying technology that enables a range of consumer products to respond to demand response events,” said Brian Seal, technical executive for EPRI.

“Consumers benefit from the selection of Smart Grid ready products that can be used anywhere in the country,” said Jon Rappaport, chairman of the USNAP Alliance. “Manufacturers benefit because they can build standardized products capable of working in any service territory. Utilities benefit because this specification reduces the risk of stranded assets.”

Circle **16** on Reader Service Card

AEP Ramps Up Economic Development Program to Support Business and Job Growth in Service Territory

Mark J. James joins company as vice president of economic and business development

Columbus, OH, November, 2011 - American Electric Power (NYSE: AEP) will increase its focus on economic development activities throughout the company’s 11-state service area and has hired Mark J. James, who previously led AEP’s economic development efforts, as vice president of economic and business development, effective on November 21.

INDUSTRY NEWS

"In today's economy, it is more important than ever that we support local, state and regional economic development efforts to attract new business, help companies expand their operations in our service territory, and create jobs," said Robert P. Powers, AEP executive vice president and chief operating officer. "Mark's leadership experience, as well as his expertise in developing and implementing economic development programs for AEP and other companies, will help us more aggressively pursue new business opportunities and coordinate our economic development efforts across the company."

James is responsible for the strategic expansion of AEP's economic development program, identifying and pursuing opportunities to increase retail load. As part of this effort, AEP will assist companies in all aspects of business development, including research, work force analysis, site and building selection, identification of financing programs, and coordination with other business contacts and public officials. James reports to Craig Rhoades, vice president of Customer Services, Marketing and Distribution Services.

Since 2002, James has served as founder, president and chief executive officer of ED Solutions, Inc., a consulting firm providing economic development tools, training and project management services. He previously spent 17 years with AEP, most recently as director of economic development a position he held from 1992 to 2002. He served as economic development consultant for AEP in West Virginia from 1985 to 1992. Prior to that, James was director of community development for the municipality of Bethel Park, Penn. and regional planner for the Bel-O-Mar Regional Council in Wheeling, W.Va.

He holds a bachelor's degree in geography and environmental sciences from Edinboro State University of Pennsylvania and a master's degree in economic geography from Oregon State University. James is a graduate of the University of Michigan's Ross Graduate School of Business Executive Management Program and is a certified economic developer (CEcD).

Circle **17** on Reader Service Card

NRECA's Smart Grid Demo Project Finalizes $26.7 Million in Contracts

Arlington, VA, November, 2011 - Effective Tuesday, November 15, 2011, the National Rural Electric Cooperative Association closed on contracts worth $26.7 million for smart grid components to be deployed at 23 cooperatives participating in the cooperatives' regional Smart Grid Demonstration Project (SGDP).

Supported by a matching grant from the U.S. Department of Energy, over the course of the project, participating cooperatives are deploying more than 75 technologies and equipment in twelve states.

NRECA has made these purchases for research and evaluation of the following smart grid features:

COMMUNICATIONS
AMI systems and digital communications software and infrastructure to enable smart grid features including demand response over AMI, load management, prepaid metering and in-home energy displays.

EFFICIENCY AND DEMAND RESPONSE
Software and equipment to improve efficiency both at the operational and end-user level, and enable automated demand response and load control. Components include load control switches, in-home displays, advanced Volt-Var control, demand response over AMI and meter disconnect collar sealing kits.


Experience
the Power
of Dow Inside
DOW
INSIDE

RELIABILITY AND POWER QUALITY
Software and equipment to improve reliability by implementing SCADA, self-healing capability, power quality monitoring and regulation and improved conservation voltage regulation.

DISTRIBUTED GENERATION AND RENEWABLE ENERGY
Equipment to assist the integration of renewable energy and distributed generation resources.

NRECA has executed contracts with the following vendors: Cooper Power Systems, Inc., HD Supply Utilities, Ltd., Stuart C. Irby Company, Larson Communications, Inc., RFIP, Inc., Ruggedcom, Inc., VFP, Inc., Alstom Grid, Inc., Nolan Power Group, Inc., Hunt Technologies (aka Landis & Gyr) and QEI, Inc.

Circle **18** on Reader Service Card

New Report Paints Detailed Portrait of U.S. Residential Energy Consumers - and What Motivates Them

SGCC's Consumer Pulse and Market Segmentation Study finds five distinct segments based on nationally representative survey of beliefs, behaviors, demographics

Atlanta, November 16, 2011 - Residential U.S. electric consumers fall into five distinct segments that influence their willingness to participate in energy management programs, according to the SGCC's Consumer Pulse and Market Segmentation Study, a national research project conducted for the Smart Grid Consumer Collaborative (SGCC) by Market Strategies International.

Unlike other segmentation studies to date, SGCC's Consumer Pulse and Market Segmentation Study is a nationally representative telephone survey that has been used to create a richer, more actionable segmentation framework. The study spent more than twenty minutes per phone call, delving deeply into beliefs, attitudes, behaviors and demographics. The results were then combined with specific energy data to create meaningful insight into consumer lifestyles, attitudes, values, motivations and communication preferences.

SGCC's Consumer Pulse and Market Segmentation Study was conducted by telephone from August 15 to September 6, 2011. A national RDD (random digit dialed) landline and cell phone sample was used. To qualify, a respondent had to be over the age of 18 and a head of household. Targeted RDD sample was also used when needed to assure appropriate representation of key ethnic and age groups, and the data were weighted by age, ethnicity, gender and region to align with national population parameters. The margin of error for the total sample size of 1,200 is ± 3.2 percentage points at a confidence level of 95%.

The study presents five distinct profiles of U.S. residential electric consumers:

- Concerned Greens (31%) are most protective of the environment and supportive of smart grid initiatives. They are highly likely to participate in energy management programs.
- Young America (23%) doesn't know much about smart grid but is interested in learning about its potential for environmental benefits and cost savings.
- Easy Street (20%) consumers have the highest income of any segment and are reluctant to change their personal behaviors.
- DIY & Save (16%) consumers are frugal and have a do-it-yourself lifestyle. Their biggest concern is providing for their family, not global environmental issues.
- Traditionals (11%)* are set in their ways and do not see the need for energy reform.

"Utilities that take the time to understand each segment's characteristics, attitudes, values and motivations can engage their consumers successfully and provide the most appealing smart grid-enabled products and services," said Patty Durand, SGCC executive director. "The results from this study have the power to change the relationship between utilities and their customers. The day of the faceless 'rate payer' gives way to a portrait of a real human being with a unique personality and distinct characteristics."

SGCC's Consumer Pulse and Market Segmentation Study marks the first of three waves of research to help utilities understand consumer perspectives toward Smart Grid issues. Download a report summary on SGCC's website. For the detailed report, contact *sgcc@smartgridcc.org*. In addition, SGCC is providing its members with a set of 12 survey questions that they can use to classify their own customers into the SGCC segments with high accuracy.

Circle **19** on Reader Service Card

ESPS | ESTS
www.esps.ca
ELECTRICAL SAFETY TRAINING SYSTEM

www.arcflash-training.ca

Multi-Media State-of-the-Art Online Safety Training System

Take control of the quality, consistency and cost of your arc flash and shock training for your electrical workers!! Increase the frequency of training which will assist you in moving the training knowledge to electrical worker electrical safety competency. **Classroom training is expensive, can be inconsistent as you get different instructors provided by the vendor and not sustainable; you can only retrain every 3 to 5 years due to the high overall cost!!**

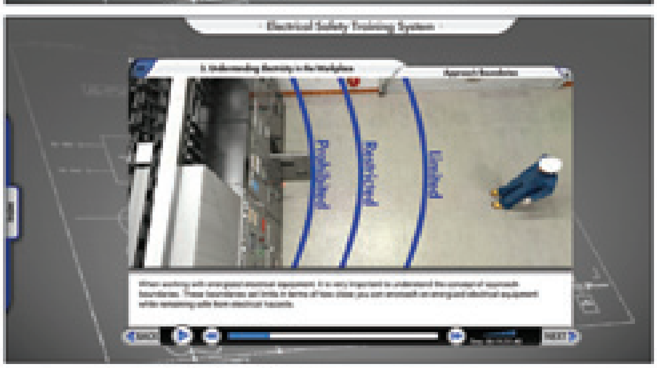
The Electrical Safety Training System (ESTS) is credible, high quality, affordable, impactful computer based training delivered over the internet or on standalone DVDs.

3D Graphics, Videos and Narrated Content
Divided into 10 modules, the four-hour online training system covers the fundamentals of the electrical hazards of arc flash and shock. It uses 3D graphics, videos and narrated content to provide information on the dangers of arc flash and shock, and how to protect yourself. It provides information on how to analyze these electrical hazards and follow up on preventive and protective control measures.

CSA Z462 Training
Unique to the ESTS system is the 3D Virtual Electrical Workplace classroom, where the student will be able to apply learning in interactive scenarios about arc flash and shock and the application of the CSA Z462 Workplace electrical safety Standard.

Terry Becker, P.Eng., a CSA Z462 Technical Committee Voting Member and indepedant Electrical Safety Consultant, is the Subject Matter Expert and Visionary of the ESTS and advises that the training system is credible, high quality multi-media adult learning delivered online. Every work can receive training.

Please call If you have your own LMS and would like to use the ESTS behind the firewall. Additionally if you want customized company Electrical Safety Program training the ESTS can be customized to suit your requirements.



Single seat access is $95.00 + GST.
(bulk seat pricing is available upon request)

For more information, contact Terry Becker, P.Eng. at ESPS.

ESPS electrical safety PROGRAM SOLUTIONS inc.

ESPS Electrical Safety Program Solutions INC.
E-mail: terry.becker@espsi.ca
Telephone: 403.532.9050
www.esps.ca

Circle **4** on Reader Service Card

INDUSTRY NEWS

Pepco Energy Selected to Implement $27.6 Million Energy Performance Contract for Maryland Port Administration

New Energy Conservation Measures will be part of Governor's EmPOWER Maryland initiative

Arlington, VA, November, 2011 - Pepco Energy Services, Inc., a subsidiary of Pepco Holdings, Inc. (NYSE: POM) and a leader in energy savings performance contracting, has been awarded a $27.6 million comprehensive energy performance and maintenance contract by the Maryland Port Administration.

A total of 14 buildings spanning more than 570,000 square feet will be impacted by the project. These facilities include the World Trade Center in the Inner Harbor, the Maryland Cruise Passenger Building, and Maryland Port Administration facilities in the Dundalk Marine Terminal, South Locust Point Marine Terminal, and Cox Creek, all located in Baltimore, Md.

"This is a win-win program for the Maryland Port Administration, our customers, and the taxpayers of the state of Maryland," said Ed Klingenstein, Engineering & Energy Manager at the Maryland Port Administration. "This is another example of how energy performance contracting can enable state agencies to achieve governmental goals and mandates, while maintaining and improving facility infrastructure and creating sustainable jobs without increasing agency budgets."

The contract calls on Pepco Energy to install 22 energy conservation measures. Highlights of the project include the implementation of a Geothermal Harbor Heat Sink at the World Trade Center. This renewable technology uses the Baltimore Harbor's water to cool the World Trade Center reducing electricity, water consumption, and chemical treatment. These benefits will help Baltimore City achieve its 2020 initiatives for the Harbor waters.

Kathy Broadwater, Deputy Executive Director of the Maryland Port Administration said, "This contract helps the State maximize energy efficiency and is a critical part of Governor O'Malley's EmPOWER Maryland initiative. We are committed to providing our customers with superior service through innovative thinking and operations, and this project is a fine example of how we are working to achieve the mission of the Maryland Port Administration."

Pepco Energy will install an aggregate 750 kW high-efficiency photovoltaic system on two building rooftops, which are the largest of the systems installed under the Maryland Department of Transportation solar initiatives. The electricity generated will be used to directly power these facilities during peak operational hours, producing an estimated $93,400 per year in electricity savings.

"This is exactly the kind of project Pepco Energy excels at implementing – it's large scale, multifaceted, and renewable with operational support to allow the Maryland Port Administration to realize the full benefits of long-term energy sustainability planning," said John Huffman, President and Chief Executive Officer of Pepco Energy. "As a result this comprehensive project will reduce the Maryland Port Administration's energy usage by more than 30 percent."

The project also includes measurement and verification services, along with equipment maintenance over the entire contract term. Maryland Port Administration employees and clients will benefit from this project as well through an Energy Awareness program to be initiated by Pepco Energy Services.

Over the 13.5-year contract term, the Maryland Port Administration will save more than $22 million in energy costs. The project will also result in a reduction of more than 4,100 metric tons of carbon dioxide emissions. The project will be partially financed through the Maryland Energy Administration's Project Sunburst Grant, as well as the local utility's Smart Energy Savers Program utility rebates.

Construction is already underway and is scheduled to be completed in November 2012.

For information, visit: *www.pepcoenergy.com*

Circle **20** on Reader Service Card

INDUSTRY NEWS

First 'Small Scale' Demand-side Projects in PJM Providing Frequency Regulation
New PJM Rules Open Market to Smaller-Scale Demand-Side, Distributed Technologies

Valley Forge, PA, November, 2011 - PJM Interconnection received the first frequency regulation services from small-scale demand resources under new rules allowing smaller projects to participate in PJM's Regulation Market. The two western Pennsylvania projects use diverse technologies.

To provide regulation service to PJM, demand resource provider Enbala Power Networks uses water pumps at a wastewater treatment facility in Washington County, Pa., adjusting its water pumps up or down to match PJM's regulation signal. The other project from Viridity Energy uses building load and a behind-the-meter battery in New Castle, Pa. The battery responds to the PJM signal – either charging or discharging as appropriate. "We've long seen the value of demand-side resources in our markets, so expanding the opportunities for demand response to participate in the regulation service market makes sense and offers a faster and potentially more accurate response," said Andrew L. Ott, PJM senior vice president – Market Services. "Our new minimum level for participation allows demand-side resources and other innovative technologies to cost-effectively enhance grid reliability."

Regulation service corrects for short-term changes in electricity use that might affect the stability of the power system. It helps match generation and load and adjusts generation output to maintain the desired frequency. Previously, system operators have relied on flexible generating resources to vary output to balance system frequency.

In October, the Federal Energy Regulatory Commission approved rule changes that reduced the minimum required amount of resources to 100 kW, from the previous minimum of 500 kW.

Circle **21** on Reader Service Card

Entergy New Orleans Files Formal Request to Join MISO
New Transmission Arrangement Would Benefit Customers, Economy

New Orleans, November, 2011 - With an eye on meeting the future energy needs of its customers, Entergy New Orleans, Inc. filed a formal change of control request with the New Orleans City Council to join a regional transmission organization, the Midwest Independent Transmission System Operator or MISO.

Entergy New Orleans is seeking to transfer functional control of its transmission facilities to MISO with a target implementation date of December 2013.The utility company will retain ownership of its generation and transmission facilities, along with responsibility for maintaining them.

Initially announced in April, Entergy New Orleans' decision to join MISO followed a lengthy period of study of various alternatives aimed at affordably and reliably meeting the long-term energy needs of the New Orleans community. The company projects that joining MISO will yield savings to customers of up to $46 million over a 10-year period, primarily due to MISO's organized power markets, which allow for a more efficient commitment and dispatch of generation resources, and to the economies of scale offered by an RTO of MISO's size. "MISO has a well-documented record of reducing production costs while strengthening reliability," said Charles L. Rice, Jr., president and chief executive officer of Entergy New Orleans, Inc. "Extensive analysis has shown that joining MISO provides important and sustained benefits for the homes and businesses we serve in Orleans Parish.

"Becoming part of MISO's extensive, efficient and reliable energy market will help keep energy costs affordable for our customers," he added. As New Orleans' retail regulator, the New Orleans City Council will continue its regulatory oversight of Entergy New Orleans and its facilities. Additionally, MISO membership brings the opportunity for the City Council to participate in MISO's large-scale regional planning process and its Organization of MISO States, which provides input to MISO's management team and board of directors.

MISO operates an electrical grid across 12 states; with the addition of the Entergy New Orleans and the other Entergy operating companies, MISO will reach from Canada to the Gulf of Mexico.

Entergy New Orleans, Inc. is an electric and gas utility serving Orleans Parish and is a subsidiary of Entergy Corporation. The company provides electricity to more than 160,000 customers and natural gas to more than 100,000 customers in Orleans Parish.

For a Frequently Asked Questions document, visit *http://entergy.com/rto/faq.pdf*. For more information, Entergy's online address is *www.entergy.com*.

Circle **22** on Reader Service Card

Avista's Pullman Smart Grid Demonstration Project

By Heather Rosentrater, Director of Asset Management and Process Improvement, Avista
and Narasimha Chari, Co-Founder & Chief Technology Officer, Tropos Networks

With the implementation of its Pullman, Wash., Smart Grid Demonstration Project, Avista stands at the forefront of comprehensive smart grid deployment. The project aims to modernize much of Avista's Pullman electric distribution system using intelligent devices and two-way communication. As part of the project, Avista is installing a wide-area private wireless broadband network as its communications infrastructure. In addition to distribution automation, the project encompasses advanced metering infrastructure and a customer pilot that will provide customers in-home energy consumption data, establish and test regional demand response signals and help the utility understand customer experience, satisfaction, and program participation.

The project's goals are to understand the value smart grid technologies can bring to Avista and its customers, as well as the costs of providing those benefits, so that the utility can better analyze costs and benefits of various smart grid applications. In addition to understanding the viability of each service used in the project, Avista seeks to understand how to best expand successful smart grid applications to the rest of the company's customers.

Avista is an investor-owned utility headquartered in Spokane, Wash. The company provides electricity to about 357,000 customers and natural gas to 317,000 customers. Its service territory spans approximately 30,000 square miles in eastern Washington, northern Idaho and parts of southern and eastern Oregon.

Avista's Pullman Smart Grid Demonstration Project is part of the Pacific Northwest Smart Grid Demonstration Project, a project led by Battelle under the auspices of the U.S. Department of Energy (DOE). The project involves 11 utilities, the Bonneville Power Administration, along with the University of Washington, Washington State University, and five technology partners. The project has a budget of $178 million split between the DOE and project participants. The project aims to verify the viability of smart grid technology and quantify smart grid costs and benefits.

Under this umbrella, Avista is implementing the Pullman Smart Grid Demonstration Project in cooperation with local cost share partners Itron, Washington State University (WSU), Hewlett Packard and Spirae. The total cost of the project is expected to be $38 million. Avista is contributing $14.9 million, Avista's cost share partners an aggregate of $4 million and the DOE is supplying a matching grant of $19 million. Other partners include vendors and contractors such as Scope, Efacec Advanced Control Systems and Schweitzer Engineering Labs.

Avista selected Pullman for the Smart Grid Demonstration Project because it is the right size and offers a good mix of industrial, commercial and residential customers. Pullman is also the home of WSU, with its acclaimed Power Engineering program. WSU's current research areas include smart home, wind integration, electrical grid security and electric grid stability. The city is also home to Schweitzer Engineering Labs, a leading vendor of protective equipment. An important aspect of Schweitzer's and WSU's participation is that both have small scale electric generation capability, critical for testing distributed generation integration and net metering.

Avista's goals for the Pullman Smart Grid Demonstration Project are to demonstrate and evaluate smart grid applications and technologies; show how the electric grid can react to sudden changes in power supply and demand; and help prepare Avista and its customers for the modernization of the electrical grid. The company will meet these goals by:

- Upgrading electrical facilities and automating the electrical distribution grid to support intelligent devices and two-way communication between the utility and all parts of the system.
- Demonstrating technologies and tools, including advanced metering, in-home devices and web tools, to understand ways to enable customers to actively monitor and better manage their energy usage.

Potential benefits of the project include:

- Less waste from lost power as it moves through the transmission and distribution system helps Avista reduce operating costs and conserves power to help meet demand.
- Distribution technology can automatically detect and isolate an outage, saving time and reducing outage frequency and length for customers.
- Partnering with customers to provide them with better information about their energy usage gives customers tools to use energy more efficiently.

Distribution Automation

Recently, advances in communication technologies have enabled the smart grid vision of distribution automation. Devices such as capacitor banks, switches, reclosers, sectionalizers and transformers can be actively monitored and operated remotely from substations and in utilities' data centers.

The distribution portion of the Pullman Smart Grid Demonstration Project encompasses 13 distribution feeders. Along these feeders, Avista has installed 34 reclosers and 30 capacitor banks. With these devices, Avista can quickly and automatically pinpoint distribution network faults, reducing the number and frequency of outages and improving system reliability. They also enable the utility to reduce energy losses, lower energy consumption and better integrate distributed renewable generation resources.

In addition, Avista is installing smart transformers in Pullman. These devices provide integrated telemetry, including voltage and current measurement, as well as thermocouples to determine internal temperature. Avista will use the telemetry data to perform conservation voltage reduction calculations for automated Volt/VAR management and to proactively determine when transformers need to be replaced. And, when coupled with the project's advanced metering infrastructure (AMI) deployment (see below), smart transformers could help the utility detect electricity theft by comparing the amount of power passing through a transformer to the aggregate power consumption measured by the smart meters downstream from that transformer.

Increased Reliability

The smart reclosers automatically reroute power to minimize the effect of an outage. They support fault isolation to enable upstream and downstream restoration of electricity with no operator intervention. This capability can increase reliability by reducing the length of outages from hours to minutes.

The example below demonstrates how distribution automation can quickly restore power in the event of a fault. During normal operation, the neighborhood has three distribution circuits, one from each of three substations, as shown in **Figure 1**.

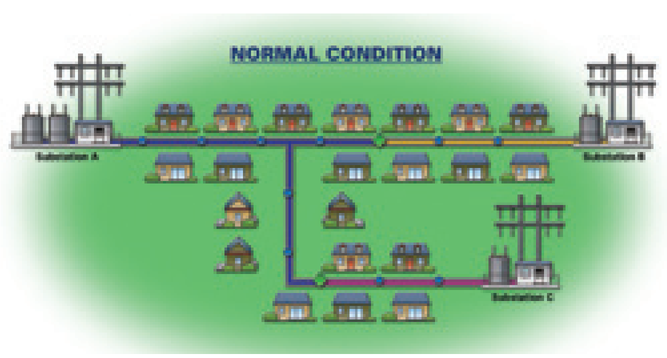


Figure 1

In **Figure 2**, a fault occurs, perhaps because a car has hit a utility pole. The fault causes all homes served by Substation A to lose power.

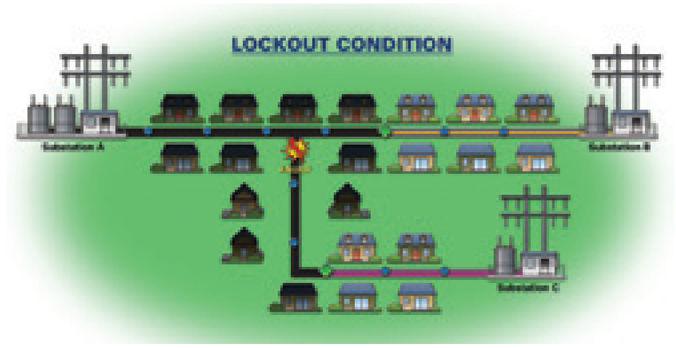


Figure 2

In **Figure 3**, service between the fault region and Substation A is restored by automatically closing the reclosers upstream from the fault.

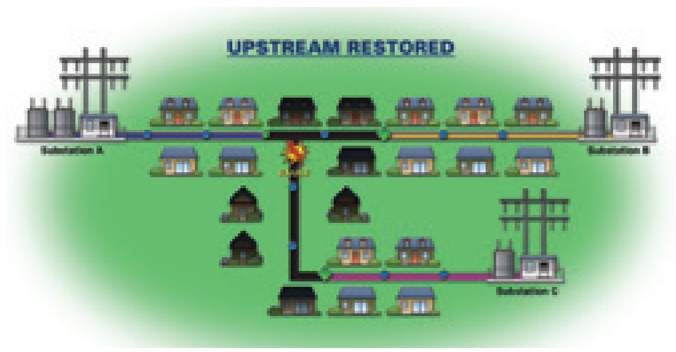


Figure 3

In **Figure 4**, service between the fault region and Substations B and C is restored by closing the reclosers serving as tie points between the distribution circuits and closing the reclosers between the tie points and the fault. Now the outage is contained to the area between the site of the accident and the nearest recloser in the direction of each substation.

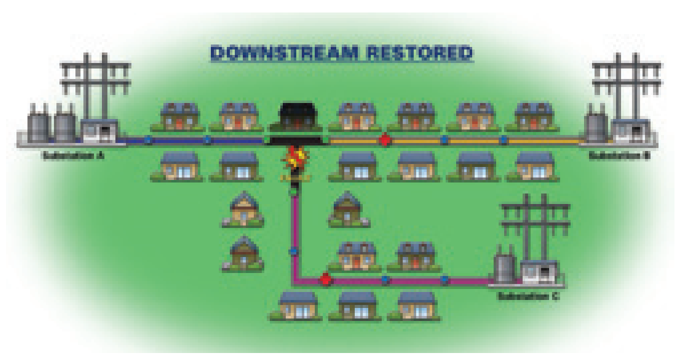


Figure 4

Without smart grid technology on the distribution system, isolating the fault is a manual process. Manipulating the reclosers requires truck rolls, which can take hours. With smart technology, the process can be computerized and automated – requiring little or no manual intervention – and could be accomplished in minutes.

Increased Efficiency, Reduced Power Consumption

In addition to increased reliability, the Pullman Smart Grid Demonstration Project promises increased efficiency and reduced power consumption. The project will use active Volt/VAR management and conservation voltage reduction (CVR) to reduce system losses that occur through distribution, saving energy and reducing carbon emissions. In addition to reducing carbon emissions from power generation, the Pullman Smart Grid Demonstration Project could enable Avista to reduce emissions and fuel consumption by reducing vehicle use for switching, outage isolation and service restoration.

Advanced Metering Infrastructure Deployment

Avista electric and gas customers in Pullman, including residential, commercial and industrial customers, have been outfitted with advanced metering. In total, approximately 13,000 electric and 5,000 natural gas meters were upgraded to advanced meters in spring and summer 2011.

Advanced metering can offer benefits to Avista and its customers alike. The utility could decrease labor costs by reducing the number of employees who must travel into the field to manually read meters. For new tenants and homeowners, the process of transferring utility service from the previous occupant will become faster because Avista will be able to conduct the required meter reading from a central location rather than having to schedule a truck roll to perform a manual, in-field reading. Service connection and disconnection can also be accomplished from a central location, without a truck roll.

In the future, the advanced metering infrastructure would also assist Avista with outage management. The meters could notify Avista when power to individual homes and businesses is interrupted. Proactive notification can enable the utility to promptly detect outages and accurately determine their scope. As power is reestablished, the meters would also notify Avista of restoration at individual locations, allowing the utility to ensure that power is available to all customers without remaining isolated pockets of outage.

The advanced meter technology can also enable Avista to provide information to customers about their ongoing energy usage. The information collected by the meters and made available to customers, using tools such as a secure web portal, can include interval usage data. This information can allow customers to actively monitor and manage their energy usage and make more informed decisions about choices that drive their costs.

Conservation Voltage Reduction (CVR)

The concept behind CVR is simple – reduce power consumption by slightly reducing voltage. Implementation, however, is complex.

Nominal 120V power has a +/- 5% tolerance, i.e., as long as the actual voltage delivered to the customer is between 114V and 126V, the power is considered to be within specification. In practice, most utilities transmit power from substations at the high end of this range to ensure that, after distribution line loss, customers at the far end of the distribution feeder receive electric service that conforms to the minimum voltage limit. The net effect is that customers can receive higher than necessary voltage and, as a result, consume unneeded power.

Using CVR, utilities lower the voltage of the electricity they transmit from their substations to conserve power. While CVR can reduce power consumption, utilities must ensure that, at all points along the distribution feeder, the supplied power remains within the specified voltage range at all times.

Utilities can make certain that voltage remains within specification throughout their distribution feeders by installing voltage measurement points. These measurement points can be remotely monitored via a wireless network. By monitoring the voltage along feeders, the utility can implement a feedback system that enables conservation voltage reduction while ensuring that customers at the far end of feeders receive voltage that conforms to specification.

Customer Pilot

The customer pilot enables customers to actively participate in the Pullman Smart Grid Demonstration Project. Plans for this voluntary pilot project include providing a home area network (HAN) and smart in-home devices such as thermostats, so customers can view and manage their energy usage in the home at the time of use. This should enable customers to detect spikes in energy use almost immediately.

Avista plans to recruit up to 1,500 volunteers to participate in this program. Another aspect of the pilot is demand response. When demand begins to outstrip supply, the demand response system can adjust smart thermostats in the homes of pilot volunteers to conserve power and better balance demand with supply. Customers can override settings or opt out at any time.

The demand response portion of the Pullman Smart Grid Demonstration Project is expected to show how the electric grid can react to sudden changes in power supply and demand. This is important for making the grid renewables-ready, demonstrating how it can adjust to intermittent renewable power sources such as wind and solar.

Transactive Signaling

The demand response functionality of Avista's customer pilot uses the capabilities of a transactive control system located at Battelle. This system continually monitors electricity supply and demand, issuing a transactive signal whose value depends on the supply/demand balance.

During times when demand outpaces supply, for example when energy use is low and intermittent renewable power sources are on line, the value of the transactive signal is low. When demand outstrips supply because of, say, a spike in usage or a drop in supply due to, for example, wind-generated power going off line on a calm day, the value of the transactive signal increases. The transactive signal is analogous to price in a product market, which will increase when demand begins to exceed supply.

In the case of Avista's pilot project, when the transactive signal rises above a programmable threshold, the demand response system would communicate with the smart thermostats in homes participating in pilot. The demand response system would adjust the smart thermostats to conserve power, better balancing supply and demand.

Pullman Smart Grid Demonstration Project Communication Requirements

In choosing a network for the project, Avista conducted a multi-dimensional technology analysis. The technologies considered, the choices that Avista made, and the factors that led them to make those choices are summarized in the following table.

Selected Technology	Alternative Considered	Factors Driving Choice
Wireless Network	Wireline Network	Lower cost, mobile workforce support
Unlicensed Spectrum	Licensed Spectrum	Ease of regulatory compliance
Private Network	Public Network	Best alignment with utility requirement
Broadband Network	Narrowband Network	Required aggregate bandwidth
Proven Technology	New Technology	Proven success and reliability

Based on these criteria, Avista elected to deploy a wide-area private wireless broadband network based on technology from Tropos Networks that is embedded in Itron AMI collectors and routers. The network's capabilities closely match Avista's requirements in each technology dimension considered.

Pullman's Private Wireless Broadband Network

Avista's network provides a high performance wireless distribution area network for smart grid communications. Based on open industry standards, it enables real time communications between the utility's data center, substation controllers, distribution automation devices, and AMI collectors and meters.

Avista's network provides a common communications infrastructure for all of the Pullman Smart Grid Demonstration Project's initial applications. It also offers the capacity, security, reliability, scalability, low latency and multi-use feature set needed to enable Avista to deploy additional applications, such as SCADA, mobile workforce automation and substation security, on the network in the future.

The network was constructed using wireless broadband routers mounted on utility pole horizontal mast arms and overhead neutral conductors throughout the coverage area. The routers provide wired 10/100BASE-T Ethernet connectivity to smart grid devices co-located with the routers and a communications path to Avista's core fiber optic network, connecting at the utility's substations.

Using the network and sophisticated head-end system software, Avista can manage the distribution system and provide both automated and operator initiated responses to faults in distribution circuits. The combination of intelligent devices in the field, a high-performance communications network and head-end software enables Avista's Pullman Smart Grid Demonstration Project to deliver increased efficiency and reliability.

The Road Forward

With the Pullman Smart Grid Demonstration Project, Avista aims to improve system reliability, reduce energy losses, lower system costs, reduce the frequency and length of customer outages and learn more about integrating distributed renewable generation resources.

The project includes advanced metering infrastructure and a customer pilot in addition to distribution automation. The project should provide Avista with data the company needs to better analyze costs and benefits of various smart grid applications. In addition to understanding the viability of each service in the demonstration project, Avista seeks to understand how to best expand successful smart grid applications to the rest of the company's customers.

Avista is using a wireless broadband network as the communications foundation. With the network providing the communications infrastructure, Avista is evaluating the deployment of many smart grid applications, including AMI with interval metering, distribution automation, home area networks, demand response, outage management, distributed generation integration, plug-in hybrid electric vehicle support, substation security and more on a single secure, reliable and scalable broadband wireless network. ■

ABOUT THE AUTHORS

Heather Rosentrater joined Avista in 1996 as a student while studying Electrical Engineering in college. Upon receiving her bachelor's degree from Gonzaga University in 1999 and was hired as an engineer at Avista. Rosentrater has held several energy delivery engineering positions. In 2009 she became the Director of Asset Management and Process Improvement. In her current role she has direct oversight of Avista's two Smart Grid stimulus projects, which have a combined project value over $80 million and project schedule of five years. She is a registered Professional Engineer, an Adjunct Professor at Gonzaga University and serves on the Advisory Council for Washington State University's School of Electrical Engineering and Computer Science.

Narasimha Chari is the co-founder and Chief Technology Officer for Tropos Networks, where he was responsible for developing Tropos Networks' core intellectual property, including the design and development of the company's wireless networking and routing protocols. Throughout his career Mr. Chari has performed research, published papers and disclosed patents in a variety of areas of mathematics, physics and wireless networking. Among other honors, he was recognized by *MIT Technology Review* magazine in 2005 as one of the Top 35 Innovators under the age of 35. He received his BS in Mathematics and Economics from the California Institute of Technology and an AM in Physics from Harvard University.

2011

GreenWays Series

Leadership for a Clean Energy Future

EnerNex

By Ben Boyd, Vice President Regulatory/Policy and
Doug Houseman, Vice President Technical Innovation

Our final *GreenWays* interview for 2011 is with two key executives from EnerNex, a dynamic and increasingly influential company nestled in the Smoky Mountains of Tennessee that has risen from a modest engineering services firm to national prominence in a relatively short period since its founding in 2003. For readers that might not be that familiar with EnerNex, they have been very active in promoting the use of standards across the Smart Grid landscape from its very beginnings. But among their most notable acccomplishments has been bringing the term 'interoperability' squarely into focus and making it a part of our daily lexicon. Under the aegis of Erich Gunther – the company's chairman, co-founder and CTO as well as Smart Grid Interoperability Panel (SGiP) Administrator – Doug Houseman and Ben Boyd are tasked (respectively) with charting the firm's technological innovations and navigating the constantly changing regulatory and policy waters of an industry in transition. A tall order indeed, but their approaches to these daunting tasks and how those efforts fit into the greater good of our national Smart Grid initiatives are the substance of this interesting discussion. – ***Ed***.

EET&D: EnerNex has been on a pretty fast ramp-up since it's founding in 2003. Maybe we can start off with a quick recap of the company's mission and vision. Ben, would you like to lead off with a brief synopsis?

Boyd: Yes, I'll be happy to do that. EnerNex provides research, engineering and smart grid consulting services, for the power industry. We focus on providing services around the development and application of new and emerging electric power technologies to engineer a cleaner, smarter energy system of the future.

EET&D: Is there any particular dimension of the company that stands out as a defining product, service or other activity, Doug?

Houseman: Well, our primary product is really information, usually packaged as technical reports, measurement data, design recommendations or expert advice. Moreover, our services are often utilized in conjunction with the development of key fundamental technologies, such as the original EPRI IntelliGrid initiative, with which our founders and early employees were integrally involved.

EET&D: So are all of your energies directed to a services model then?

Houseman: No, we do get involved in some product development, such as programmable communicating thermostats and utility consumer gateways. Our business also involves us in the basic research and development of these new technologies, leading to proof of concept implementation projects as well as mainstream deployment products and projects. And more recently we've been at the forefront of technology and integration issues for large-scale wind generation, where we are leading efforts to build tools and models for better understanding the impact of large wind plants on transmission network operations.

EET&D: I think it's fair to say that you've played an important role in bringing the Smart Grid standards and standardization process to an elevated status over the past few years as those initiatives have evolved. Talk a little bit about that, if you would...

Houseman: We have always worked hard to understand the intersection of technical and operational requirements and practice an evolutionary, standards-based approach to solving real-world power systems operational problems, so it's really in our DNA to take a leadership role in that dimension of Smart Grid evolution. We take great pride in the work we do, and our quality is ensured by the dedication, expertise and teamwork of all of our employees.

EET&D: Part of what you have been doing – a large part, I would say, has been toward making interoperablility a practical reality across what were once disparate networks, products and systems. But interoperability is one of those terms that everybody likes to use – and thinks they understand – but in reality, there are probably a lot of different definitions and interpretations out there. So what do you mean by interoperability? Is there a succinct way to describe what that term really means?

Houseman: Yes, I think there is. Interoperability is the ability of two or more networks, systems, devices, applications, or components to communicate and operate together effectively, securely and without significant user intervention. And if you want to dig a little deeper, other more technical factors come into play. For example, communication requires agreement on a physical interface and communication protocols; exchanging meaningful and actionable information requires common definitions of terms and agreed upon responses; and consistent performance requires standards for the reliability, integrity, and security of communications. Ben, anything you'd like to add?

Boyd: I would also say that interoperability also embraces the "plug-and-play" concept – the ability to simply connect functionally dissimilar entities and have them work together seamlessly and support interchangeability, the ability to readily substitute components without corrupting or interrupting safe and reliable operation.

EET&D: Are there any noteworthy developments on that front that may be of interest to our readers?

Houseman: As you mentioned earlier, we place a huge emphasis on interoperability, and interoperable Smart Grid applications have recently moved beyond talk and into real-world technology implementations. For example, by the time this issue is published, we will have provided a first-of-its-kind demonstration of Smart Grid interoperability in a literal show-and-tell of devices and systems in action. Today, Smart Grid vendors are truly "walking the walk" by demonstrating real-world applications of Smart Grid interoperability, albeit with simulated end-to-end utility systems – from the back office to the residential consumer's thermostat.

EET&D: Does that mean we have actually reached the practical implementation stage then?

Houseman: Yes, standards and standardization efforts are now bearing real fruit. Within the next thirty days, a cross-section of industry organizations will be able to demonstrate 15 to 20 examples of emerging, evolving and mature interoperability standards in three categories: 1) Demand Response, including both residential and commercial and industrial (C&I) products and solutions; 2) Interoperability of transmission and distribution devices that monitor, protect and control modern power delivery networks; and, 3) Enhanced cyber security features for electric utility control systems such as SCADA (supervisory control and data acquisition) and distribution management systems. We have a large demonstration making its debut at an upcoming conference that will showcase the state of the art in detail.

EET&D: Let's switch topics here to the customer side of the business; something that has been getting quite a lot of attention lately. Ben, in your opinion, are consumer attitudes about the grid changing, and of so, what do you feel is driving those changes?

Boyd: Let's face it, Mike. The electric power grid we have all known and loved for over a hundred years is undergoing a revolution, even though on one level it continues to be part of an ongoing technological *evolution*. Clearly it's some of both, but one thing is certain: the consumer is rising to the level of equal partner in the new equation of the 21st century,

something that will not likely change anytime soon, if ever.

EET&D: I certainly don't disagree that the voice of consumers is definitely being heard louder than ever before, but speaking both as a former regulator[1] and now a consultant, to what do you attribute that trend?

Boyd: For one thing, consumers are now being allowed to voice their concerns in certain venues where they were not heard before. This cultural shift engages all players instead of just the utility representative and the regulator as was often the case in the past. So called creative collaboration is made up of consumer advocates, policymakers, regulators, utilities, technology companies, service providers, and the media. And why not? The electric grid affects everybody. Issues such as health concerns from radio waves, consumer data privacy and access, and dynamic pricing impact on revenue-challenged consumers demand that those directly impacted and those in a position to impact have a seat together at the decision-making table before the regulator must make a decision, if at all possible.

EET&D: What would you say are some of the challenges associated with this dramatically heightened level of consumer engagement?

Boyd: There are many challenges indeed. I'm sure we won't be able to cover them all here, but let me summarize a few of the most important ones…

First of all, the Smart Grid message has not been focused on consumer benefits

– that is, highlighting and showcasing benefits that would be particularly meaningful and very tangible in the eyes of consumers. For example, utility bills typically represent a relatively small percentage of monthly expenses for a large portion of the population. So, if the average electricity bill is $60 per month, a savings of 10%, or $6, on the bill is not something for most consumers to get excited about. Today, for the most part at least, they are happy with the status quo because they have not been educated as to the reasons for change. As energy costs increase – as they are predicted to do – then those attitudes will likely change and the questions to the regulators will increase.

Second, the Smart Grid movement has very little inertia upon which to build. Again, for the most part, there has been little relationship – or at least not a satisfactory one – between the utility and the customer, although it is improving. To the degree that there has been dialog with utilities regarding Smart Grid, it has tended to be mostly acrimonious. The regulatory process tends to be adversarial, with advocates on every side arguing for positions ostensibly in support of their special interests. This simply cannot continue since sooner or later everyone will have to realize that like it or not, we're all in this together.

[1] Ben Boyd is a former member of the Texas Public Utility Commission, which regulated rates before Texas became restructured. He also worked for the Texas Railroad Commission, which regulates natural gas rates.

Finally, and following from the previous point, consumers do not typically trust their utility. Again, that is something that will likely change as previously monopolistic utilities, now facing potential competition on several fronts and on various levels, will have to learn a new kind of customer service, which is in many ways in stark contrast to what they had been accustomed to in the past.

EET&D: How does that change to collaborative thinking begin?

Boyd: Since 2008, the idea of a creative collaborative has become popular enough for industry regulators to order the local utilities to pay for this foundational planning exercise. A premier example is the Illinois Statewide Smart Grid Collaborative, ordered by the Illinois Commerce Commission as part of an order resulting from a smart grid cost recovery filing by Commonwealth Edison (ComEd), headquartered in Chicago. The stated goal of that collaborative was to ensure that consumers are the primary beneficiaries of smart grid deployments in Illinois.

The Illinois Collaborative addressed a wide range of stakeholder smart grid issues, including how regulators should evaluate proposed smart grid investments, technical issues – including security, standards, and interoperability – and consumer issues (e.g., data privacy/access, consumer education, etc.). A wide range of stakeholders participated in the Illinois Collaborative.In addition to the investor-owned utilities and Commission staff, participants included consumer advocates, municipal governments, environmental groups, retail electric suppliers, RTOs, and vendors. What better way exists to bring all stakeholders to the table?

In this case, EnerNex was very fortunate to be named the facilitator for the Collaborative. Through this process we learned that, in spite of the many differences in stakeholder concerns and perspectives, much common ground exists and that collaborative planning can result in a smarter Smart Grid plan or roadmap.

EET&D: What were some of the primary benefits gained through this process?

Boyd: Certainly a better understanding of Smart Grid technologies among stakeholders provided a more realistic view of potential benefits, costs, and risks. It also afforded the participants a much clearer picture of consumer-related Smart Grid issues as well as a clarification of the various, and sometimes divergent, stakeholder views/positions on these issues.

EET&D: Were there any tangible outcomes from the Illinois Collaborative effort?

Boyd: Yes, absolutely. It produced a range of specific consensus recommendations from the stakeholder group on many issues for the Commission to consider. It also narrowed the issues on which the Commission must focus its future efforts, reduced the potential for future litigation, and established a dialog among stakeholders on Smart Grid issues that will likely continue.

But perhaps more importantly, the idea of changing to a culture of listening and collaboration is alive and well at the Illinois Commerce Commission. I'm personally aware that regulatory commissions in Arkansas, Colorado, Hawaii, Michigan, Minnesota, New York, Oregon, Rhode Island, and Vermont have expressed interest in learning more or are in the process of taking on this approach to planning for the Smart Grid.

Also, it would be inaccurate to omit California and Texas from the list because of their tremendous head start with smart metering; however, since I have not talked to their Commissioners directly about this approach, I can't speak with the same level of certainty. What I can say is that the value of a collaborative approach can be stated in one phrase: Consumers become partners in the process instead of victims. Trust is more likely to evolve as the process unfolds. Old attitudes of "us versus them" can dissipate, and the potential for a Smart Grid that is consumer-friendly and consumer-valued can be vastly enhanced through this type of process. ■

LightsOn

Advanced Distribution Management Can Bridge the Chasm in the Road to Grid Modernization

By Rodger Smith, Senior Vice President and General Manager, Oracle Tax & Utilities Global Business Unit

By focusing on individual electricity issues and addressing them with Advanced Distribution Management, utilities can help their communities advance incrementally toward grid modernization.

The U.S. is experiencing a period of reflection and re-evaluation in our evolution to the smart grid.

Think back to the projections of 2005. Most utilities planning to launch smart grid projects saw smart metering and new residential pricing options as a necessary first step. Analysts anticipated a year or two of utility pilot programs, rapid deployment of smart meters – perhaps an 89 percent market penetration in North American by 2012[1] – and a continent-wide roll-out of residential and commercial dynamic pricing programs for electricity.

That is not, of course, what happened. Today, most utilities either have not started or are still in the pilot stage of smart metering programs. The number of pricing programs reliant on smart meters is growing very modestly, according to the Federal Energy Regulatory Commission (FERC); in the case of time-of-use pricing, program numbers are actually expected to decline.[2]

	Number of Programs*		
Program Type	2010	2011-2012	2013-2015
Direct Load Control	253	324	563
Critical Peak Pricing with Controls	13	19	22
Time-of-Use Pricing	219	205	193
Critical Peak Pricing	42	62	68
Real-Time Pricing	24	30	29
Peak Time Rebate	13	27	27

FERC foresees only modest growth in pricing programs that rely on advanced meters. In the case of time-of-use pricing, the number of programs appears likely to decline.

*Numerical Data from *Demand Response and Advanced Metering*, Federal Energy Regulatory Commission, 2010

Similarly, smart meter penetration has been slower than projected. By the end of 2010, fewer than 9 percent of U.S. customers had smart meters. Projections for the end of 2012 hover between 25 and 38 percent – and even that may prove to be too high.

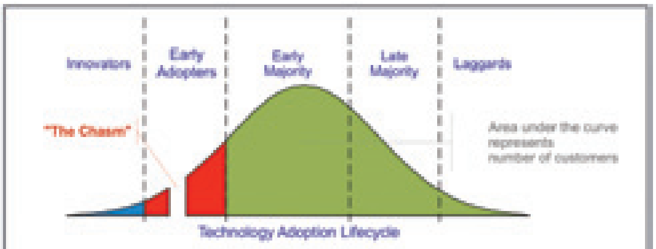
A Standard Stop on the Road to Technology Adoption

Today's reassessment of smart grid plans is only to be expected. Hesitation is a common characteristic of the way individuals and societies undertake almost any major change.

Initially there's an inspiring idea, an outlined goal, a new product. Participants eagerly sign on. Then comes a period of pushback. Some see the goal or product as too costly. Others believe it will threaten specific groups or time-tested ways of doing things. Others just want to think more about the issue, take more time, and gather more facts.

1 Datamonitor, 2007. Reported at http://*www.energybusinessreports.com/articles/view.asp?id=438* and elsewhere.
2 2010 Assessment of Demand Response and Advanced Metering, http://*energy.gov/sites/prod/files/oeprod/DocumentsandMedia/FERC_Assessment_of_Demand_Response_and_Advance_Metering.pdf*

Not all pushback is well founded. The charge that smart meters cause negative health effects, for instance, appears to be scientifically invalid. Frequently, however, those pushing back make points that resonate widely. The Governor of Illinois and the Maryland Public Service Commission are not the only smart grid stakeholders who see value in more review, more ratepayer protections, and more consumer involvement.



The Chasm in Geoffrey A. Moore's Technology Adoption Lifecycle illustrates the reassessment that invariably occurs on the road to technology adoption.

Source: "Crossing the Chasm, Harper, 1991. Licensed under the Creative Commons Attribution 3.0 unported license, 2009.

Bridging the Gap

This period of reassessment has become a standard feature of technology adoption. Even when we anticipate it, however, the gap in forward movement invariably feels like a setback to those who see the value of the goal. Fortunately, leaders can bridge what Geoffrey Moore refers to as "The Chasm" in technology adoption by listening to opponents' arguments and modifying plans accordingly. That re-alignment in smart grid planning is now taking place at utilities across the country.

A first step in the reassessment of the smart grid evolution has been a change in rhetoric. To many, the term "smart grid" has come to connote a change that is occurring too rapidly and without enough thought. To alter perceptions, many utilities are replacing the goal-oriented "smart grid" phrase with terms that better connote thoughtful process, such as "grid modernization."

A second step toward restarting the future has been to shelve rapid deployment of new consumer pricing programs. In 2005, rapid deployment appeared necessary as a way to cope with constantly rising electricity demand. But falling demand resulting from global recession has dramatically curtailed the need for dynamic pricing as a path to conservation. While no one would have wished for today's faltering economic conditions, they have given both utilities and consumers the opportunity to step back from implementation of pricing proposals for which consumers were simply not prepared.

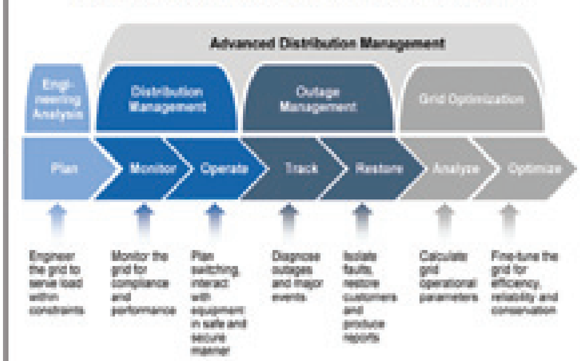
The Role of Advanced Distribution Management

A third step utilities are taking to bridge the grid modernization "chasm" is to broaden the scope of the project and to reorder the steps in the process. They no longer describe the goal as creating a platform for vaguely defined "new services" or "21st Century business processes." Instead, they are increasingly defining modernization projects as a series of optional, independent steps, each focused on solving a definable problem, and each delivering tangible benefits.

Often, these projects resonate best with stakeholders when they focus on utility basics like improving reliability and efficiency. And the technology increasingly proposed to solve the problems is not the smart meter but instead new class of software known as Advanced Distribution Management (ADM).

The emergence of ADM represents a different approach to change – a commitment to phase and stage solutions to a near-term, definable set of grid objectives and customer benefits.

Product Contributions Across the Grid Life Cycle



Source: Gartner, Inc., Market Definition: Advanced Distribution Management System Products, Randy Rhodes and Zarko Sumic, 14 December 2010.

ADM is an umbrella name for a set of software systems that exercise full control over existing and new grid hardware – sensors, nodes, embedded devices, and advanced meters. Viewed as a whole, ADM:

- Increases "situational awareness" by providing a full 360-degree view of the grid for management, operations, crews, service representatives, and customers.
- Increases grid efficiency, reliability, and security.
- Defers the need for new grid construction by safely taking existing assets to their physical limits though improved monitoring and asset analytics.
- Responds to new customer technology challenges like electric vehicle adoption and efficient use of 'beyond-the-meter' customer generation from intermittent renewables (e.g., solar rooftops) – including operational and forecast modeling.
- Maximizes use of intermittent, renewable power produced both locally and remotely.

It is helpful, however, to view ADM not in the aggregate, but instead as a set of targeted solutions, including:

- Power flow and suggested switching objectives.
- Volt/Var optimization that will also leverage customer voltage violations from AMI investments.
- Feeder Load Management that not only forecasts when feeder capacity constraints could arise, but also suggests optimal switching plans to avoid it altogether.

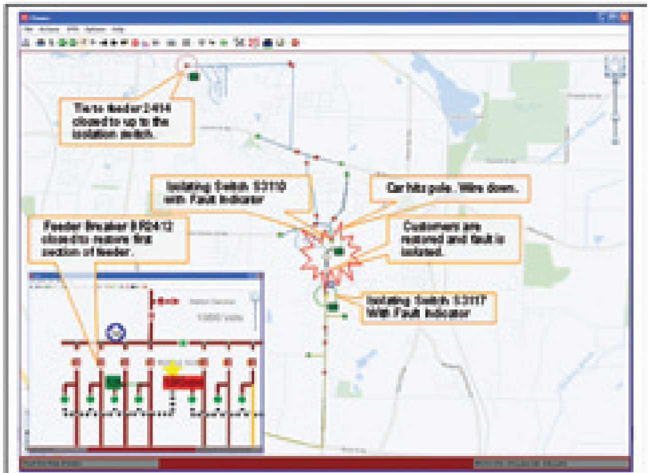
- Incorporation of increasingly diverse supply (for instance, from intermittent renewables and small, distributed generation sources).
- Fault location, isolation, and service restoration (FLISR).
- Conservation voltage reduction (CVR).
- State estimation.
- Support for reducing peak demand and recharging electric vehicles.
- Distributed grid management through microgrids that:
- Support distributed generation and distribution optimization in a remote environment.
- Operate under the overarching authority of a centralized ADM system, as required for safe and reliable operations.

These solutions – deployed individually or in groups of two or three – can solve a wide range of utility, customer, and community issues.

Issue: Expectations for Reliability are Changing **Solution**: ADM's Fault Location, Isolation, and Service Restoration (FLISR)

North American utilities' reliability records are generally outstanding. But as utilities are beginning to discover – much to their chagrin – yesterday's top SAIFI and CAIDI numbers may not satisfy today's consumer.

The reason is change in lifestyle. Yesterday, "downtown" reliability during the workweek generally took priority over neighborhood or suburban reliability. Multiple alternative sources automatic fail-over switchgear kept office workers productively at their desks. Customers noticed short weekday neighborhood outages only when blinking clocks indicated that homes had lost electricity while they were gone.



FLISR can significantly shorten outages for many customers and turn the experience into a "non-event."

Today, increasing numbers of employees work full- or part-time from home. They notice short neighborhood outages because they suddenly lose use of their computer peripherals. Outage times that drop Internet connections and exceed laptop batteries lead to unhappy customers' seeking the nearest operating Starbucks for power and Internet access relief.

At-home workers are not the only change among residential customers. Today's communities are highly sensitive to tree trimming. Yesterday, complaints focused on aesthetics. Today, utilities face far stronger environmental attitudes and stringent local regulations aimed at preserving tree canopies.

ADM is one way to address expectations for higher levels of reliability despite restrictions on tree trimming. Fault location, isolation, and service restoration (FLISR) and Fault Location Analysis can turn outages into momentaries by isolating faults and pinpointing outage locations before crews arrive, identifying customers who can be served by still-operating lines, and reconfiguring the network to serve them while restoration proceeds.

Issue: Incorporate More Renewables
Solution: ADM's Detailed Network Model

Despite recent reductions in electricity demand and the vast supply increase in more environmentally friendly natural gas, green mandates remain on the books in many states. And they are likely to remain there, challenging utilities to maximize their use of locally sourced renewables.

Today, the introduction of energy resources at the electric distribution level – for instance, power generated from solar rooftops – challenges many operational systems when they need to accept unconstrained levels of alternative energy resources. Today's systems often lack the detailed models that can provide an accurate accounting of the energy injections and flow of power across the distribution network in addition to real-time, near-term forecasts that anchor a complete assessment of the nature of power delivery in the distribution network.

To integrate intermittent renewables successfully, network models must expand to include:

- Circuit models showing the distribution lines connected to source nodes, network equipment, grid devices, etc. These are usually derived from a GIS or other circuit mapping system source.
- Customer connectivity through secondary services or data linkage to service transformers.
- Conductor and cable type, including overhead line construction type and underground cable spacing to calculate engineering parameters such as line impedances and thermal loading limits that add unbalanced 3-phase impedance and capacity characteristics to the model. This operates the real-time unbalanced load-flow for system optimization.
- Engineering and forecasting models of customer loads, intermittent renewable resources, electricity storage, and their network connections to the dynamic models.
- Customer meters and beyond-the-meter resources (e.g., backup generation, electricity storage characteristics, electric vehicle charging profiles, demand response capability).

ADM solutions' enhanced models proactively identify probable locations and durations of intermittent supply drops; then, identify alternate sources of supplies. If the need materializes, ADM solutions can orchestrate alternative generation, demand response options, and storage supplies to accommodate both short-and long-duration supply drops.

Once in place the detailed network models, vital to use of intermittent renewables can also underpin a wide variety of additional ADM solutions that increase grid efficiency, monitor and adjust voltage, and heighten service quality.

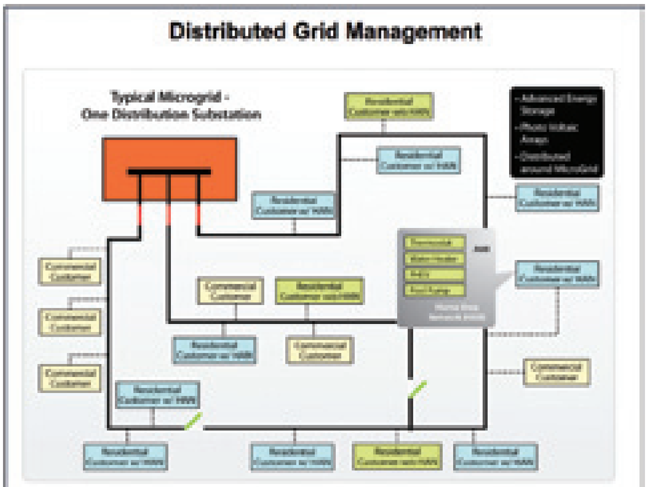
Issue: Recharge Electric Vehicles
Solution: ADM's Microgrids

North America anticipates a slower adoption of electric vehicles (EVs) than do more densely populated countries in Europe and Asia. Per capita infrastructure costs, driving distances, and the availability of locally produced fossil fuels will likely retard EV growth in North America. Some utilities, however, will be challenged to make fast, off-peak refueling available in specific cities or specific neighborhoods where two-income households, private parking spaces, and environmental commitments produce concentrations of early EV adopters.

Handling this new demand will increase the need for ADM solutions. The same enhanced modeling required for handling of intermittent renewables will be a necessary component. So will equipment upgrades and control strategies that permit utilities to ensure that EVs are all appropriately recharged at some point during an overnight refueling cycle.

Additionally, distributed grid management and its associated microgrids can play a strong role. Microgrids solve one or a combination of problems that are difficult to handle on a large scale but manageable when confined to a small geographic area. They:

- **Integrate power from small, distributed generation facilities, such as rooftop solar, into the grid.** Today's net-metered generation – frequently consisting of a few kilowatt hours delivered on an unpredictable schedule – is largely useless within the context of a large utility geared to handling megawatts of power for tens of thousands of customers simultaneously. Microgrid software, in contrast, can be fine-tuned to the potential production from local sources and supplemented with weather and other information that brings considerable predictability to "non-dispatchable" generation from variable renewables.



Customers can readily picture their own neighborhoods on simplified diagrams of microgrids.

- **Charge non-fleet electric vehicles.** Today's utility aims to accommodate, without brown- or blackouts, any amount of demand at any time. Using this model to accommodate electric vehicles would likely require a massive increase in infrastructure and generation. A microgrid, however, could use local, variable generation to charge vehicle batteries intermittently, as power was available. Such a model could, of course, be managed on a large, centralized basis, but it is likely to be far easier to delegate distributed control and optimization on a smaller scale.
- **Incorporate electricity storage from batteries and other storage devices.** Microgrids could use excess local generation to charge these resources in off-peak periods, where low-priced energy is readily available, and draw from them at peak-demand periods when power runs short, and spot prices are highest, thus limiting the amount of generation they require from central generators. Microgrids can manage storage (charge-discharge algorithms) in order to provide an energy arbitrage benefit that more than offsets the round-trip efficiency losses of the storage technology.
- **Assure safety and reliability with the overarching authority of centralized ADM to provide real-time dispatcher interaction to the distributed microgrid processes.**

Presented as an abstract concept, microgrids frequently fail to garner consumer interest, much less support. Presented as an efficient recharging strategy in neighborhoods with large EV concentrations, they attract attention. And described in terms of values like independence, local control, and energy security, microgrids can become an exciting community project.

A Grid that Meets Customer Needs

Utilities well understand the need for an improved grid. But the concept has proven too large and abstract for many customers to swallow. And the decision to launch smart grid projects with advanced meters – a move many thought consumers would welcome – has instead created backlash.

As a result, an increasing number of utilities are starting grid modernization programs from the other end – by implementing advanced distribution network solutions that, in the aggregate, dramatically increase efficiency and prepare the grid for a resumed period of growth. Winning support for these ADM solutions may be faster when utilities portray the solutions – completely accurately – in terms of the customer and community issues they address rather than in the engineering terms most network operators find compelling.

ADM solutions can serve as a bridge between engineering reality and emerging customer needs. They can permit network engineers to respond clearly and directly to customer-generated requirements. They can help utilities place the investment and maintenance costs of meeting those requirements in the context of other utility business applications. Today, ADM solutions are helping to break down the walls between a utility's operational and business departments, creating a utility increasingly fine-tuned to its customers. ■

Rodger E. Smith is senior vice president and general manager for the Oracle Tax and Utilities Global Business Unit. In this position, he leads the global business unit's solution groups, strategic planning, product development, sales, service, and support.

Mr. Smith is the former president of Enterprise Management Solutions (EMS), the management consulting division of Black & Veatch. In this position, he grew the division into one of the largest management consulting organizations specializing in energy and water. He previously held positions with PricewaterhouseCoopers and Southern Company, the latter one of the largest electric utilities in the United States.

Zones of Protection: A Substation Security Strategy

By Robert McFetridge, Strategic Account Manager, GarrettCom, Inc.

Ethernet and the IP protocol bring tremendous advantages to power utilities – and in particular substations – through international standardization. This keeps the cost of equipment low, ensures interconnectivity among equipment from multiple vendors, and provides future-proofing and backward compatibility – all of which are important considerations in an environment where equipment is expected to last for 30 years or more. Nonetheless, current estimates are that only about 50 percent of power utility substations in North America today are using integrated IP communications strategies to get data from the Smart Grid – and data generated in the substation itself – to the central office. This must and will change.

Accessing, transporting and managing the massive amounts of data being collected in today's power utilities requires sophisticated technology. In addition, in an increasingly insecure world, Ethernet provides a rich set of security protocols and applications that can help keep substations secure. "Zones of protection" is one strategy that can be used to provide the level of security demanded today.

Protective relay engineers keep utility grids and equipment safe from faults and system unbalances by dividing the grid into zones, each with a unique protection scheme. Overlapping zones provide backup protection. This same strategy can be used to provide communications zones of protection to address the rich information that is collected in the course of operation today. Ethernet is the best protocol for supporting that strategy.

Figure 1 is a one-line of a typical substation depicting the zones of protection within the substation. Notice that zones overlap each other to provide backup protection should a primary zone fail.

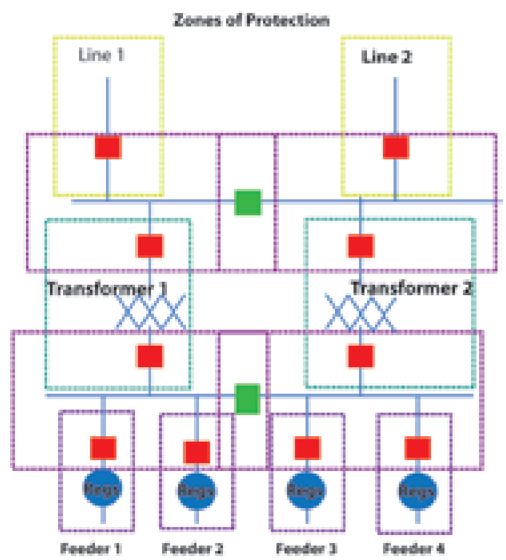


Figure 1: Zones of protection for a substation

As the figure above shows, there is a zone of protection covering from each feeder breaker (Blue dotted lines), a zone covering each low-side bus, a zone covering each transformer (Green dotted lines), a zone covering each high-side bus and a zone covering each incoming transmission Line (Yellow Dotted lines). The Transformer Zone acts as a primary zone for faults internal to the transformer and a backup zone to faults on the low-side bus and feeders.

IEDs – The Information Enabler

Intelligent Electronic Devices (IEDs) collect valuable information such as fault location, relay targets, and customer usage in increasingly fine granularity to support Smart Grid. Protective relays, meters, remote terminal units, LTC/regulator controllers, and predictive maintenance equipment are becoming rich sources of data that can be made readily available to remote users. This new information requires increased communications bandwidth and a secure strategy for transporting the information to its destination points throughout the utility, which can be best provided by an Ethernet-based architecture.

Ethernet – The Information Transport

Typical concerns with moving to Ethernet include cost of replacement of existing equipment, and, more to the point of this article, the challenge of providing security over Ethernet.

Ethernet is a more open protocol than the traditional closed serial strategies, but as StuxNet proved in 2010, even unconnected systems can fall victim to the good old "Adidas network" as employees intentionally or unintentionally expose systems to malicious attacks. Ethernet provides the flexibility and rich supporting protocols and applications that enable a utility to create powerful zones of protection for both physical and cyber assets

Ethernet offers three major advantages for substations: bandwidth, simultaneous access, and support for multiple protocols.

Bandwidth:

With current IEDs supporting Ethernet technologies, 100MB is a typical bandwidth, and it is several orders of magnitude faster than serial ports. Speeds of 1GB and 10GB are on the horizon. Ethernet allows the large amounts of data, such as setting files and fault records, to flow across the network without slowing down time critical information such as SCADA data. Increased bandwidth also enables new applications such as inter-relay protection schemes over communications networks.

Simultaneous access:

Ethernet allows multiple users to access the same IED at the same time; e.g., a user can access an IED for viewing and changing of settings or uploading historical data at the same time SCADA is polling the IED for real-time data. Serial protocols have a master/slave relationship, with one master that can poll only one slave device at a time. When multiple masters need to access the same slave, it is a complex process. More importantly, with Ethernet, it is possible for users to access this data remotely, saving additional time and expense.

Multiple protocols:

Ethernet allows multiple protocols to run on the same network at the same time; the user above can be using vendor-supplied software and protocol at the same time SCADA is accessing the same IED with a different protocol. Serial links cannot support multiple protocols simultaneously; each IED responds only to one pre-selected protocol. For instance, an IED may use DNP 3.0 for SCADA information but may use Modbus to change settings or download historical data.

Security in the Ethernet Era

When multiple users simultaneously access devices from outside the substation, the network is open to security challenges that would not be a consideration with serial communications. However, as mentioned previously, demand for rich and timely data, and demand to reduce costs through activities such as remote access, is driving Ethernet adoption, and security solutions are available.

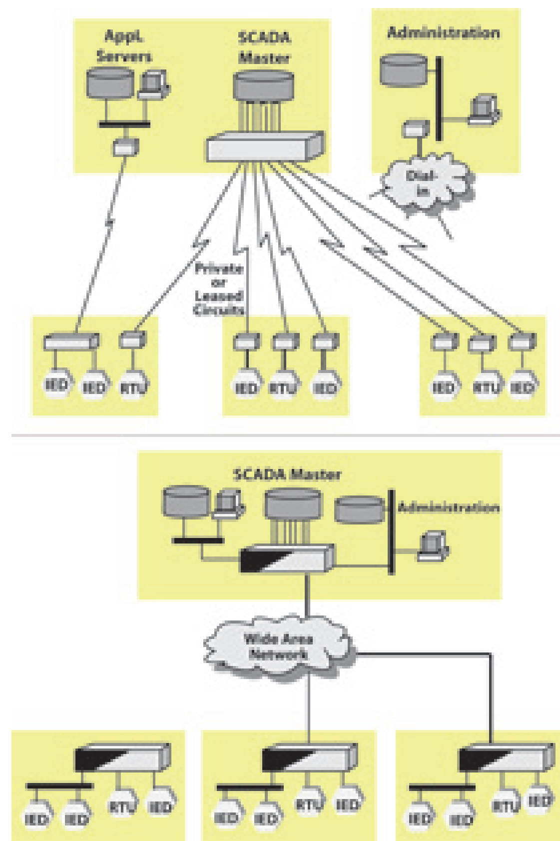


Figure 2: Contrasting a serial substation with a hybrid Ethernet/ serial substation architecture

In the above diagram, a pure serial substation and a hybrid Ethernet/serial substation architecture are contrasted. A pure serial substation has certain levels of protection in the use of dial up modems, while a hybrid substation architecture simplifies communication and increases bandwidth among various parts of the utility. As this section demonstrates, the security capabilities of Ethernet reduce the risk while providing increased benefits in terms of simplicity and increased bandwidth.

In a hybrid or full Ethernet architecture, multiple levels of protection are required: protection against unauthorized users (authentication); protection against authorized network users accessing devices or control for which they are not authorized (authorization); and protection against snooping and hacking.

Authentication

Firewalls, typically contained in routers, are a first zone of protection. Their job is to keep unauthorized outsiders from accessing the networking within the substation where the IEDs reside. Authorized addresses are managed from a common firewall file and pushed down to all routers and switches. Remote users must be properly authenticated when logging into a router or switch using IEEE-supported security protocols such as RADIUS and TACACS+. Using a secure, encrypted tunnel to process authentication (passwords), settings and configuration files, is critical, and replacing Telnet with SSL will support that process.

In addition, routers and switches can limit physical connections to the network by blocking ports that are not assigned or disconnected without authorization, and by verifying IP addresses and MAC addresses authorized to access a port. If an unauthorized user is detected, the router or switch can turn off the port and send an alarm to the network administrator.

Authorization

A password protection zone keeps users from accessing devices where they have no privileges. NERC CIPs require IED passwords to be a minimum of eight characters, with a combination of numbers, letters and other characters.

In a system with thousands of IEDs and multiple levels of passwords within each IED, it is impractical to manage passwords manually. Technology exists that allows a server on the network to manage all passwords. An extra level of protection is available when the server not only authenticates a user, but also performs logging into authorized IEDs. In this way, the users never need to know their actual passwords. Subnet Solutions and other vendors provide password management systems that allow, servers to manage and change passwords on a periodic basis and also to disallow access to personnel who have changed functions or left the utility.

Snooping and Hacking

VLANs and VPNs offer virtual protection zones that suppress snooping and hacking. Virtual networks (VLANs) segregate IEDs connected to the same physical switches from each other for protection. To pass data between VLANs, users must goes through a Layer 3 device such as a router. These Layer 3 devices contain the firewalls to limit access from one VLAN to another. Using separate VLANs for remote access to protective relays, and placing a firewall between the remote user and the VLAN that recognizes only specific device addresses adds to security.

If a user is allowed to access certain devices on the network (e.g., regulator controls but not protective relays), these devices should be segregated onto separate VLANs. Layer 4 Ports (used by UDP or TCP) can also limit user activity. For example, a user could poll a protective relay for SCADA data using DNP 3.0, but not be able to Telnet into the protective relay to change settings.

Virtual Private Networks (VPNs) can be set up between remote users and field devices so that the user is authenticated and all data is encrypted. Sensitive data such as passwords, settings and fault data are encrypted, removing the possibility that it could be deciphered by another user on the network (snooping).

Ethernet and Physical Zones of Protection

Physical security within the substation provides an additional zone of protection through devices such as card readers installed on control house doors and outdoor cabinets such as transformer cabinets. Security cameras monitor substation access and watch over sensitive areas to guard against unauthorized penetration, copper theft and other attacks. Security data may be logged onto a substation server and also sent through the network to a central monitoring area for viewing in real-time or for archiving. When configuring communications transport for physical security data, it is important that Quality of Service (QoS) levels are set that ensure that data will be received in a timely manner.

Getting to a Secure Modern Substation

The secure modern substation requires a different approach to substation communications architecture. The demand for both security and for timely data will necessitate a series of interrelated, but not necessarily interconnected LANs, in an overall interconnection strategy connecting both downstream devices and upstream data centers, some of which have been described in this article. This architecture addresses both security and network integrity, and it must provide a migration path from serial networks and from lower bandwidth interconnection technologies.

Because many of the IEDs that support only serial communications are relatively newly installed and can be expected to perform their primary functions for an additional decade or more, utilities, of course, want to maximize their investments. They are not looking to replace these devices prematurely. Nonetheless, these devices have several limitations that must be addressed.

Integrating Serial Connectivity into the Zones of Protection

When integrating serial IEDs into an Ethernet-based substation communications architecture, it is important to consider password security and secure connectivity as integral to the overall network.

First, many of the older IEDs supported only simple 4-character passwords. The new password management systems, with their tiered levels of password support, can map the serial IED's password into a more complex 8-character password that will meet CIP requirements.

Second, there are two fundamental approaches to integrating serial devices securely onto the overall network: gateways and terminal servers.

A gateway can be inserted between the serial IEDs and the network that will poll the IEDs via serial communications and collect the data into a common database that can be accessed over the Ethernet network. Gateways are typically hardened computers that act as small SCADA masters, polling IEDs using various protocols and converting and combining the data into a common database that can be accessed from the main SCADA system or by remote users.

Figure 3: Typical Hybrid Substation Automation LAN with connection to WAN

Gateways can be expensive and time consuming as each gateway must have a separate database that needs to be programmed and maintained.

Terminal servers, on the other hand, perform a basic Ethernet-to-serial conversion so the end users can access the IEDs as if there were connected directly to the network, and thus eliminate the need for additional databases. Some terminal servers also support secure communications such as SSL and RADIUS to maintain the ESP.

Summary

The performance, flexibility and data management capabilities of Ethernet-based make a strong argument for transitioning to Ethernet-only solutions. However, practically speaking, hybrid transitional architectures will be standard operating procedure for the foreseeable future.

While security concerns are real, they can be easily overcome by deploying proper zones of protection. These zones start in the network equipment and access to upstream control centers and users, and also propagate through password servers to the downstream IEDs.

The costs of fiber-based connectivity have decreased, making fiber an affordable alternative to telephone lines for connectivity with the central office. Security protocols and strategies have advanced to address concerns associated with cyber attacks. Today, networks, engineered properly through the use of today's security and connectivity technologies, can provide the required functionality and security without disregarding the existing investments in serial devices. ■

ABOUT THE AUTHOR

Robert (Bob) McFetridge, Strategic Account Manager for GarrettCom, Inc., has worked in the utility industry for more than 25 years, including seven years at two large investor-owned utilities in the Southeast. His experience includes protective relays, SCADA, substation automation, distribution automation and Volt/VAR SmartGrid projects.

SCADA Security: New Standards Protecting Old Technology

By Scott Howard, Representative
Trusted Network Connect (TNC) Work Group, Trusted Computing Group (TCG)

Supervisory Control and Data Acquisition (SCADA) systems have undergone a technological revolution over the past 20 years that has been nothing short of mind-boggling. Inexpensive, high-performance network connectivity combined with innovative software solutions on PC platforms have driven huge improvements in service quality as well as cost reductions. However, at the same time, the integration of these new technologies can subject existing SCADA systems to new stresses and threat sources that they were never designed to handle. Many legacy devices and communication protocols such as Modbus and OPC, designed in an era of isolated standalone systems, have now been force-fit into network environments where authentication and access control issues can result in serious security vulnerabilities.

Even efforts to protect the networks can lead to unintended consequences. Regulations such as the Critical Infrastructure Protection (CIP) standards from the North American Electric Reliability Corporation (NERC) drive integration, as electric ISOs seek access to production data in real-time to demonstrate compliance. Ironically, the pursuit of security itself can lead to exposure! Protective measures such as centralizing access control to minimize tampering, or extending closed circuit TV (CCTV) monitoring or voice over Internet (VoIP) to remote stations, require increased accessibility.

Looking into the future, what happens when smart meters are integrated into the grid, offering the capability to not only monitor but also remotely disconnect customer facilities? How can we be certain that access to these devices is available only to authorized parties? Cyber security is an issue that will not go away, but will only increase in importance over time.

Challenges of Interconnectivity

Clearly, interconnectivity is the wave of the future – but many control system components were conceived in the past. Control devices, and the PCs that manage them, are very vulnerable – not only to malicious attacks using malformed network data, but in many cases even to high levels of correctly-formed network traffic. PLCs and remote terminal units (RTUs) are typically optimized for high-performance real-time I/O, rather than for robust networking. In addition, SCADA systems run continuously for weeks or months at a time – disabling some of these systems even for only a few minutes can result in significant financial, service or even safety impacts. As a result, the PCs in these networks are often not up to date with security patches or anti-virus definitions.

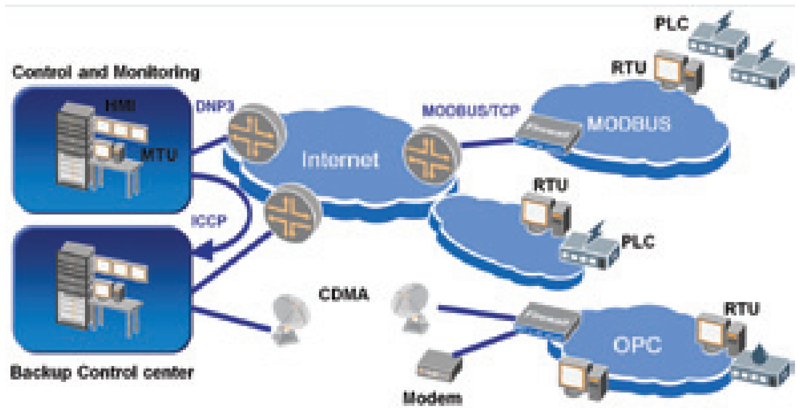


Figure 1: Relationships between common components of a SCADA network

In the early days, SCADA systems were implemented as very simple 'islands' of automation, but they have steadily grown in size and complexity over time. As a result, many SCADA networks are poorly segmented, with little or no separation between subsystems or even across physical locations. If a problem occurs in one area of the network, it can spread rapidly to other unrelated systems elsewhere in the network. Poor segmentation also makes it very difficult to locate the origin of a problem and resolve it at the source.

The third common issue is the existence of multiple paths of entry into these networks. Many control network managers will swear up and down that their control systems are not connected to the enterprise network or the Internet, but authorized penetration testing often shows otherwise. Here is what the U.S. Department of Homeland Security has found:

"In our experience in conducting hundreds of vulnerability assessments in the private sector, in no case have we ever found the operations network, the SCADA system or energy management system separated from the enterprise network. On average, we see eleven direct connections between those networks. In some extreme cases, we have identified up to 250 connections between the actual producing network and the enterprise network."

In addition, there are often other transient paths of entry that don't even show up on a network diagram: VPN connections, laptops or even USB memory sticks traveling in and out of the plant can easily carry viruses right into the heart of the SCADA network.

Theoretical vulnerabilities lead to real-world incidents with far-reaching consequences including loss of productivity, revenue, and even loss of life. In 2003, the Davis-Besse nuclear power plant in Oak Harbor, Ohio, was infected with the MS SQL 'Slammer' worm that originated in a network connection from a contractor, resulting in the plant process computer being inaccessible for over 6 hours. Then, in August of 2006, the failure of two water recirculation pumps due to excessive traffic on the control system network forced the manual shutdown of the reactor at the Browns Ferry Nuclear Plant. And a year later, the National Transportation Safety Board found that an unresponsive SCADA system at Olympic Pipe Line Company contributed to a pipeline rupture and subsequent fire that killed three young men in Bellingham, WA. There are also many less serious incidents that have gone unreported in the press.

Taking Control of the Network

Most IT managers have significant experience addressing cyber security issues in enterprise networks, so why can't managers of control and SCADA networks simply apply the same technologies in their systems? Control systems have unique requirements that until recently have not been addressed by available security solutions. These requirements include harsh physical and electrical environments; support for the unique communication protocols that are common in control networks; and the ability to install, configure and test these security solutions in a 'live' operating network without putting the plant at risk. As a result, most SCADA and control networks today run with little or no security measures in place.

The first step in securing a network is to document a clear security policy for network access. This policy will typically establish some criteria to allow initial access to the network, as well as further criteria that define acceptable endpoint behavior after access has been granted.

A typical security access policy might look like this:

- Access to the network is granted only to certain authorized users – the identity of each PC user must be validated.
- Access is granted to endpoints (PC and otherwise) that can demonstrate that they are 'healthy' and will not present a risk to the network. For example, PCs must be up to date with their security patches, have approved anti-virus software installed, etc.
- Once granted access, endpoints must continue to demonstrate behavior that is appropriate to their assigned role. For example, a laser printer should not be creating connections to an RTU– if it does so, then it is probably not really a laser printer!

Once the security policy has been defined, a set of tools and procedures can be put in place to implement the policy.

A wide range of products is available to address network security for enterprise and IT networks – for example, the series of UAC (Unified Access Control) appliances from Juniper Networks. Other products such as Tofino Security from Byres Security make it simple to adapt existing IT security technologies and practices to the unique requirements of SCADA and control networks.

The Next Generation of Network Access Control

Current solutions work well and can demonstrate measureable improvements in network security. But the competitive and regulatory pressures that got us to this point are not going away. If anything, these pressures will only increase over time. SCADA networks will increase in size from dozens or hundreds of devices today to thousands or even millions of devices, but staffing levels almost certainly will not increase proportionately. New tools and technologies will be required to keep pace with the growth and evolution of these systems. New standards will be required so products from multiple vendors can interoperate seamlessly. And these systems must be flexible so customers can easily configure them to automate their unique security policies and procedures.

Open Standards for Network Security

Trusted Network Connect (TNC) is a work group of the Trusted Computing Group (TCG), an industry standards organization focused on strong security through trusted computing. TNC is completely vendor-neutral; the full set of TNC specifications is freely available for anyone to implement, and TNC-based products have been shipping for over five years.

TNC standards provide a flexible architecture and open interfaces that allow interrogation of an endpoint to determine its integrity and compliance with security policies. When an endpoint requests access to the network, a policy server queries the endpoint, determines user identity and endpoint health, and makes an access control decision based on the resulting information. The policy server sends a policy decision to an enforcement point, telling it whether to permit access, deny access, or quarantine the endpoint. TNC interfaces standardize communication between these components at the network, transport, and application layers.

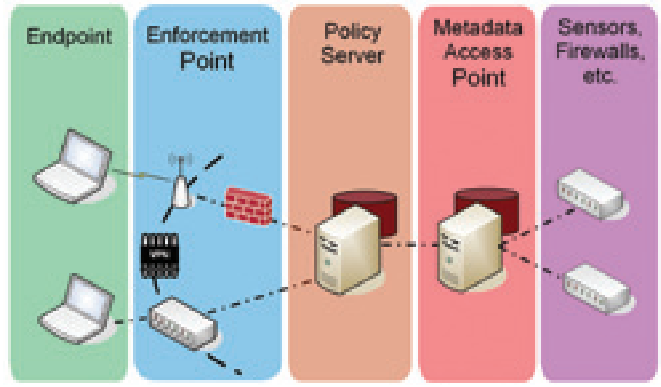


Figure 2: TNC standards enable integration of best-of-breed networking and security products to ensure dynamic, intelligent access control decisions.

IF-MAP – TNC's Cornerstone of Interoperability

TNC's IF-MAP (Interface – Metadata Access Point) standard extends the TNC architecture to allow data sharing across a huge variety of security and networking systems. The Metadata Access Point, or MAP, is a central clearinghouse for endpoint metadata; MAP clients can publish, search for, and subscribe to notifications about that metadata. Any networking and security technology can be a MAP client; examples include intrusion prevention system (IPS) platforms, vulnerability scanners, dynamic host configuration protocol (DHCP) servers, physical security systems such as badge access solutions, and even application servers. These components can act as sensors adding data to the MAP and/or act upon information received from other components.

The open interface to MAP enables customers to implement the 'appropriate behavior' requirements of a security policy in ways that would be difficult, if not impossible, using proprietary single-vendor solutions. As an example, one could connect Hirsch access control systems to a MAP server in order to monitor physical security of facilities. What if user 'Joe' is connected remotely to the SCADA network via VPN, but then the access control system reports that he just scanned his badge to gain entry to a substation? Clearly, Joe cannot be in two places at the same time. The open, multi-vendor nature of TNC and MAP enables this type of integration today, taking advantage of the best available products from multiple vendors to build customized solutions quickly and inexpensively.

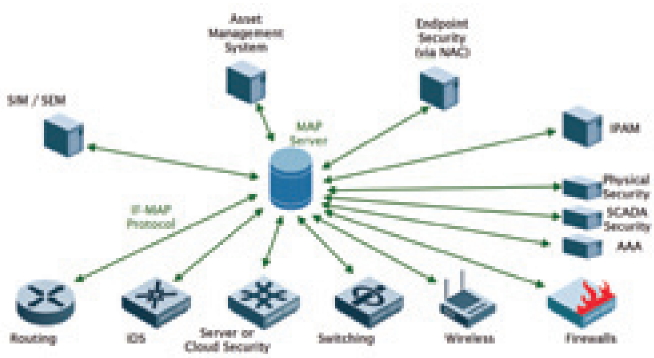


Figure 3: The MAP enables integration of security products from different vendors, allowing them to share information in real-time.

Onward into the Future

Now, more than ever, organizations interconnecting control system networks with corporate IT networks need to be aware of potential risks. Planning, processes, and technology are required to adequately reduce exposure, mitigate the risks associated with a hyper-connected environment, and prepare the infrastructure to securely handle change.

The current trend towards higher levels of integration between enterprise and control/SCADA networks will continue to accelerate as operators seek improved productivity and return on investment (ROI). However, this ROI will not be realized without significant improvements in control system security. TNC and MAP provide an open ecosystem of interfaces, tools, and products that enable robust and flexible security architectures to be deployed quickly and cost-effectively. Moreover, integration of specialized security products demonstrate that open standards from TNC enable management of security policy for both the enterprise and control networks from a single set of tools, offering high levels of security in a very cost-effective solution.

ABOUT THE AUTHOR

Scott Howard serves as a representative to the Trusted Network Connect Work Group of the Trusted Computing Group (TCG). TCG is a not-for-profit organization formed to develop, define and promote open, vendor-neutral, industry standards for trusted computing building blocks and software interfaces across multiple platforms. Scott also serves as System Architect at Byres Security Inc. and has over 30 years of experience in embedded system development, technical sales and product support with companies such as Motorola (now Freescale) Semiconductor, Embedded Support Tools and Wind River Systems.

Scott has been with Byres Security since 2007, where he was Product Development Manager during the first two releases of the Tofino Industrial Security Solution until transitioning to his current role in 2008. He is a graduate of the Electrical/Electronics Technology program at Camosun College in Victoria BC. (Scott can be reached for questions or comments via email to *scott.howard@tofinosecurity.com*.)

Volume 8 No. 2

With William T. (Tim) Shaw
PhD, CISSP

SECURITY SESSIONS

But all my friends are doing that!

Welcome to this installment of Security Sessions, a regular feature focused on security-related issues, policies and procedures. Several cyber security incidents have gotten industry media attention over the past couple of years and have started people thinking about how to protect the 'less than obvious' potential avenues of cyber attack. That's a good thing. But one bad thing I still find when evaluating and planning cyber security for industrial automation systems is the lack of a realistic assessment of the value and impact (particularly negative) of some of the things done to try and protect them. On occasion it seems to me that the cure has in fact made things worse. Blindly applying security controls just because they are called out in some standard or recommended practice may lead to unnecessary expense and an actual reduction in your security posture. – ***Tim***.

In previous columns I have made the point that blindly applying IT security mechanisms and practices to industrial automation systems is not always (or maybe ever) a good idea. There are many security controls and practices that make very good sense in an IT environment, but which may actually have a negative impact on overall cyber security if applied to a plant automation system and plant environment. But rather than just repeating that simple statement this time I would like to give some prime examples.

The helpful and talented folks at NIST (the National Institute for Science and Technology) have published a long list of recommended cyber security best practices. I consider their "800 series" documents to be mandatory reading for anyone who considers themselves to be a cyber security expert. One of their documents (specifically Special Publication 800-53 "Recommended Security Controls for Federal Information Systems and Organizations") is a comprehensive set of recommended technical and administrative security "controls" for application to government IT facilities and IT implementations. I have often heard this document referenced when discussing how to implement cyber security in industrial settings, but I do not believe that was what the authors intended as they are very clear about its 'IT' orientation. The authors also encourage making informed decisions about the application of their recommendations. Let me enumerate some of the controls from that document that are clearly questionable in an industrial setting:

AU-5 Response to Audit Processing Failures – This control deals with maintaining system use and access logs and suggests (as one alternative) failing a computer (preferably to a backup, if available) if it loses its ability to continue generating and storing audit records. Loss of auditing helps to hide the actions of an attacker that is tampering with a system so some attackers intentionally shut down auditing functions. This would NOT be the typical recommended course of action with an industrial automation system since maintaining control of the process is paramount.

SC-20 Secure Name/Address Resolution Service – This control deals with making sure that when a user or application needs to convert a computer or domain name into an IP address this process isn't co-opted by an attacker providing a false address (something called 'DNS poisoning'). This functionality is mainly needed by users sending email and browsing the Worldwide Web. Users of industrial automation systems really ought not to be doing such things as it implies connectivity with the Internet. In addition, most industrial automation systems are composed of a small number of computers, so it is viable to maintain a fixed pre-defined list of computers (called a "hosts" file) that you need to know about.

SC-17 Public Key Infrastructure Certificates – This control deals with obtaining and verifying digital certificates ("certs") so that when your computer is making a connection to another computer you can verify its identity by asking a trusted third-party (the supplier of the "cert") to verify the certificate it offers as identification. This is great when doing on-line shopping, but again it implies a need to make random connections over the Internet – not something that should be happening with an industrial automation system. Someone will probably argue that you can use a PKI architecture within a plant or corporate network, and not have any Internet connectivity involved. This is true, but then you end up with a central server acting as a certificate authority, which can be a potential single point of failure. Several years ago the California ISO used this approach and had all of their digital certificates in all of their equipment spread all around the state expire on the same day at the same time. The results were, needless to say, ugly. The various computers in their systems stopped talking to each other because they were told, by their own central certificate server, that the certificates being offered as identification were no longer valid.

SC-25 Thin Nodes – Managing all applications and databases centrally and only offering users a "remote desktop" makes software license management, malware scanning and software updating/patching much easier. Thus, an IT system manager may greatly prefer a thin-client design. But industrial control systems may not benefit from such a design. Most of the distributed control system (DCS) designs, including those based on PLCs, are in fact "fat client" designs where each workstation (operator or engineering) contains a copy of all of the software needed for the various users. This is done usually as a means of providing fault tolerance and redundancy. Such a design does not have a single point of failure such as a central server where all applications are actually running. This is not to say that some industrial automation vendors have not going to a thin-client design; there are SCADA systems that have that architecture. But it is not always appropriate in every application.

SC-13 Use of Cryptography – This control, as specified in the NIST document, is primarily intended to protect the confidentiality of sensitive/secret information when transmitted over a network or retained in computer storage. There are industrial automation systems that contain confidential information related to trade secrets (e.g., product formulations) and competitive marketing data. But for the most part the information in most industrial automation systems is not worth the effort to encrypt and in fact encryption/decryption could have a negative performance and timing impact. Encryption capabilities don't tend to exist within the current process controller and PLC product offerings so adding it would be messy and of questionable value. Encryption may well be appropriate for interconnections between independent systems that need to exchange data – for example, between a regional reliability coordinator or ISO and an EMS system – but that is not so much for confidentiality as to ensure that message traffic over an insecure network cannot be "spoofed" (i.e., fake messages sent with bad/malicious data values).

SC-10 Network Disconnect – This control requires that 'sessions' (communications between computers) be terminated after a defined period of inactivity. This is so that a user who walks away from their workstation/PC (or goes home for the day) gets logged out automatically, thus preventing a take-over of their still-active workstation by someone for nefarious purposes. In many plant control rooms there are operator workstations that communicate with plant controllers and display constantly-updated plant information, but which do not receive any user input (i.e., mouse movement or keyboard activity) for hours or even days on-end. Having an operator workstation go 'blank' and require a user login to reactivate it, because no operator banged on a key or wiggled a mouse in the last 15 minutes would not be considered acceptable in most plants I've visited. In fact, it would be seen as dangerous and a safety risk.

I could come up with many more examples from the long list of recommended controls enumerated in that NIST document. Again, I am not saying that there is anything wrong with the controls recommended by NIST in special publication 800-53. Actually, I have high regard for the work done by the people of NIST in this area. I am saying, however – and I think the authors of that document would agree – that those controls were specifically identified as being appropriate and important in an IT environment. You need to consider their purpose and security basis when making the decision to apply them to an industrial control system and in a plant environment.

Every control, be it a physical control (i.e., locked doors and cabinets) a technical control (i.e., a firewall or malware scanning software) or an administrative control (also called operational and management controls; i.e., policies, procedures and training) addresses a potential threat, attack pathway or vulnerability. By understanding these you can make an informed choice about which controls make sense and which don't. I have done some work recently in trying to write-up the cyber security basis for each of the controls specified in the NIST document. I plan to offer some examples shortly. But that will have to be the subject matter for a future column. ***Tim***.

ABOUT THE AUTHOR

Dr. Shaw is a Certified Information Systems Security Professional (CISSP), a Certified Ethical Hacker (CIEH), a Certified Penetration Tester (CPT) and has been active in industrial automation for more than 35 years. He is the author of Computer Control of BATCH Processes and CYBERSECURITY for SCADA Systems. Shaw is a prolific writer of papers and articles on a wide range of technical topics, has also contributed to several other books and teaches several courses for the ISA. He is currently Principal & Senior Consultant for Cyber SECurity Consulting, a consultancy practice focused on industrial automation security and technologies. Inquiries, comments or questions regarding the contents of this column and/or other security-related topics can be emailed to tim@electricenergyonline.com.

Balancing FERC Compliance, Public Concern and Delivery of Safe, Reliable Power

By Darin Sloan, Portfolio Manager,
DuPont Land Management

> Utilities face a difficult task when it comes to balancing the public's desire for uninterrupted power and landowners' tolerance for what it takes to deliver that service. On one hand, unmanaged vegetation in utility rights of way can cause power outages that disrupt people's lives. On the other hand, the same people who don't want to miss their favorite television program due to a power outage may protest when a crew applies herbicides or trims trees under power lines adjacent to their land.

Massive blackouts on the East Coast in 2003 vividly demonstrated what can happen when vegetation interferes with power lines. That sequence of events led the Federal Energy Regulatory Commission (FERC) to enforce stricter clearance guidelines with hefty fines – up to $1 million per day – for vegetation-induced outages.

Many U.S. utility companies are responding to increased regulations with integrated vegetation management (IVM) programs, while trying to win support from their power line neighbors. The key to turning former critics into allies of an IVM plan is open communication about the many benefits IVM offers, including safe, reliable power transmission and enhanced natural habitats.

What is an IVM program?

IVM compiles the most appropriate vegetation control techniques for electric rights of way projects, according to the North American Electric Reliability Corporation (NERC), the organization designated by FERC to develop transmission reliability standards. NERC guidelines give land managers flexibility to implement a customized plan that includes the right mix of biological, chemical, mechanical, manual and cultural methods to meet the brush-control needs of each site.

Nelsen Money, president of NRM-VMS Inc., and past president of the Utility Arborist Association, has more than 37 years of utility vegetation management experience. He advises utilities that creating an IVM program helps minimize interruptions caused by vegetation while maintaining a harmonious relationship with the environment and surrounding land users. To create an effective IVM plan, he suggests these steps:

1. Set clear objectives around what you want to accomplish.
2. Identify compatible and incompatible vegetation, including any noxious or protected species.
3. Determine optimal timing for various control methods and how that varies by landowner, land rights, etc.
4. Develop criteria for evaluating and selecting appropriate control methods.
5. Make a plan for implementing control methods.
6. Determine how and when you'll evaluate results.
7. Record what you've done so you can adjust the program over time.

Keeping costs in check

A long-range IVM program considers not only the best approach for this season, but also what will fulfill the site's objectives for years to come. A well-designed IVM plan saves labor and reduces operating costs over the long term. Since vegetation management often represents a utility company's largest operations and maintenance cost, it makes sense to incorporate practices that promote self-sustaining habitats for less mowing and trimming and fewer herbicide treatments.

While mechanical-control-only programs provide immediate relief from overgrown vegetation, this approach may not be the best – or most efficient – long-term solution. For example, a program that includes continuous mowing tends to trigger sprouting and/or live stem regrowth, which must be mowed regularly to meet FERC standards. This ongoing expense stresses rights of way maintenance budgets.

A study that evaluated the efficiency of IVM practices was conducted recently by Richard Johnstone, also a past president of Utility Arborist Association and president of IVM Partners, Inc., a 501-C-3 non-profit corporation, and principal of VMES, LLC, an independent consultant who helps utility companies, conservation groups, and federal and tribal agencies develop IVM programs. He evaluated vegetation control methods on a power distribution right of way adjacent to a forest. According to Johnstone's calculations, the initial cutting and herbicide treatments cost the utility approximately $300 per span, but after the initial cleanup that figure dropped to $10 per span for selective touch-ups.

Money cites similar cost comparisons, estimating that a utility working to reclaim a right of way that's been uncontrolled for several decades might incur initial mechanical clearing costs of $5,000 to $8,000 per acre, depending on site conditions, varying labor costs, regulatory restrictions and other factors. When that program is followed the next year by selective herbicide retreatment of sprouts, the estimated application cost can drop to $500 to $800 per acre. Using a selective herbicide that allows low-growing shrubs and herbaceous plants to flourish will stymie new tree growth and encourage the site to become more self-sustaining. Subsequent spot treatments on the few brush or weed species that survive may not be needed for five or six years.

Restoring native plants, minimizing environmental concerns

Johnstone notes that an effective IVM program releases native prairie grasses, wildflowers and low-growing shrubs, which out compete taller-growing species. This approach can reduce labor, herbicide use and equipment costs, while enhancing habitat for pollinators, birds and other wildlife. Following the IVM program's management plan will help prevent the area from returning to overgrowth, which triggers more costly mechanical control measures.

He followed this approach when advising a natural gas company with 15- to 20-foot tall vegetation along a transmission pipeline right of way that crossed land managed by the U.S. Army Corp of Engineers. He initially mowed the area and let it sprout one year, then made a follow-up herbicide application and a later touch-up application. The program controlled overgrown brush and allowed restoration of low-growing native vegetation that was visually appealing to the public, and met the natural resource management needs of the Corp.

By reducing necessary mowing, utilities decrease both maintenance costs and the environmental disturbance from heavy mowing equipment that fosters invasive weed spread. Ruts created by big machines also can lead to erosion problems. Worker safety is another concern when operating mowing and trimming equipment.

Selective brush and weed management

To help restore native vegetation, appropriate selective herbicides can target undesirable brush and weed species while allowing desirable vegetation to flourish. Eliminating invasive species that compete for water, sunlight and nutrients helps native plant populations return, providing valuable habitat for wildlife and pollinators and creating an aesthetically pleasing landscape.

By using non-federally restricted herbicides with low use rates, utilities gain multiple efficiencies. With non-restricted products, applicators have greater flexibility to treat where applications will be most beneficial. And low-use-rate products require less storage, hauling, measuring and mixing, which reduces the chance for error and allows applicators to prepare and apply tank mixes more quickly and confidently. Favorable environmental profiles also help support public acceptance.

Effective IVM programs also give managers more options when working with land managers. Because rights of way land crosses through nature preserves, ranches and other types of areas, Johnstone and Money advocate discussing land-use goals with landowners and working toward a mutually beneficial control plan. For example, Money says if the land manager works for an entity that promotes cavity nesting areas, a solution might be to use a herbicide application technique that kills trees in place, which allows them to remain standing after they're killed and provides nesting habitat for bird and animal species, or hunting perches for raptors.

Johnstone also incorporates wildlife habitat concerns into vegetation management plans when working with national wildlife refuges, and national forests and parks. His recommended practices include the selective use of herbicides that allow wildflowers, forbs and grasses to grow, while retaining shrubs for songbird nesting and food.

Communicate, communicate, communicate

To win support for IVM efforts, good communication is essential. That means educating internal and external audiences about what will happen, why it's happening and what the long-term environmental benefits will be. This exchange with stakeholders should start before work begins to preclude any initial problems or misunderstandings.

Money recommends clearly defining key messages that will be conveyed to audiences and delivering them directly and positively. Suggested messages:

- We are using IVM best management practices.
- Our goal is to create sustainable vegetation types of grasses and low-growing shrubs.
- We are using EPA-approved herbicides and professionally trained applicators.
- The vegetation will provide a diverse habitat for wildlife, plants and pollinators.
- Our program is designed to reduce visits to your property to maintain the right of way.

Johnstone also relates that IVM management reduces greenhouse gases and pollution from oils, fuels and hydraulic fluids that are inherent in mechanical mowing operations. At a time when the industry is trying to lower its carbon footprint, regular mowing practices become difficult to defend.

Implementing an IVM program offers a variety of benefits for adjacent landowners, the public and the utility. By communicating how the program ensures safe, reliable power distribution, as well as sustainability and enhanced environmental benefits, you'll win support for your efforts from concerned parties. Educated internal audiences will also respond positively when they learn how IVM techniques add greater efficiencies and economic benefits for the utility.

Reference Materials & Additional Information

A downloadable copy of the FAC-003-2 Technical Reference is available at *www.nerc.com*. Detailed information on developing and implementing an IVM program can be found in the American National Standards Institute (ANSI) *A300 Part 7: Tree, Shrub, and other Woody Plant Maintenance-Standard Practices (Integrated Vegetation Management a, Electric Utility Rights-of-Way)*, available at *isa-arbor.com* or *tcia.org*. Examples case studies of successful IVM programs are available at www.ivmpartners.org, and an IVM video produced by Virginia Tech can be viewed at *www.vegmgmt.com*.

ABOUT THE AUTHOR

Darin Sloan is a portfolio manager for DuPont Land Management, where he oversees development of new herbicide products designed for vegetation management professionals. He earned a B.S. degree in mechanical engineering from Mississippi State University and a M.S. degree in industrial administration from Purdue University.

ADVERTISERS INDEX


Smart Grid
RoadShow
St. Petersburg, FL
April 23-25, 2012
www.smartgridroadshow.com
HOST
Progress Energy