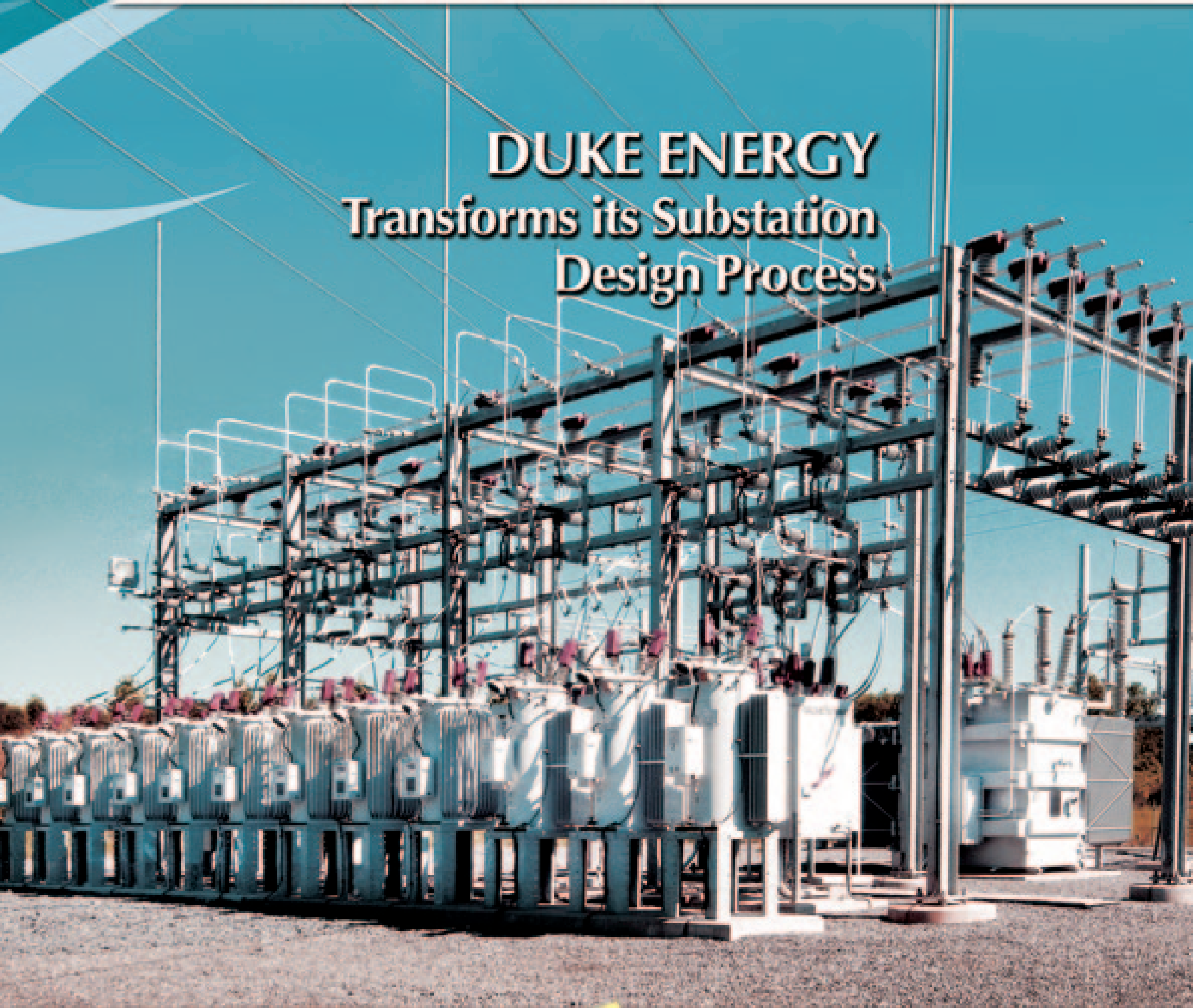
PP40010982

www.electricenergyonline.com

Electric Energy T&D MAGAZINE

NOVEMBER-DECEMBER 2009 Issue 6 • Volume 13



DUKE ENERGY
Transforms its Substation Design Process


The going never gets too tough
for our transformer oils.

Electric Energy T&D MAGAZINE

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
Gregory K. Lawrence, Partner; McDermott Will & Emery LLP
glawrence@mwe.com

Advertising Sales Manager:
Jimmy Desjardins: jimmy@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.

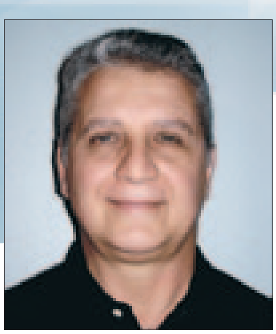
Post Publication mail agreement #40010982
Account #1899244

BPA WORLDWIDE BUSINESS

COVER PAGE IMAGE: Duke Energy

GRIDLINES

Michael A. Marullo, Editor in Chief



The barometer is rising!

The other day while having my morning cup of coffee and looking over the usual avalanche of email, I started reading an article about the decline of business journalism and it's impact on the ability of company CEOs to share their corporate stories clearly and accurately in the business press. What started out as a casual reading, however, became more and more intriguing as I read on.

The primary message being put across in that article was that with younger, less experienced staff increasingly replacing broadly experienced veteran reporters all across the business media landscape, *"…it falls to public relations professionals to spend more time explaining how a company fits into a broader social or economic trend — articulating their company's stories in a way that the reporters can understand and appreciate. In the past, news organizations provided this perspective, but that capability has been steadily declining for some time now."* [1]

The article goes on to point out that it's more important than ever for CEOs to develop core communications messages that go beyond the issue of profitability and stock price. The broader and still unanswerable question is whether the decline in the quality of business journalism will have an impact on the critical business issues of the day.

That got me thinking about the emails, abstracts and manuscripts we receive from potential editorial contributors to the magazine almost daily. Some of these come directly from the originating companies and authors, but today we see an increasing portion coming from – though not necessarily written by – public relations firms and communications consultants; and not only those from major corporations with PR firms on retainer. The fact is, we're also starting to see more of these articles coming from PR agencies serving smaller companies, which also need (and deserve) professional representation for this vital business area.

I must say that I find all of this quite interesting; especially since it wasn't so very long ago that it was almost impossible to find a public relations firm that could be of practical use to automation/IT companies. By this I mean the kind of automation and information technology companies serving the energy and utility industries – not consumer electronics companies. Why the distinction? Because being able to offer interesting insights about something as mundane as a sectionalizing switch for feeder automation is a much different challenge than putting a shiny purple MP3 player in the hand of an attractive, technologically hip model for a TV or magazine spot – even if your target audience really, really likes cool sectionalizing switches!

Indeed, it has never been all that difficult to find a PR firm capable of handling consumer-centric technology products. But finding one that could grasp the applications and nuances typical of industrial markets used to be a rare find – and believe me, I've spent a lot of time trying to find them over the years. Even in big media towns like New York, Chicago and Los Angeles, PR firms with tangible technological skills and experience were relatively few in number, at least until the "dot com" explosion began in the late 1990s.

During that period, high-tech PR and communications agencies were springing up almost everywhere – even here in New Orleans, where local firms have traditionally depended primarily on jewelry stores, restaurants, shipping and tourism to sustain them. Even the coverage by major oil and gas media consultants was mostly about financial reporting and annual reports; not much at all on the technical side of the energy business. But as is often the case, that was then, and this is now. To be sure, we still don't have the legion of PR choices that places like Atlanta and Dallas have at their disposal, but it's definitely a lot better than it was.

Today, almost any major city (as well as a lot of smaller ones) offers a choice of PR firms ready to help craft and polish your image and your message. Perhaps one of the reasons more – and decidedly better – resources are available in our market space today is that the energy and utilities market is suddenly at the center of the universe when it comes to publicity; not just in the industry trade press, but across virtually all forms of media. But whatever the reasons, it's easier than ever to portray your company in a positive light and get professional help in doing that.

You've probably heard the cliché, "bad press is better than no press," but why make that trade-off? While most of the editorial material we receive here at the magazine – regardless of the originating source – is quite good, there are still a few companies and individuals that have yet to fully grasp the basic concepts of business journalism. Keep in mind that the goal isn't the Nobel Prize for literature – just some fact-based content; a coherent flow of information; a couple of interesting visuals and conforming to the basic format guidelines will do just fine.

Although by reading through the pages of this issue you can readily see that we get a lot of excellent editorial material, other submissions are rejected because they fail to present the information in a format that allows readers to easily absorb the salient points and value in an interesting (and non-commercial) way. There are some very good PR firms that can help you avoid the pitfalls and present your story accurately, stylishly and professionally. Seek them out, and you just might be surprised at the impact it can have on getting your material published – and read.

In conclusion, let me say that despite the glitz of the advertising component, I believe that editorial quality is the true barometer of the media business… and thanks to a new breed of tech-savvy communications and public relations resources, that barometer is rising!
– ***Ed.***

[1] *What a Declining Business Media Means to CEOs*; Holstein, William J.; Strategy+Business; Oct. 3, 2009


The energy
to go clean™

Oncor, Landis+Gyr Reach National Leadership Milestone in Advanced Meters

300,000 Meters Installed in North Texas; Call for Other Industry Participants to Take Action

- Oncor, the owner and operator of the largest distribution and transmission system in Texas, and Landis+Gyr, the global leader in next generation energy management, today announced a milestone in its advanced meter system rollout with the deployment of more than 300,000 smart meters in the Dallas metro area. By year-end, Oncor anticipates nearly 700,000 advanced meters and the supporting network communications systems will be in place, making the deployment one of the largest and most quickly installed in the US.

With the support of Texas lawmakers and utility regulators, consumers in Oncor's service territory are now part of the most advanced grid in the United States. By 2012, Oncor will install more than 3 million smart meters that utilize Landis+Gyr's Gridstream(TM) solution to all of its residential and small business customers. Oncor is currently collecting and transmitting electricity usage data in 15-minute intervals for each of its deployed advanced meters, providing data to retail electric providers, and equipping the network to support in-home functionality such as in-home displays that further enable consumers to be involved in the energy management process

"Oncor is already on-the-ground making the benefits of smart grid technology a reality. Our consumers can more easily take control of their electric usage the way they want to, instead of how their utility wants them to," said Bob Shapard, Chairman and CEO of Oncor. "Combined with our customer education program, the installation of this smart metering infrastructure will empower 7 million customers to save more than $284 million annually and avoid the need for more than a dozen new power plants over the next decade. If every home or business in the United States had a smart meter, consumers could put $20 billion back in their pockets. That's real savings for real Americans."

Cameron O'Reilly, CEO of Landis+Gyr added, "Our partnership with Oncor is a significant step toward securing our nation's energy future. In the Texas market, we've worked with Oncor to discard old philosophies and to start thinking creatively about energy management. Using Gridstream as the platform, Oncor is making impactful and immediate improvements on the distribution side rather than the generation side, enabling both consumer involvement and operational efficiency gains at the utility."

Besides the obvious advantage of using less electricity, the benefits materialize through customers getting information about their energy use, and understanding that there can be a benefit to them for using more energy at off-peak hours, which in turn allows utilities to supply a steadier flow of energy, slowly phasing out the dramatic peaks and valleys that currently define energy supply patterns. Load-shift, as this is more commonly known, is proven to offer enormous benefits. A recent Brattle Group study found that just a 5 percent drop in peak demand nationally would eliminate the need for installing and running some 625 infrequently used - and highest emissions-emitting - peaking power plants, translating into annual savings of approximately $3 billion along with all the environmental benefits.

Circle **22** on Reader Service Card

OPOWER Unveils New Energy Efficiency Program with Seattle City Light

Program Supplies Customers with Comparative Home Energy Reports; Provides Customers with the Information Needed to Save Money on Monthly Electricity Bills

- OPOWER, the energy efficiency software company, announced that Seattle City Light, the nation's ninth largest public electric utility, has launched a new energy efficiency program based on the OPOWER Home Energy Report. Beginning October 14, 20,000 randomly selected homeowners in the Seattle area will begin receiving comparative Home Energy Reports, providing residential customers with the critical information needed to reduce energy consumption and save money on their monthly utility bills.

"The OPOWER Home Energy Reports deliver significant value to our customers by arming them with the information they need to control their monthly electricity bills and reduce their impact on the environment," said Bob Balzar, conservation resources director for Seattle City Light.

Industry News

"Based on the success of Home Energy Reports at utilities across the country, we expect the program to result in considerable savings for our customers, while enabling us to offset new energy demands through better efficiency and conservation practices."

The OPOWER Home Energy Reports are created using advanced analytics to evaluate customers' energy usage patterns, combined with behavioral science techniques proven to motivate action. Each report provides an anonymous, detailed analysis of individual monthly energy use as compared to similar households within the same geographic location, while recommending specific energy efficiency tips for every customer based on their household characteristics. The program is expected to generate more than $500,000 in electricity bill savings for Seattle residents over the next 12 months — all through simple behavior changes and by utilizing the energy efficiency tips provided in the Home Energy Reports.

"We're excited to partner with Seattle City Light, the first utility in the US to reach 'Net Zero' greenhouse gas emissions, and help Seattle maintain its position as a leader in clean energy," said Alex Laskey, president and co-founder of OPOWER. "The Home Energy Report program will enable Seattle City Light to more effectively engage their customers to help them better understand their energy use and provide insight into the simple steps they can take to realize significant energy and cost savings."

Circle **23** on Reader Service Card

3TIER Launches Next Generation of Solar Assessment Products

Industry's most advanced, scientific resource analysis available today

3TIER® unveiled a first-in-class suite of solar assessment products that give utility-scale developers a higher degree of certainty in the availability of solar resources and a more complete picture of the production potential of their projects. The products provide a 10+ year irradiance dataset, calibrated to observational data if available, and include a wind and temperature climatology to give developers a comprehensive, long-term outlook of their operating environment.

"A year of observational data simply doesn't provide enough information to make a prudent investment in a solar project," said Kenneth Westrick, founder and CEO of 3TIER, the global leader in renewable energy information services. "However, 3TIER can use that data to correct biases in our solar irradiance dataset to help developers understand, with greater accuracy, the long-term variability of their solar resource.

"Another important consideration is wind and temperature, as they affect the efficiency of PV and other solar technologies," added Westrick. "Their impacts are significant and need to be factored in for a complete analysis of solar resources."

The products are based on 3TIER's 10+ year solar irradiance dataset, the most advanced, high resolution solar irradiance dataset ever created. They also leverage 3TIER's expertise in numerical weather prediction (NWP) modeling, a capability the company has developed as a leading innovator in wind energy assessment and forecasting. The new products feature a complete wind and temperature time-series, as well as the option of using observational data to correct biases in the solar irradiance dataset, providing a full 10-year irradiance time-series.

"As the solar industry matures, and in light of the credit crunch, the squeeze is on to produce supply-side efficiencies," said Westrick. "Our new solar products give developers and financiers the information they need to maximize the value of their solar projects, while mitigating the risk of solar resource variability.

"The integration of wind and temperature as part of a solar study is available through 3TIER's FullView Solar Site Climate Variability Analysis. Product features include:

- Annual and monthly-mean irradiance maps of GHI, DNI, DIF
- Monthly variation of Irradiance
- Diurnal variation of Irradiance
- Irradiance histograms for GHI, DNI, DIF
- Monthly temperature and wind speed variability (min, mean, max)
- Diurnal temperature and wind speed variability and 12x24 table of hourly means
- Time-series for solar GHI, DNI, DIF
- Time-series for 10 meter wind speed and 2 meter temperature (length dependent on region of purchase)

3TIER's most in-depth and advanced product, FullView Solar Site Resource Assessment, allows developers to provide their own on-site irradiance measurements to calibrate 3TIER's solar dataset. Data is adjusted using Model Output Statistics (MOS) incorporating output from a high resolution numerical weather prediction (NWP) model run. The process produces a 10+ year, MOS – corrected solar irradiance time-series with greatly improved solar values and significantly reduced bias.

FullView Solar Site Resource Assessment product features include:

- Monthly variation of Irradiance (with MOS correction)
- Diurnal variation of Irradiance (with MOS correction)
- Irradiance histograms for GHI, DNI, DIF (with MOS correction)
- Monthly temperature and wind speed variability (min, mean, max)
- Diurnal temperature and wind speed variability and 12x24 table of hourly means
- Time-series for solar GHI, DNI, DIF
- Time-series for solar GHI, DNI, DIF with MOS correction
- Time-series for wind speed and temperature based on 4.5 km NWP model run
- Validation Report on the MOS-corrected irradiance time-series compared to observations

3TIER's dataset is based on more than a decade of half-hourly high resolution (roughly 1 km) visible satellite imagery that has been processed to create hourly values of Global Horizontal Irradiation, Direct Normal Irradiation and Diffuse Irradiation at a horizontal resolution of roughly 3 kilometers. The dataset currently covers the Western Hemisphere.

To capstone the solar product suite, 3TIER also offers more basic solar resource reports, as well as GIS data layers and API applications of the proprietary solar dataset. To learn more about 3TIER's basic solar reports visit *http://firstlook.3tier.com/solar*.

In addition to solar, 3TIER provides a full suite of assessment and forecasting products for wind and hydro energy projects. 3TIER uses its knowledge about weather, climate and their impacts on weather-driven renewable energy resources to help clients make better decisions about their investments – before, during and after their projects are built.

Circle **24** on Reader Service Card

Aclara ENERGYprism Customer Care Solutions Power Six of the Top Ten Electric and Gas Websites in Recent Study

Wellesley, MA – October 19, 2009 – Aclara, part of the Utility Solutions Group of ESCO Technologies Inc. (NYSE:ESE), today announced that six of the top ten electric and gas utility web sites, as well as the utility customer benchmarked as number one in the recently published E Source 2009 Review of North American Electric and Gas Company Web Sites, employ its ENERGYprism® web-enabled customer-care solutions. Additionally, 40 of the top 100 U.S. and Canadian utilities ranked in the E Source study have contracted to use Aclara applications. Avista Utilities, ranked number one in the benchmark survey, uses ENERGYprism modules to help customers analyze their utility bills and audit their energy usage. Spokane, WA-based Avista Utilities is an investor-owned utility with annual revenues of more than $1.3 billion, providing electric and natural gas service to approximately 481,000 customers within a 30,000-square-mile service territory.

Dana Anderson, Director of Service Development and Marketing for Avista Utilities, said that Aclara was a key partner in providing value-added capabilities to the utility's customers through the web site. "We really felt the energy audit was important to educate our customers on ways to save energy and lower their bills," said Anderson. "In the first quarter, we did a promotion that resulted in about 9,000 completed audits. We followed up on the customers who completed the audit and sent them information about specific energy efficiency program offers that would help them to reduce energy use."

On-line, self-service and web based energy analysis functions such as Aclara's are becoming more important to the success of utilities who wish to score well on the E Source web site benchmark study. The study evaluates 31 key capabilities recognized as important by the customer including the ability for the consumer to monitor energy usage, analyze their utility bills, select variable pricing options, and receive important service updates regarding outages and other activities.

"As more customers turn to their utility's web site to report problems or pay bills, the focus of these web sites needs to be online self-service," said Andrew Heath, Director of E Source Customer Satisfaction Services for E Source. "Surprisingly, we have found one of the hardest features to use on most utility web sites is simply making a payment." Although utilities have come a long way in the past few years in terms of offering self-service options, there is still work to do. This year, 56 of the utilities benchmarked offered E Source access to password-protected self-service options. "Self-service has become a big determinant as to how utilities ultimately rank," said Heath. Reviews done for the benchmark study are based on the responses of multiple reviewers visiting each web site. Reviewers are asked to assess their overall experience including their use of secure-access options.

E Source, which provides independent research as well as advisory and information services to utilities, major energy users, and other key players in the retail energy marketplace, performs the benchmark study to offer utility customers insight and guidance on what customers are looking for in websites.

Circle **25** on Reader Service Card


Reliable Systems.
Proven Services.
On Time. On Budget. On Site®.
Schweitzer Engineering Laboratories provides cost-effective engineering, procurement, and construction capabilities and delivers complete turnkey solutions. SEL also offers engineering services to support the application and operation of SEL equipment and other intelligent electronic devices. These services fill a growing need, as companies deal with the impacts of smaller engineering staffs and increasingly complex requirements for protecting, automating, and controlling their power systems.
To learn more about the capabilities of SEL engineering services, visit www.selinc.com/11eetd.
Worldwide 10 years Warranty
SEL
Celebrating
25 Years of Innovation
www.selinc.com
info@selinc.com
+1.509.332.1890

LightsOn

Austin Energy Delivers First Smart Grid in the US

By: Andres Carvallo,
Chief Information Officer,
Austin Energy

Many utilities around the country have announced plans to deploy smart meters (or will at least add some level of intelligence to their wires over the next few years) with many of those projects scheduled for completion between 2012 and 2015. Xcel Energy's Smart Grid City project in Boulder, Colorado is well under way and will be completed next year. But in Austin – where things are routinely done in that uniquely Texas way – their initial smart grid project has already been completed – now, in 2009 – while a lot of other utilities are just getting started.

Moreover, a newer and even more aggressive phase of Austin Energy's smart grid plan (designated Smart Grid 2.0) was already getting started as early as December 2008. Now, as AE rolls out its pilots for its The Pecan Street Project – a unique and exceedingly innovative vision for what can legitimately be called the Smart Grid of the Future – the enabling technology for even more advanced stages of their Smart Grid blueprint is already in place. Here's the rest of the story from Austin Energy's dynamic, forward-thinking CIO, Andres Carvallo...

Smart Grid 1.0

By the end of this year, Austin Energy will have deployed 500,000 devices (86,000 smart thermostats; 410,000 smart meters from Elster, GE and AMI partner Landis + Gyr, covering all of our service footprint; 2,500 sensors; and 3,000 computers, servers and network gear), gathering 100 terabytes of data and servicing a million consumers and 43,000 businesses throughout the Austin metro area.

Our initial Smart Grid 1.0 deployment was completed in October 2009 - the first fully operational Smart Grid deployment in the U.S. This landmark project comprises the seamless integration of our electric grid; a communications network; and the hardware and software needed to monitor, control and manage the creation, delivery and consumption of energy by every one of our customers. Smart Grid 1.0 goes from the central power plant, through the transmission and distribution wires, to the meter and back. It took us five years to deploy the full solution set at a cost of approximately $150 million. Smart Grid 2.0 will carry our Smart Grid plans even farther, providing the enabling technology for the advanced Smart Grid initiatives envisioned by our Pecan Street Project.

We began deploying our first 127,000 smart meters in January 2003. Today, five years later, the 410,000 smart meters we now have installed can deliver consumption data every 15 minutes. Austin Energy is testing the meters for the next phase of deployments now and plans to introduce some innovative new programs early next year that will allow customers to start seeing tangible benefits from those substantial investments in our future. The benefits will come primarily in the form of more efficient and less costly data acquisition and faster and more accurate information about how energy is being consumed.

AMR Meter Programming
Automated meters being installed and receiving initial programming

AMR Meters Support Pecan Street Project
Austin Energy has already installed 500,000 smart devices to enable its Pecan Street Project objectives.

The Pecan Street Project defines Austin Energy's smart grid initiative – a collaboration like no other. It all began in December 2008 when Austin Energy, the City of Austin, its Chamber of Commerce and the University of Texas teamed up to create Austin's next-generation smart grid implementation. But this ambitious project involves several other important organizations as well; these include: Applied Materials, Cisco, Dell, Freescale Semiconductor, GE, GridPoint, IBM, Intel, Microsoft, Oracle, the SEMATECH consortium and the Environmental Defense Fund, all of which have a role in our smart grid vision.

Why "The Pecan Street Project"?

The city picked the historic name "Pecan Street Project[1]" to advertise its ideas and concepts around energy efficiency, conservation, renewables and smart grid initiatives to the public – and indeed, the world – to allow all interested parties follow, evaluate and better understand our intentions.

Sixth Street in Austin is our New Orleans Bourbon Street, and as such, it is a major artery of Austin's famous live music culture. But you're no doubt wondering, why Pecan Street instead of Sixth Street? Well first, the original name of Sixth Street was Pecan Street. But more importantly, the team that came up with the Pecan Street Project name chose it because we are aspiring to achieve in clean tech that same kind of leadership position that is associated with the live music Austin represents to people of all geographical regions and walks of life the world over.

Next: Smart Grid 2.0

Austin Energy started working on this second phase of the project – Smart Grid 2.0 – in December of 2008. Since then, the team has been laser-focused on finding the answers to one vitally important question: *What happens to the smart grid beyond the meter and into the premises, the homes, factories and businesses?*

Smart Grid 2.0 is being driven by a growing vision of how homes and businesses will be different when they have access to some form of distributed generation – perhaps a solar rooftop, for example – connected to electric storage and smart appliances with an electric vehicle or two. And perhaps more important: How could those consumer assets be integrated into the grid in a way that you would preserve balance on the grid? That is, once distributed generation is feasible, not only will those consumers be using energy, but they will also be putting energy back into the grid.

Let's imagine for a moment that in 2015, 80,000 automobiles come from all over the continent to enjoy *South by Southwest* – our famous music and film festival – filled with people from the North, South, East and West. And let's imagine that those 80,000 vehicles are either plug-in hybrid electric vehicles (PHEVs) or some other type of electric cars, trucks or SUVs.

As those drivers ease into their seats they will set their in-vehicle navigation systems for South by Southwest in Austin, Texas. The cars themselves will communicate with the Austin Energy smart grid, identify the characteristics of the vehicles (and also their batteries) and initiate a whole new kind of "charge accounts" for their drivers. With these new accounts – and their corresponding charging station networks – up and running, our smart grid will provide the vehicles with information about where drivers can charge their vehicles, including a choice of high-speed or regular charging mechanisms at restaurants, hotels homes or other convenient locations in and around the city.

[1] Additional information about Austin Energy's Pecan Street Project is available on the Web at http://www.pecanstreetproject.org

Meanwhile, the grid will negotiate directly with the vehicles – wirelessly – and communicate price options for variable charging locations, which feature charging points that could take up to 10 hours to charge – or as little as two hours – depending on cost, urgency and other factors.

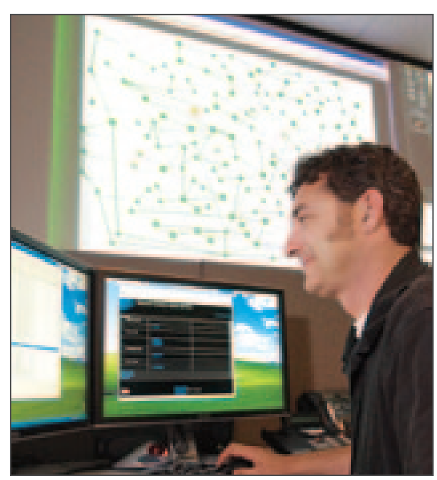
The "back-end" of the system Austin Energy creates will be able to handle that scenario and more. Yet what's really missing is the car having the ability to interact with us as human drivers. To address and solve that challenge, we're already working with Mercedes, Ford, GM, Chrysler and Toyota to create as seamless and transparent an experience as possible for driver and vehicle alike.

More Than Just Another Smart Grid Project

The main goal of the Pecan Street Project is to transform Austin Energy into the urban power system of the future while making the City of Austin and its local partners a model clean energy laboratory and hub for the world's emerging clean tech sector. In doing so, we seek to prove that it is possible to transform the way we traditionally produce, use, store and trade energy into a new behavior that is simultaneously consistent with our economical, environmental, social and security objectives and responsibilities.

Implementing this vision will likely include the following types of innovations:

- Connected homes that incorporate smart end points such as meters, appliances, and local generation, integrated with smart markets and distributed smart grids to enable two-way electricity flow
- Smart home energy control systems/portals that provide consumers with more information, alternatives, and decision support
- Smart appliances and devices that can turn off during times of peak demand or high energy prices, driven either by the energy services provider's policies or by consumer preferences
- Smart markets that feature pricing built on supply and demand models and that vary according to the time of day, day of year, etc. when the enegrgy is actualy consumed
- Smart policies and government stimulus approaches that foster the innovation and implementation of these technologies and markets
- A "green economy" workforce that can build, design, test, install, maintain, operate and continually improve and invent sustainable energy resources and innovative demand response capabilities
- Smart business plans that enable Austin Energy to continue to lead in this reinvention of the energy system without compromising its sound financial foundation
- Smart political leadership and popular will that shares the vision to make this project – and future projects – a reality
- Innovative laboratory environments supported by public, educational, private and NGO (Non-governmental Organization) partnerships
- Energy communities and networked information platforms that enable social network community development, community energy markets and sustainable economic improvements
- Smart transportation systems that incorporate two-way distributed approaches to information flows, energy flows, and unified information and energy storage
- Smart working alternatives that provide more green options to citizens, from smart working centers with virtual life size video alternatives, to alternative mass transportation, alternative routes, and stay-at-home options
- Connected and sustainable buildings for management of commercial and personal real estate; whether by tenants, owners, or energy services providers
- At least, 300MW of alternative, distributed generation through distributed wind and solar



Technology Control Center
Michael Owen, Network Systems Administrator in the Austin Energy Technology Control Center, which monitors the ITT network connecting AE facilities. The TCC is a one-stop technical support unit that handles more than 30,000 calls annually with first-call resolution of issues 85% of the time.

The Pecan Street Project comprises three distinct phases along with several parallel efforts. Although only the first two phases are described here in any detail, the third phase involves a potentially new research consortium and is even more creative and ambitious than the prior phases.

As previously mentioned, Smart Grid 1.0 was completed in October (2009) and focused on developing an action plan for Austin Energy and identifying key barriers that had to be overcome for long-term success. At the outset of Smart Grid 2.0, these barriers were organized into the following categories: Technology, Workforce, Markets & Business Models, and Policies.

The Technology section will then be divided into three sub-categories; namely: 1) Projects ready for implementation (for example, motion sensors for hallway lights); 2) projects that need to be tested and verified when integrated into the grid; and 3) projects that need to be developed. Some projects will be further categorized as generation, storage, efficiency, and low-tech options.

Distribution Management Pilot
Power Control System Supervisor, Stephen Driskell, programs an air switch for a distribution management pilot program. Thirty-nine of the air switches and related equipment will be tested with a software system that enables the devices to communicate in real-time with Austin Energy's Energy Control Center.

As technologies are verified over the first few years, they will be moved into implementation phase. And, as technologies emerge from the initial research process, they will be re-categorized as ready for testing and verification.

Policies will also be organized into several additional categories that accelerate adoption with incentives for consumers, energy services providers, the City, and also the private sector. Various economic stimulus approaches will also be examined and deployed, ranging from investments, bonds and tax incentives to R&D partnerships – just a few of the methods we will carefully explore, evaluate and select to build out the desired impact of green economy and Clean Tech Economy jobs.

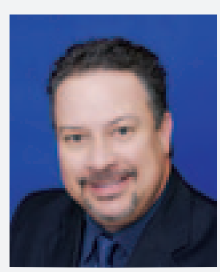
Some policies can be readily identified for implementation. For example, removing the ability of homeowner's associations or others to prohibit the installation of solar panels, while others will be identified, developed and worked through the appropriate regulatory, policy, and consumer acceptance models.

Conclusion

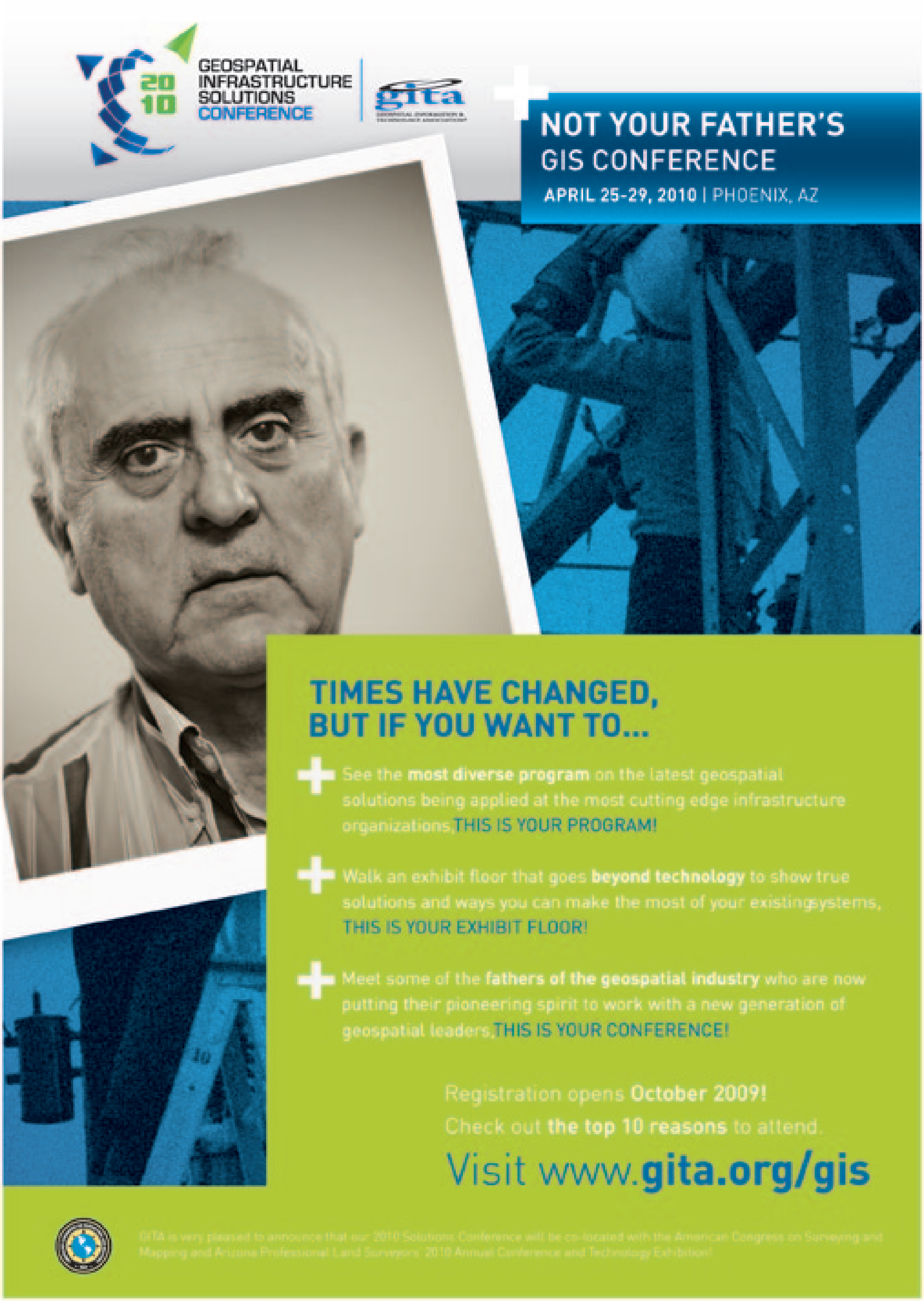
It is recognized that in order to change behaviors toward these positive opportunities, the Pecan Street project must strive for an unprecedented level of collaboration among city, state, and federal authorities will be required to ensure higher levels of consumer acceptance, satisfaction and a commitment to contribute to a sustainable economy in Austin.

Just as it took a century to invent today's energy system, the Pecan Street Project will require many years to reinvent it. Consequently, the cycle of technological innovation and implementation is expected to take place continuously. The inflection point of these two aspects will cause a disruption and accelerate the transformation cycles from what would ordinarily have been decades, to a decade or less. ■

About the Author



Andres Carvallo is the Chief Information Officer for Austin Energy, where he is responsible for the technology vision, planning, development and operations across the enterprise. An expert in hardware, software and communications, Carvallo joined AE in 2003 with the specific goal of freeing up capital and operating dollars to build a new business for the company, the major outgrowths of which are AE's Smart Grid initiatives and the subsequent Pecan Street Project.



GEOSPATIAL INFRASTRUCTURE SOLUTIONS CONFERENCE
2010
gita
NOT YOUR FATHER'S GIS CONFERENCE
APRIL 25-29, 2010 | PHOENIX, AZ
TIMES HAVE CHANGED, BUT IF YOU WANT TO...
See the most diverse program on the latest geospatial solutions being applied at the most cutting edge infrastructure organizations, THIS IS YOUR PROGRAM!
Walk an exhibit floor that goes beyond technology to show true solutions and ways you can make the most of your existing systems, THIS IS YOUR EXHIBIT FLOOR!
Meet some of the fathers of the geospatial industry who are now putting their pioneering spirit to work with a new generation of geospatial leaders, THIS IS YOUR CONFERENCE!
Registration opens October 2009!
Check out the top 10 reasons to attend.
Visit www.gita.org/gis
GITA is very pleased to announce that our 2010 Solutions Conference will be co-located with the American Congress on Surveying and Mapping and Arizona Professional Land Surveyors' 2010 Annual Conference and Technology Exhibition!

The 2009 Automation/IT Leadership Series

Brian Ahern
President & CEO

Walter Sikora
Vice President, Security Solutions

Industrial Defender, Inc.

(Foxborough, Massachusetts)

> "Shortly after 9/11 at the 2003 National Cyber Security Summit, Tom Ridge, then Secretary of Homeland Security, underscored the fact that the security of our nation's critical infrastructures could not be achieved without public education campaigns and public-private partnerships. He noted further that, 'the federal government can't succeed in these efforts alone.' Since that time, these words have resonated as an ideal rather than a reality. As the new Obama administration moves to enhance cyber security, revising critical infrastructure protection mandates from voluntary to mandatory status, the concept of public and private sector collaboration is at the forefront once again."
> *– Brian Ahern, President & CEO – Industrial Defender Inc.*

EET&D: Gentlemen, I've personally been aware of your company for quite a long time – well before the name change to Industrial Defender in 2007 and even before that, when it was still part of Hewlett-Packard's RTAP Division. Although you're rapidly moving up on the industry awareness scale, I think I can say with some certainty that many of our readers are probably not nearly as familiar with your company – yet. Therefore, I hope you won't mind quickly recapping the origins of the company before we turn our attention to the here and now.

Ahern: Not at all, Mike. Today, Industrial Defender is a privately held company with over 18 years of industrial control system and SCADA industry experience, and more than seven years of industrial cyber security experience. As you pointed out, we have deep roots in the automation business, particularly in SCADA and process control markets around the world, which began nearly two decades ago as the R&D group that produced HP's RTAP SCADA platform. After being spun off from HP, we were known as Verano, Inc. for several years before we changed our name to more accurately reflect our core business model.
Altogether, we have completed more than 100 process control/SCADA cyber security assessments; have in excess of 10,000 global security technology deployments in securing critical infrastructure systems; more than 3,000 mission critical SCADA deployments; and, we provide managed security services for 170 process control plants in 21 countries.

EET&D: That's quite a resume. It would seem that your real-time automation beginnings have served you well in making the transition from an automation systems company to a security solutions provider. The high degree of synergy within and across those areas of business and technology is certainly a big differentiator in a field where lately we've seen an ever-increasing supply of security solution providers.

Sikora: Yes, that's a very valid point, Mike, and it's one that really sets us apart from most other security solution providers. Our comprehensive knowledge of mission-critical control systems comes from having been there and done it; not just from reading about or otherwise studying the control systems business. To really understand how these systems have evolved from bit-oriented controllers, minicomputers and microcomputers programmed in machine language to modern-day automation platforms running sophisticated operating systems with a high degree of built-in intelligence, multiple communications platforms and Internet connectivity is no easy task – even for the most technologically savvy companies. In our case, we designed, built, installed and supported those systems for well over a decade before cyber security emerged as a major issue. not just from reading about or otherwise studying the control systems business.

EET&D: Okay, let's fast-forward to today. For the past several months, the Stimulus Bill has been top of mind for anyone associated with the interrelated goals of protecting our infrastructure and restoring the economy. Cyber security is not only an implicit part of those initiatives, it is also a stated national priority that we hear and read about regularly on local, national and international levels. No one can say that this is an obscure topic or one that begs for relevancy, yet there still doesn't seem to have been a whole lot of funding available to get the job done properly – if at all. Is that a valid perception, or is there more going on that may not be as visible as other dimensions of the infrastructure issue?

Ahern: Well, let's take the Smart Grid initiative as a prime example. No one doubts that, from both a reliability as well as a security standpoint, there is a clear need for an IT-enabled electric "smart" grid, paving the way to – among other things – significantly expand renewable energy resources. To that end, in his stimulus package, President Obama allocated $4.5 billion dollars to electricity delivery and energy reliability, underscoring the need for the legacy electric grid to make the move into the 21st century – and enhanced critical infrastructure protection is clearly an integral part of it. However, it remains to be seen exactly what portion of the Stimulus funding will actually make its way into cyber security R&D and real-world cyber security projects.

One way to realize true collaboration and foster mutually beneficial relationships is for the federal government to provide monetary incentives – perhaps in the form of funding grants or tax credits – to private sector entities willing and able to invest in cyber security threat monitoring and protection technology to support both this "next generation" critical infrastructure undertaking as well as ensure the security of the nations bulk-electricity system including power generation, energy control centers and transmission substations.

EET&D: What else is needed to help move security initiatives from concept to practical solutions?

Sikora: In addition to financial incentives, private sector operators of critical infrastructure must work in concert with the government to warn both the private sector and the public of potentially dangerous cyber security incidents. To facilitate this collaborative environment, the government should also strongly consider the concept of "Hold-Harmlesss" Protection. This would remove concern over the public relations ramifications associated with a critical infrastructure operator sharing threats and incidences; ensuring an open and collaborative line of communication between the private sector and public sector in the interest of public safety, national security and economic integrity.

Another consideration is the development, through the joint efforts of the public and private sectors, of a comprehensive "cyber heat map." This would ultimately provide transparent visibility into the current cyber security threats, as well as provide access to detailed information on each specific threat occurrence. Incorporating these proposals – while undoubtedly an aggressive undertaking – would allow for both increased cyber security protection as well as the flexibility to expand these infrastructure platforms to support future needs.

EET&D: What do you see as your role in this rapidly escalating focus on cyber security as it relates to the critical infrastructure we are simultaneously trying to preserve and protect?

Ahern: Industrial Defender is the first company to offer a completely integrated defense-in-depth cyber security solution designed to protect the industrial control system and SCADA environment in a flexible and cost effective platform. Our comprehensive "lifecycle solution" enables the efficient assessment, mitigation and management of cyber security risk within the critical infrastructure network domain. But no single company – nor even a group of companies – is likely to achieve effective, pervasive and sustainable cyber security without the collaborative involvement of the private and public sector.

EET&D: What are some of the things you would like to see that could help move the cyber security cause forward?

Sikora: For starters, a greater level of investment in defense-in-depth sensor technology, including electronic security perimeter, remote access and authentication, network intrusion detection, host intrusion detection, and patch monitoring and management, thus enabling real-time aggregation of threats and incidences for real-time reporting. FERC Order 706 also calls for "defense-in-depth" subject to technical feasibility considerations with NERC oversight.

Ahern: There's a whole host of other things we'd like to see, but we know that there's going to be a long road ahead. For example, one area of focus should be a centralized clearinghouse for the correlation of alerts and threat statistics. Such central oversight would provide intelligence regarding widespread information gathering and other attacks. For this type of centralized correlation to work, cooperation of large managed service providers and large self-managed networks is needed in order to send the necessary standardized alerts and threat statistics to the US government.

If a central agency were the real-time clearinghouse for conclusions about threat patterns and the correlation of such conclusions, that agency would be able to correlate suspicious activities across many industrial networks. Such correlation – especially correlation of threat threat profiling results – might allow the central monitoring agency to identify widespread information-gathering activities targeted at critical infrastructure networks. Such activity is a logical precursor to a widespread attack on infrastructure. It would also allow a central clearinghouse to draw conclusions about widespread infections, which might also be a sign of a coordinated attack on very many sites.

Recently, in testimony before Congress, we formally recommended that the Federal government investigate establishing a program, correlation infrastructures and technologies, and the necessary data exchange standards to permit real-time alerts and threat statistics to be aggregated centrally. Individual managed security service providers and large industrial security/network control centers would be encouraged – or required – to participate in the program and provide the central authority with the statistics and other information that the agency requires to calculate high level correlations. Such a program could provide government and various intelligence-gathering agencies with important insights into the overall health of industrial networks as well as insight into sudden changes or widespread patterns indicative of preparations for a large-scale attack.

Sikora: Another area of focus would be to strongly encourage control system vendor partnerships with the U.S. Department of Energy's National Supervisory Control and Data Acquisition (SCADA) Test Bed programs at Idaho National Laboratory and Sandia National Laboratory. There also needs to be a continued and raised emphasis on control system security product and technology assessments to identify vulnerabilities and corresponding mitigation approaches when systems are being designed and built.

EET&D: What do you feel is the rightful role for government in all of this?

Ahern: Escalation of threats and exposure of incidences are essential components of successfully thwarting cyber attacks against the nation's critical infrastructure. With 85 percent of the nation's critical infrastructure owned and operated by the private sector, the public and private sectors must work collaboratively, with trusted and open lines of communication to ensure the timeliest communication of critical cyber-security information. The private sector represents a valuable source of operational intelligence, which must be harnessed in order to effectively communicate and drive action to reduce the consequences of pending attacks.

EET&D: We hear a lot about NERC standards and guidelines these days. Do you feel that the NERC CIP standards are adequate at this point?

Ahern: While the NERC CIP standards have been a catalyst towards private sector action, unfortunately the vague nature of the standards have left many questioning whether this has been simply an exercise or has it really enhanced the security of the bulk electric system? It is our observation, based upon interaction with our clients, that the standards are unclear and undefined (subject to interpretation), punitive vs assistive, unfunded and a moving target. Based upon feedback from clients presently undergoing audits, there appears to be widespread disparity in process and approach by the various audit entities.

Our own internal analysis has shown that less than 15% of the total utility assets have been deemed "critical assets" with less than 10% of the total assets being deemed to have "Critical Cyber Assets". This begs the questions: 1) from a bulk electric system security perspective is the risk less today than before implementation of NERC CIP standards, 2) Does compliance equal "security"?, 3) has this been an exercise in futility that has driven a further wedge between Private Sector and Public Sector?

If the ultimate goal of critical infrastructure security regulations is to ensure public safety, national security and economic integrity then regulations have to provide equal amounts of incentives for compliance as they do penalties for non-compliance. A public sector/private sector relationship built upon trust and well defined goals and objectives will yield greater results.

EET&D: As you look further down the road, what do you think will be the ultimate outcome of the battle to protect our critical infrastructure from the rising wave of malware and potentially debilitating attacks?

Ahern: With the introduction of the Smart Grid the challenge becomes greater, not easier. The possible attack profile on critical infrastructure moves from nation/state adversaries and organized crime to a possible domestic/civilian threat as intelligence is extended down to the consumer. The dependency on achieving a truly "Smart Grid" relies extensively on an intelligent, fully integrated "smart utility." As such, far more of our critical assets will become intelligently interconnected, thus yielding far more critical cyber assets that ultimately require security.

EET&D: And if there's an "end game" here, what might that be, and in your opinion what do you feel has been learned thus far that you consider to be of lasting value?

Sikora: One of the greatest challenges we face in securing the bulk-electric system is establishing security for the current legacy infrastructure. At the time when much of the national electric infrastructure was installed, security was not at the forefront of design criteria. If there is a lesson to be learned as we contemplate future Smart Grid infrastructure investments, it is that security MUST be a key design criteria; not an afterthought. Presently the security of the electric utility supply-side infrastructure is vulnerable to attack; investments in consumer–side infrastructure ahead of securing the supply-side seems illogical.

EET&D: Brian, I'll let you have the last word on this…

Ahern: I fully anticipate that security of the entire electric power "supply chain" will one day be regulated. The key focus now must be ensuring the integrity of the electric power supply infrastructure while – as Walter just said – ensuring the future Smart Grid infrastructure investments are secure from the day of installation rather than an afterthought.

Duke Energy Transforms Its Substation Design Process

By: Arnold Fry, Supervisor for Substation Engineering Services Duke Energy

With the advent of CAD, work order management, and purchasing technology in recent decades, substation engineering underwent a transformation. Design, purchasing, and construction management transitioned from completely manual, paper-based tasks to being faster, digitally enabled processes. Substations that might have taken years to design and build can now be completed in under a year.

Virtually every electric utility in the United States relies on technology to complete critical pieces of the substation engineering and design process, but too often the pieces are not connected. Many companies use manual processes and time-consuming duplicate data entry to connect processes and systems.

Today, another transformation is underway. Electric utilities, including Duke Energy, are developing integrated workflows that automate key aspects of the substation engineering and design process. Soon these companies will have processes that are not only significantly faster, but also smarter and more intuitive.

The Case for Continuous Improvement

As one of the largest electric power companies in the United States, Duke Energy delivers energy to approximately four million customers in North and South Carolina, Ohio, Kentucky, and Indiana. Through its wholesale energy business, Duke Energy helps other companies meet the needs of their customers during peak usage times. The company's total U.S. generating capacity is 35,000 megawatts, and it relies on more than 3,500 substations to help safely transmit power to its customers' homes and businesses.

Duke Energy employs 18,000 people, each of who takes to heart the company's mission to make people's lives better by providing gas and electric services in a sustainable way. Success requires a constant effort to find better, more efficient ways of doing business. From customer service to outage management to power distribution, leaders in every area of the business are looking for opportunities to enhance efficiency. Recently, the substation design process has been the focus of a concerted process improvement effort at Duke Energy.

Traditional Processes Slow, Manual

At first glance, Duke Energy's substation design process might not seem like an ideal candidate for improvement. It's based around widely-used and well-regarded technology, and the quality controls supporting the process have done a good job of preventing significant errors, such as those that can negatively impact safety or construction costs. However, on more in-depth examination, challenges emerge.

Let's look more closely at the substation design process and workflow to gain an understanding of those challenges. Whether for new 'greenfield' projects or 'brownfield' retrofits and enhancements, the process begins with a request for a new substation in a given area. Requests are sent to the substation engineering services department via email, and a supervisor then routes the request to an estimator for scoping or directly to a designer, as appropriate. Most requests for new substations are thoroughly scoped before going to a designer, but many brownfield projects are routed directly to a designer. The estimator begins the process by creating a Microsoft Word template that details the project location, probable equipment requirements, desired completion timeframe, and necessary capacity. When the scope is established, the completed template is sent to a designer using email.

The designer reviews the email, and begins the design process in a traditional, 2-dimensional CAD (computer-aided design) application. Often, that requires incorporating elements from an existing paper network drawing into the design. The designer retrieves the drawing from the archives, scans it using an application that turns the raster image into vector data, which is the kind of data a CAD application creates and modifies. The designer then creates plans for the new substation.

Performing many calculations manually, the designer determines the specific capacity requirements for the substation, and emails a materials specialist who decides the types of transformers and other equipment that will be used. With the equipment specifics established, the designer creates a detailed plan that includes all the transformers, electrical connections, circuits, protective systems, and structural elements. The designer also needs to account for and order any necessary soil tests or survey work. Just as importantly, the designer must order any equipment that has a long lead time for fulfillment, meaning it's time to create a bill of materials (BOM) for the job.

Creating an accurate BOM is one of the most time-consuming aspects of the design process. Much of the time goes not into simply creating a list of needed materials; rather designers devote significant effort to following a quality assurance process that prevents over-ordering, under-ordering, and omissions. Over-ordering could add restocking costs to projects. Under ordering and omissions could lead to downtime and delays in the field. Duke Energy's quality assurance process does result in reliable BOMs, but currently, the process is highly manual, involving the counting and recounting of materials at key points in the design process. In fact, on a job that might take 200 engineering hours, managing BOM quality checks and entering BOMs into the purchasing system would represent as much as 40 hours of the total.

While its substation engineering process resulted in effective substations, Duke Energy recognized that its highly skilled designers were spending too much of their time counting materials and entering data across systems. The company decided to explore its options for connecting, automating, and accelerating the process.

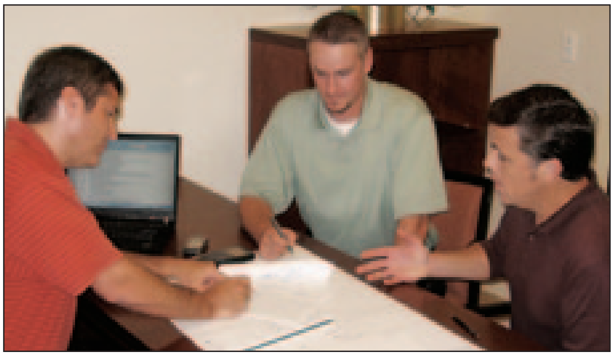
Casting a Wide Net

Duke Energy approached the re-engineering of its substation design process with an open mind and a set of clear requirements. Any new solution had to:

- Link the business systems involved, such as work order management and purchasing
- Automate all or significant portions of the BOM creation process
- Enable designers to easily leverage existing substation plans in projects
- Improve or automate load and capacity-related calculations
- Streamline the communication of design intent to construction crews

The company issued a request for proposals from organizations with significant experience with design technology, the utility industry, and process integration. From among a number of strong proposals, one from Autodesk caught the attention of Duke Energy. It was notable not because it accounted for all the company's key requirements – all the proposals received were adequate in that regard. What stood out was the fact it proposed a solution that exceeded the company's selection criteria and, that it was based around model-based design concepts more commonly used in the manufacturing and building industries than in the utility industry.

Duke Energy chose to build the Duke Energy Substation Design Solution (SDS) around Autodesk Inventor, AutoCAD Electrical, and Autodesk Vault software. In the solution, Inventor allows engineers to design using a 3D digital model, AutoCAD Electrical supports the design of electrical control systems, and the Vault software manages a library of reusable design elements. Each part of the solution allows for integration with other business systems. While it may seem unorthodox to use model-based design software to design electric substations, Duke Energy chose the solution because its leaders believed that the elements were all present to transform their disconnected design process.

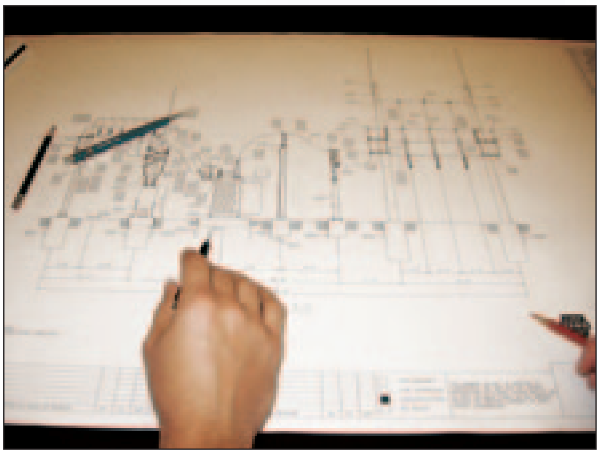


Automation Saves Time

Duke Energy is currently in the final stages of developing and implementing the SDS. When it is rolled out to the substation engineering group, the design process will employ a significantly transformed workflow, one that heavily leverages process automation. Work assignments will come directly from Duke Energy's enterprise and asset management systems, and those assignments will be routed directly to designers' SDS interface.

Before work even begins on a design, the solution will scope the work and produce a basic estimate of parameters and materials, which the designer can then fine tune. If the estimate contains any equipment with a long lead-time for ordering, the designer can route that specific material for immediate or scheduled purchasing.

Throughout the process, the solution automatically maintains an accurate BOM, and because the solution integrates with Duke Energy's purchasing system, ordering materials no longer requires any duplicate data entry. The old quality assurance check involving endless counting and recounting of materials across 2D drawings will be a thing of the past, and the risk of ordering issues will be greatly reduced.



To speed the design process, the solution automatically selects potentially useful existing drawings from the design library. The designer can use those designs as a starting point for the new substation model. So before core design work even begins, the designer can pull together appropriate transformers, breakers, and structural information from past jobs. For very simple enhancement projects and new substations, the design will be almost complete just a few hours into the process. The designer may only need to do minor modifications to ensure the elements identified suit the project.

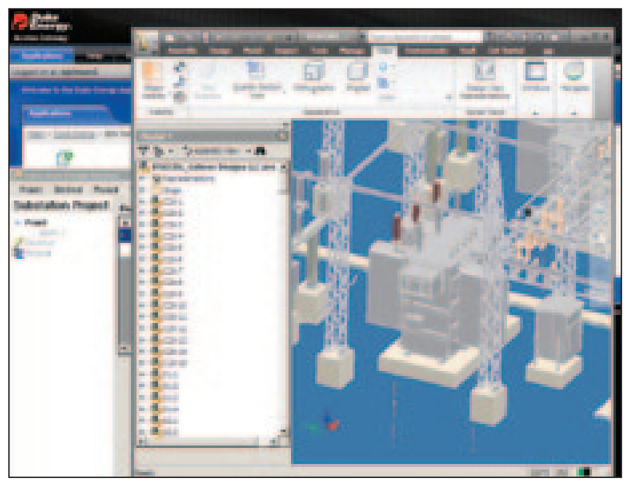
Enhancing the Design Process

As the job progresses, the solution automatically performs many routine calculations, including short circuit analysis, routing calculations, and bus calculations. When information that does not exist, such as the results of soil borings, needs to be incorporated into calculations, the solution flags it, so that the designer can find the information needed or order the relevant tests. Duke Energy expects that automating routine calculations will not only save time during design, it will also accelerate the quality control process by making it harder to generate inaccurate calculations in the first place.

Because the solution uses parametric modeling, it incorporates changes automatically. Basically, when one element of the 3D substation model changes, the solution dynamically modifies the parameters of the rest of the model to account for the modification. In contrast, with traditional 2D tools, users had to incorporate changes manually into each sheet within a design. Again, Duke Energy sees an opportunity for both timesavings and quality enhancement stemming from greater automation.

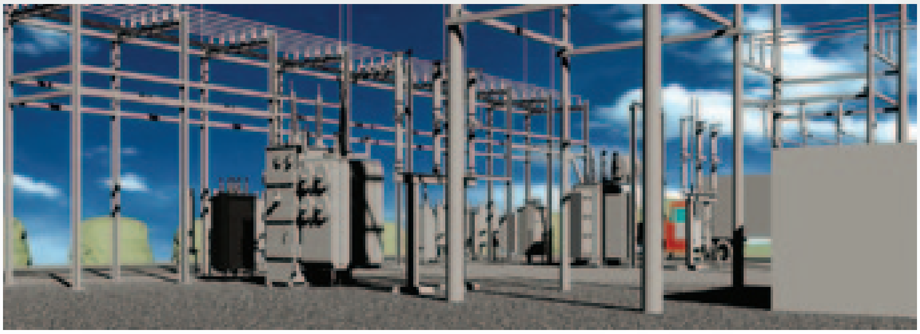
3D Substations

Duke Energy is looking forward to compressing design time by using automation to remove steps from the process, but the new process also includes an interesting addition: 3D visualization. As they work, designers will create an integrated 3D model of a substation that includes all the equipment, connections, and structural elements. They will see exactly how the whole substation comes together.



In a sense, they build a digital prototype of each substation before it's built. If a beam is impeding access to equipment, they see it immediately, and they can take steps to improve access. Duke Energy believes that 3D modeling has the potential to help enable better and more sustainable design. With 3D modeling, the designer will be able to easily explore how changes might improve substations or could lead to minimized waste and rework during construction.

Usability will take center stage in the design process. When designers ask "what if," they'll see the answer as soon as they make the change. For example, they can explore equipment placement with the comfort and safety of field crews in mind. A tiny modification in the placement of an equipment mounting bracket or a bus connection could make a huge difference in the time and risk involved in servicing nearby equipment. Buildability will also play a more prominent role in the new process. Construction crews will be able to see exactly how substations will look when complete.



It can be difficult for even the most experienced people to visualize the whole project, working only from lines on multiple design sheets – and that's what you get with 2D tools. The new 3D model-based design approach will allow construction crews to explore the big picture and the smallest detail of the design. This will help them to plan their work more efficiently and avoid rework due to misunderstanding some aspect of the design.

Looking Ahead

Every step of the way, Duke Energy is accelerating the substation design process with automation and integration. Soon, the company's substation design specialists will be able to devote virtually all of their attention to developing substations that are high-performing, safe, and cost-effective – instead of focusing on data entry, simple calculations, and counting.

The company estimates that the Duke Energy SDS will reduce overall design time by at least 50 percent on both greenfield and brownfield projects. With the time saved, the company believes that it will be better positioned to meet its customers' evolving capacity and service demands, including adding new substations to its network and completing the design work needed to enhance existing substations with smart grid technology. The Duke Energy SDS provides a clear example of how a technology that transforms one process – substation design – can help pave the way for more integrated, intelligent, and sustainable processes overall. ■

Smarter Substations for Smart Grids

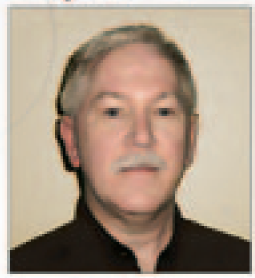
Soon in Ohio, Duke Energy will begin the process of deploying smart grid technology, including 80,000 smart meters by the end of 2010. The meters will enable near real-time information which customers will be able to use to better manage their energy consumption. In a sense, energy efficiency has the potential to become a "fifth fuel" – along with coal gasification and advanced pulverized coal, nuclear, natural gas and renewables – by helping large numbers of people to easily and proactively manage their energy usage, save money and reduce their carbon footprint.

The Duke Energy SDS will come online just in time to support the move to smart grid technology. Smart meters require the support of smarter equipment in substations. With SDS, the company will be able to create a template for the new equipment required in existing substations. Designers will leverage the template to complete the repetitive portions of the designs and BOMs very quickly, enabling Duke Energy to undertake a massive number of substation enhancements on an ambitious schedule.

SECURITY SESSIONS

Volume 1 No. 3

With William T. (Tim) Shaw, PhD, CISSP



One of the most controversial security-related issues that I run into – on a rather regular basis – is whether or not IT personnel are sufficiently knowledgeable about industrial automation (in general) and SCADA systems (specifically) to be put in charge of security for these types of industrial automation systems. And, whether they can/should be put in charge of ongoing technical support for such systems.

Quite frankly, in the 1970s and 1980s the groups that purchased, operated and supported computer-based automation systems were dealing with computer technologies very different from those of "office automation" or IT. (The existence of Information Technology as a separate entity actually evolved in the late 1980s.) That is, the IT folks were dealing mainly with IBM, Univac or Burroughs mainframe computers and the industrial automation folks were dealing with minicomputer manufacturers like Digital Equipment Corporation (DEC) and Data General.

The operating systems were totally different, the programming languages used (assembly and 'C' versus COBOL) were totally different, the computer hardware was totally incompatible and the networking (if there was any) was vendor-specific. But during the 1990s – and certainly today – most of those vendor boundaries have either disappeared or have been moved into specialized areas by contemporary suppliers.

Today, most automation systems are typically running on some type of MS-Windows/Intel platform, interconnected locally with other computers and devices using high-speed Ethernet[1] and connected over greater distances by TCP/IP networking technologies. The basic operating systems used in these systems (except in most [but not all] real-time 'controllers' and RTUs) will be either a Microsoft Windows™ variant or a Unix/Linux variant. And even in the controllers and RTUs there has been a move toward using commercial embedded operating systems rather than having vendors write their own. It is also probable that other 'standard' information technologies such as SQL-compatible relational databases, Web servers, etc. will be incorporated into those systems.

So, in other words, a large percentage of the elements that form those systems – as well as their overall architectural design – look just like those of a conventional IT/business system. You might even say that the major difference between an automation system and a business system today, is just a matter of the applications they are running. Personally I wouldn't super-simplify quite to that level, but the argument can be (and is being) made.

The observation that platforms have standardized is one reason why senior management in many organizations sees no reason why the "IT guys" can't also be responsible for the SCADA systems. I am aware of several organizations where the SCADA systems, and associated support and operational personnel, have actually been placed (i.e., organizationally), under the IT umbrella.

Historically there has been no love lost between the SCADA/operations folks and the IT department. That is undoubtedly the result of numerous factors. Over the years I've personally witnessed more than a few heated arguments between members of those two groups. The IT personnel usually don't see that there is any difference between the SCADA system and the business systems (or any that do exist are obviously minor). The SCADA personnel come from the standpoint that getting that system installed,

[1] Ethernet (IEEE- 802.3) is a registered trademark of Xerox Corporation; Norwalk, CT

commissioned and operating was a massive undertaking and they are loathe to make any modifications or let 'outsiders' do so. There are valid reasons for both viewpoints, but there are also critical differences that are not always apparent.

Conventional IT training and operational philosophies put a focus on three vital objectives for the computer systems they administer and support: Confidentiality, Integrity and Availability. Most texts about IT frequently refer to the acronym "CIA". These three objectives are also being listed in the priority order that makes the most sense from an IT viewpoint. Keeping the information in business systems confidential and trustworthy is critical. Keeping those systems operating and available is important. Usually nothing much bad happens if the IT guys need to reboot the servers. Although it would be nice, business systems don't always have the requirement for 100% availability that industrial automation systems are (and always have been) expected to provide.

Now before I get a pile of hate email from IT folks, let me say that the IT world does recognize the need to try for 100% uptime and some applications can cost-justify the necessary redundant elements. If you have a web based sales portal, downtime means lost orders and customers who might go to your competitor. But downtime generally doesn't mean potential for injury, death or massive physical damage. And that brings us to the main difference between the IT world view and that of the people running industrial automation systems: the issue of safety.

If a SCADA, DCS or PLC system is disabled, malfunctions, or is commandeered and used to manipulate field/process equipment and devices, there is a possibility – depending on the process involved and other safety and backup systems – that an unsafe condition can be created, potentially leading to injury, death and/or physical, and even environmental, damage. Of course, in the design of mission-critical systems we usually make them fully redundant and may even have a totally separate, backup system, located in a physically separated site impervious to intentional attacks and/or natural disasters.

Common practices that are low-risk in the typical IT environment, may be considered as too risky in the control systems world, specifically because of the safety implications. Examples of such practices could include deployment of new applications with less than exhaustive testing or the wholesale and immediate (and unquestioned) installation of unverified patches.

My own experience upgrading to Microsoft Office 2007 exemplifies that application pre-testing in the IT world doesn't have to be as rigorous as in the process control world. Indeed, there are numerous well-documented incidents where vendor-approved patches were installed on industrial automation systems, that resulted in system malfunctions and requiring restoration to a previous version.

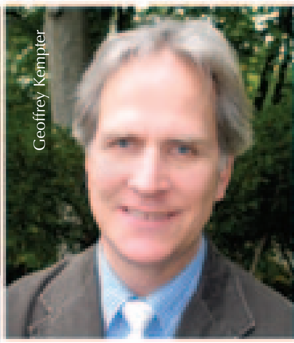
So, what about the question at the beginning of this column? In general, I believe that the best situation is to have cooperation between real-time operations organizations and IT organizations, each having a mutual respect for the experience and knowledge of the other group. The fact is, a great deal of what is needed to secure industrial automation systems comes directly out of the playbook used by IT. On the other hand, the SCADA folks have serious safety concerns and have devised processes and procedures that allow for safe support and modification of their systems.

By getting these two groups to engage in meaningful dialog and make a concerted effort to work together, you achieve the best of both worlds – and undoubtedly a higher level of security! There are team-building exercises that can help in making this happen… but perhaps that will be the subject of a future column. ■

About the Author

William T. "Tim" Shaw (PhD, CISSP) has been active in industrial automation for more than 30 years and is the author of Computer Control of BATCH Processes and CYBERSECURITY for SCADA Systems. Tim has contributed to several other books and is a prolific writer and presenter on a range of technical topics. He is currently a senior security consultant for SecuriCon, an information security solutions firm, based in Alexandria, Virginia. Tim has been directly involved in the development of several DCS and SCADA system products and regularly teaches courses for ISA (International Society of Automation) on various topics. Inquiries or comments about this column may be directed to Tim at *Tim@electricenergyonline.com*.


Jim Orr


Geoffrey Kempter

Improving Operational Performance Through Automatic Vehicle Management

By Jim Orr & Geoffrey Kempter
Asplundh Technical Services, Asplundh Tree Expert Company, Inc.

Since the federal government allowed public access to the satellite-based global positioning system (GPS) in the 1990s, innovation has led to a variety of uses. Fleet management is just one of many areas where this technology is proving to be highly beneficial. When combined with wireless communications technology, it is possible to continuously gather and report data from vehicles scattered across a wide area.

Over the past year, the Asplundh Tree Expert Co. has initiated a full-scale deployment of an Automatic Vehicle Management System (AVMS) to track the location of its assets. The system has already improved the safety and efficiency of Asplundh operations as it is being deployed incrementally across the enterprise. With its widespread, decentralized vegetation management and line clearance operations, Asplundh was, in many ways, ideally suited for deployment of a GPS-based system. However, the company quickly discovered that a suitable off-the-shelf system was not readily available.

Prioritizing the data and designing a system that would provide information in readily usable form were deemed critical success factors. Asplundh worked closely with Telogis (Aliso Viejo, Calif.), to design a system that could deliver critical operations information while minimizing cost and avoiding unnecessary complexity.

After completing several regional pilot projects, it was determined that the system significantly improved operational performance and the overall value of service delivered met or exceeded expectations. Much of this improvement is due to behavioral changes among field personnel, who are less likely to break rules (e.g., speeding), deviate from work plans, or take inefficient routes to and from work locations with the new system in place. The company has already installed over 7,500 units and is continuing to evaluate additional rollouts with the objective of having most of the fleet equipped and operational by the end of 2010.

How it Works

AVMS tracks vehicle location with a GPS receiver mounted under the dashboard of each truck. (A small wire antenna for the unit is attached to the windshield.) The GPS data, plus additional information about the truck, is collected every 15 seconds, and every two minutes the data is sent to a central computer server via a cell phone modem, which is located in the same box as the under-dash GPS receiver.

Once uploaded, the data is processed by remote software and can be viewed by any computer having Internet access. And, because it is Web-based, no special user software is required. This enables users to obtain a variety of information – both historically and in real time – about their operations.

A reporting hierarchy based on the manager's level of responsibility assures that only authorized personnel can access this information. For example, a general foreperson can access information about his/her area of responsibility but not that of other general forepersons. Likewise, regional managers can only obtain information about their own regions.

Choosing the Right Information

It's certainly no secret that information can be expensive to gather and interpret. An important part of designing an optimal AVMS program is identifying the most important information and then creating a system that will deliver that information in a format that is easy to use and understand. In this case, all levels of management use the system – from front-line supervision to executives – adding up to hundreds of people.


After his crews head out to their job sites in southeastern Pennsylvania, Asplundh Supervisor Jude Solis logs into the AVMS to track crew member progress. Among other benefits, the AVMS helps manage fuel costs and encourages working in a safer and more efficient manner.

Therefore, the system must provide efficient delivery of pertinent information in a way that would not waste valuable time at any level.

Initially, several data points that would provide the greatest overall improvement in the safety and efficiency of operations and that were obtainable without excessive cost were identified. These data points included:

- **Engine start/stop times**, to report when and for how long the main engine of a truck is running;
- **Pony motor (auxiliary lift engine) usage**, to report when the aerial lift is being operated;
- **Geographic zone alerts**, provided when geofencing boundaries are crossed (geofences are GPS-defined areas where access may be authorized or unauthorized depending on time and location);
- **Stops made** over the course of the workday;
- **Routes taken** to and from jobsites;
- **Total miles driven** over a given time period; and
- **Vehicle maintenance requirements** based on mileage and time.

Interpreting the Data

Though company personnel are highly skilled in crew and fleet management, until now many of the field management staff had only limited experience with this type of computer technology. Careful specification, prudent planning and close cooperation with the system supplier resulted in a user-friendly system that is capable of delivering key information quickly, accurately and efficiently and at a reasonable cost.

General forepersons now carry Wi-Fi equipped laptop computers that can access the Internet from most locations. As a result, the exact locations of crews are never in doubt.

Using the data points listed above, a map depicting the work history of any crew can be created – from the moment the truck starts in the morning until the crew pulls back into the yard at the end of the day, as illustrated in the map diagram, following.

This "breadcrumb" trail allows management to easily identify any number of problems, such as:

- Late departures and/or early arrivals;
- Deviations from scheduled work;
- Excessively long stops; and
- Misuse of equipment, such as speeding, excessive idling, or not enough use of the pony motor.

Each level of management is provided with information relevant to that particular operation. Maps that provide real-time locations or historical information can be obtained with a few simple mouse clicks. Alerts are provided for operations outside of expected norms, such as after-hours use or other geofencing violations, speeding or other pre-determined areas of concern.

Map of crew movement during one 24-hour period

Utility Interface

Utility personnel can also access the system via the Internet with a username and password. Much of the critical information, such as start and stop times and a "breadcrumb" trail, is available. Another key feature is the ability, with just a few clicks of a mouse, to find the closest crew to a trouble call and determine the best way for that crew to get from their current location to the trouble location.

Performance Benefits

Once the system was deployed and operational, Asplundh identified several operational improvements Crews move more efficiently, use less fuel, depart and arrive on time, complete more work, can be easily located by supervisors, and are generally more accountable for their performance. A more detailed explanation of these notable improvements appears below.

Reduced Fuel Usage: By monitoring crew location, supervision assures that drivers are following the most direct routes, thereby reducing miles driven (and, incidentally, time on the job). Monitoring the use of the main engine reduces excessive idle time, and maximizing use of the pony motor (rather than the main truck engine) to drive the aerial lift saves fuel.

Safety: Reducing incidence of speeding is one very important benefit. Asplundh can monitor the trends of individual drivers, and if necessary discipline those with excessive speeding alerts. Additionally, in the event of a crisis, the location of the crew is always known, and aid can be rapidly dispatched.

Using GPS and wireless technology, AVMS helps Asplundh know exactly where a vehicle is located, even during "off-road" status. This can help expedite a response to a trouble call, storm emergency or medical problem.

Improved Start/Stop Time: With widespread operations it can be difficult to be at every start and stop location every day. Through geofencing, supervision can be alerted if a vehicle departs late or arrives early at a parking location.

Monitor & Assist with Efficient Routing: Trucks can be routed more efficiently, traffic bottlenecks can be averted, and crews with multiple work locations in a single workday can be provided with turn-by-turn directions to jobsites.

Eliminate After-hours Usage: Obviously, trucks should only be used for company-authorized work. Engine start/stop and geofencing allows supervision to be alerted via email and text message if a truck is started or moved after hours.

Storm Management: Storm response is an area where AVMS is proving exceptionally useful. Crews moving to remote locations can now be tracked from deployment to destination, even over hundreds of miles. Once on the job, routing and scheduling can be accomplished far more efficiently.

Areas of Concern

As with any significant change, some pushback is inevitable; indeed, both management and crew personnel have expressed concerns. However, most employees have quickly adapted, while most of the expressed concerns underline the need to adapt to changes in routine operations. Some of the specific areas of concern were…

Learning Curve

This type of technology can be intimidating to learn and usually results in the need to change individual habits, some of which may be deeply entrenched. Even with the ease of the computer interface, learning how to obtain, interpret and ultimately use the data can be difficult for some people. To help offset this reality, the AVMS program was rolled out in phases, assuring that each region was able to obtain the necessary training and administrative support during these critical early learning stages. Then, as additional units were installed, experienced personnel were available to assist as needed.

Workforce Acceptance

The notion that "Big Brother" is watching is also intimidating and requires a period of adjustment for some employees. To assuage those concerns, the program rollout was accompanied with information for crew members, emphasizing safety and asset management as the key reasons for deploying the system. Most employees quickly realized that the company was not asking them to do anything other than what they were already expected to do as part of their job, and as a result, they ultimately welcomed the opportunity to help improve overall performance and customer satisfaction.

Technological Limitations

The selected system operates only where both satellite and cellular communications services are available. Fortunately, this includes the vast majority of areas where the company typically has crews deployed. However, in certain remote areas, weather and terrain can sometimes compromise coverage. As communications technology improves, the system will need periodic upgrading, though it is anticipated that the current technology should be adequate for several years before any major upgrades are required.

Conclusion

AVMS has proven beneficial in the areas where it has been deployed. It has allowed better management of key company assets, including vehicles and personnel. Total miles driven have been reduced, and overall operational efficiency has improved. Moreover, crew members are more likely to drive safely and comply with established driving rules. The company has every reason to believe that improvements will continue as the system is deployed in additional areas.

One challenge will be assuring that management and crew personnel continue to maintain high standards of performance rather than finding or creating ways to circumvent the technology. However, there has been no evidence of such behavior thus far.

The introduction of new technology can sometimes fundamentally change how organizations are operated and managed. Considering the value of the truck fleet and its importance to the performance of daily operations, AVMS is proving to be a technology that will bring about change for the better, both in the short term and over the longer term as well. ■

About the Authors

Jim Orr is Vice President, Asplundh Technical Services, and heads up the task force that is deploying the AVMS system for the Asplundh fleet. He is a past president of the Utility Arborist Association and is a recognized expert in utility arboriculture. He has been instrumental in advancing research efforts and applying new technology to improve operations.

Geoffrey Kempter, Manager, Asplundh Technical Services, provides customer service, training and other support of Asplundh field operations. He serves on the ANSI A300 Standards Committee, chairs the ISA Certification Board and is the author of "*ISA Best Management Practices Guide for Utility Pruning.*"

Bridging the Knowledge Gap to Identify Energy Theft

By Michael Madrazo, CEO, Detectent

Energy theft has become big business for thieves – racking up losses for utilities totaling an estimated $6 billion annually. It is a serious financial issue as well as a major public safety concern. In today's economy, most utilities find themselves struggling with increasing theft occurrences, realizing that no territory is immune, and no service is safe from theft. With a little knowledge and a little nerve, or the right contractor, anyone can tap into electric, gas, or water services.

The majority of theft occurs in the residential sector, but the majority of revenues lost to theft — estimated at between one and three percent of total distribution revenues — occur in the commercial account sector. A utility with $1 billion in revenues potentially loses between $10 million and $30 million each year to theft, and the majority of the lost revenue is to a relatively small number of commercial accounts.

Traditionally, the utility has relied on meter readers and service personnel for tips on energy theft. Meter readers, visiting each meter every month to collect a reading, made for a very effective line of defense against theft. With the advent of Automatic Meter Reading (AMR) and Advanced Meter Infrastructure (AMI), the manual task of meter reading is being phased out and replaced by electronic readings so the utility has lost its eyes and ears in the field. No one is keeping an eye on the utility's cash register.

Automated Meter Reading systems provide tamper flags that are designed to identify energy theft when the tampering occurs at the meter, and while they can alert the utility to tampering, they also trigger far too many false alarms. According to a Chartwell research report, "AMR is not a perfect system for detecting theft and many customers have discovered this, coming up with clever ways to bypass or tamper with the meter without triggering a tamper flag. Plus, some of the utilities consulted for this report say tamper flags do not always indicate theft, but are a product of oversensitivity and benign outside forces."

Unfortunately, tamper codes are often triggered by valid field activities or external forces and so valid flags are lost in the myriad of false ones. As a real-life example, a utility with 128,000 electric meters on a fixed network AMR system received over 1,600 tamper codes daily. Clearly, there is a need for a way to use the valuable information supplied by the automated meter reading systems in an efficient and intelligent way. But harnessing the flow of tamper flags is just part of the solution. A broader more encompassing solution is required if the utility is going to safeguard itself against all forms of energy theft. The complete solution requires the utility to understand how each of their customers uses energy and focus on those that deviate from expected usage patterns.

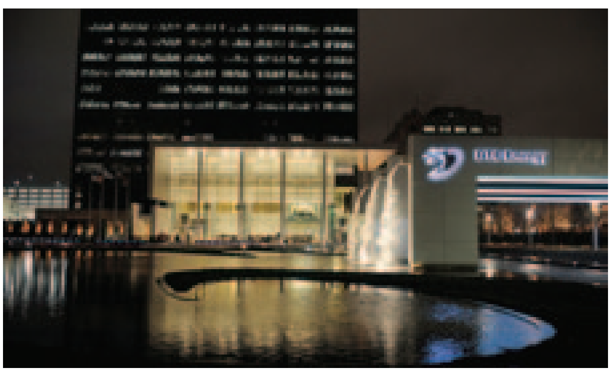
Know Thy Customer

Knowing the customer is vital. Typically, utility data consists of the account holder's name, phone number, address and for commercial accounts, type of business and maybe the name of the business. The utility may know a client account is a restaurant, for example, but probably doesn't know how large the premise is or whether it's a sit-down or take-out establishment. For commercial accounts, additional information such as the number of employees, chain affiliation and other metered services on the account need to be a part of any intelligent usage analysis. For residential accounts, knowledge of the size of premise and heating and cooling sources is also very valuable.

Understanding the characteristics of an account provides valuable insight into the customer's use of energy. With this insight, energy usage can be compared to a group of "like peers" with similar characteristics and outliers can be flagged for further analysis and investigation.

The process of detecting theft analytically can only truly be accomplished once multitudes of characteristics of an account are identified and proper peer grouping is done. Useful data for analysis includes:

- Usage from other meters for the same service type on the account
- Usage from other metered services
- Correct business codes
- Square footage
- Business information such as number of employees and hours of operation



Case in Point

Detroit Edison has been addressing energy theft issues since the 1930s - the difference today is the magnitude of the problem. With DTE Energy serving over 3.4 million customers, deploying the right technologies and processes to combat theft is crucial. "First and foremost addressing energy theft is important to DTE Energy due to the potential safety hazard it creates. This illegal activity can create safety hazards for both the residents at the location engaged in the theft and those in the surrounding neighborhood should an explosion or fire result," said Mark C. Johnson, revenue protection manager for DTE Energy. "Product losses can also impact DTE Energy's earnings and the rates paid by our customers."

As part of stepping up their efforts to combat theft, the utility is now utilizing sophisticated Customer Intelligence Solutions from California-based Detectent, Inc. By complementing DTE Energy's revenue protection processes with Detectent's peer analysis and characteristic analysis, DTE Energy is able to identify a wider spectrum of theft cases.

Using information from many sources, advanced analytics and proven processes, utility resources can focus on cases that have the highest likelihood of uncovering theft and the maximum potential for revenue recovery. This repeatable process allows DTE Energy to collect more revenue and obtain more intelligence about their customers, year over year. The result is a more efficient use of back-office and field resources and increased revenue.

Customer Intelligence

Utility customer data can be significantly enhanced and improved by acquiring third-party data and integrating it using sophisticated pattern matching algorithms. Correct business codes as well as a myriad of additional premise and operational information can be gathered and thereby dramatically extend the known customer information for each account.

Energy theft detection models generally fall into two categories: peer comparison and characteristic analysis. Peer comparison models contrast all available information about residential and commercial customers to similar homes and businesses within similar geographical and environmental settings. Deviation from expected usage can indicate that not all the energy used by a customer is being metered correctly. Characteristic analysis looks for anomalies in a customer's consumption pattern that might be indicative of un-metered equipment in an account.

For example, you can expect a Laundromat to have a relationship between electricity consumed by washing machines and gas consumed by dryers. If one service is not metered to the expected ration of the other, then it may be indicative of one of the services not being metered correctly or having been tampered with. When combined, these two types of theft detection models can monitor for adherence to peer usage and micro-analyze energy usage for expected characteristics.

Proper Analysis is Key

Analysis on its own does not totally replace the need for the common sense and intuition that people bring to an equation. So even with all of the known data captured and analyzed, a review of all available information needs to be done in order to confirm that the indications of energy theft are not in fact simply the work of other outside forces. For example, one needs to consider if demographically, the area has declined, or if the business is going through renovation or other legitimate changes that might lead to a deviation from the expected normal usage.

resources can expend energy where the payback is likely to be the highest. Unlike simpler query tools, the energy theft detection solutions that have emerged in recent years have the capability for organizing cases in order of value and probability so that both back office and field resources are used most efficiently. For commercial accounts, this might be accomplished by determining:

- Average consumption compared to the capacity of the installed meter(s)
- Ratio of one service's consumption to that of another
- Degree of deviation from expected normal values

Using many data sources and a combination of models that look for independent features in a customer's consumption profile have transformed theft detection into a viable and cost-effective solution for utilities. Previous attempts to analytically identify energy theft resulted in marginal improvements over past practices and typically were not cost effective. The newer solutions, which have emerged only in the past three to five years, have significantly increased in cost effectiveness.

To illustrate this point, a recent case featured on Fox-TV in North Carolina involved a large restaurant that was paying for about 1000 kilowatt hours of electricity on average, per month. In reality, the restaurant was consuming in the range of 10,000 to 12,000 kWh per month. The average monthly bill that the customer was paying was in the range of $150 to $180 while the amount should have been at least $1300 to $1500. This had been the case for more than eleven years.

The cause of the problem was a wiring fault and not an actual theft. But did the customer know that he was underpaying? Did the proprietor know that something was amiss after the monthly electricity bill miraculously dropped by 88% in one month and then stayed at this much lower level?

One can assume that the proprietor did in fact know that the bill was far too low, but chose not to draw attention to it. The case came to light in the summer of 2009 after the utility deployed an analytic theft detection solution from Detectent and began making use of peer comparison and characteristic analysis. The account, once other external data was gathered and matched to the information from the utility's Customer Intelligence System, was compared to a group of similar restaurants and immediately jumped to the forefront.

The utility corrected the problem in the field, recognized the loss of over $171,000 and billed the cost for 12 previous months of unmetered usage to the amount of $15,869. Although significant revenue was unfortunately lost and ultimately passed through to the ratepayer base, the utility has avoided future losses by identifying and correcting this situation.

Compare, Contrast and Learn

With an analytical approach to energy theft, it's important to know that no one analytical model stands alone. Numerous models need to run in parallel in order to evaluate an account's energy usage from a variety of angles and flag anomalies based on different forms of assessment. Today's energy theft detection systems do just that and therefore go well beyond the utility's traditional high/low and zero-consumption reports.

Deploying an energy theft detection solution is not only important to the future of a utility with an AMI or AMR deployment; it is also critical to traditional utility operations. Economic conditions have caused utility customers – both residential and commercial – to act in ways and do things that they have not done in the past. All indications are that energy theft in both the residential and commercial sectors is rising rapidly across the country. As well, with revenues dropping from reductions in industrial energy usage, remediating theft conditions and other conditions causing revenue loss can be a valuable stream of revenue to the utility.

As with the restaurant example above, only by truly understanding the customer and how they use energy can utilities expect to detect cases of theft and other forms of revenue loss. Utilizing sophisticated customer intelligence tools, today's utilities can identify and reduce future revenue losses by analytically and proactively protecting their power delivery networks from tampering, malfunctions and theft.

About the Author

Michael Madrazo is the founder and CEO of Detectent, the pioneer in delivering customer intelligence for utility business decision support. He has over 25 years of providing complex analytical software solutions to the utility industry.

Helping utilities attain sustainability through 'Green IT'

By Maureen Coveney, Industry Director and Senior Principal, Utilities Industry, SAP AG

A huge green economy has been developing for the last few years. In 2006, for example, renewable energy and energy efficiency technologies generated 8.5 million new jobs, nearly $970 billion in revenue, and more than $100 billion in industry profits. Then, in December 2007, former President George W. Bush signed the Green Jobs Act to train workers for green collar jobs, authorizing $125 million for workforce training programs targeted to veterans, displaced workers, at-risk youth, and families in extreme poverty.

Now, nearly two years later, energy and natural resource efficiency is timelier than ever since current President Barack Obama signed the American Recovery and Reinvestment Act (ARRA) which includes more than $11 billion to create a bigger, better, smarter electric grid. The combined total of these investments will allow for the integration and use of greater amounts of renewable energy, increased utilization of innovative efficiency technologies, and a reduction in the electric congestion that costs consumers billions of dollars each year.

So, amid the challenges facing the U.S. and global economies, a critical opportunity exists to expand prior initiatives and further develop the industries and skilled workforce needed to support a transition to a clean energy economy. The ARRA will create a sustainable, public program that leverages significant private labor-management funds and provides more quality workforce training linked to good jobs that are created by federal renewable energy and energy efficiency initiatives.

However, natural resources continue to become increasingly scarce and expensive. Thus, utilities need to take better control of their business processes to optimize energy and natural resource consumption of enterprise-wide operations (IT data centers, for example) and protect profitability in light of economic volatility.

The dual role of IT

So, like any other industry, IT must also step forward and make itself "green". Green IT – the reduction of energy use in data centers – can help utilities use a sustainable approach and optimize resources at every stage of the lifecycle: manage (not only account for) carbon emissions; anticipate and meet stakeholder expectations with transparency; and actively engage employees, customers, and partners in these efforts essential to economic and programmatic goals of the entire economic stimulus effort, including in the latest innovations such as advanced metering infrastructure (AMI) and Smart Grid.

Faced with challenging and complex business processes to address sustainability, utilities, like other companies, need – and want – a consistent and integrated business process to address sustainability initiatives. There's greater opportunity in sustainable business practices to:

- Reduce cost of compliance and reduced business risk in the face of proliferating local, regional, and global regulation in the areas of people, health, and safety, product safety and stewardship, and environmental compliance. A utility can leapfrog the competition by embracing consistent practices across the business network for competitive differentiation.
- Protect and enhance brand value, market share, and market capitalization by employing best business practices in sustainability performance management, including risk management and strategy management, and effectively engaging all relevant stakeholders with visible and accessible analytics.
- Optimize energy and natural resource efficiency of a company's manufacturing processes for reduced cost and emissions, such as leveraging AMI solutions to optimize customers' energy consumption.
- Measure, mitigate, and monetize greenhouse gas emissions and other environmental impacts across internal operations and the supply chain.

Using a viable software solution, utilities and their customers can reduce the cost of maintaining a comprehensive carbon emissions inventory, manage regulatory changes, and enhance brand value by providing transparency into sustainability initiatives.

- Establish Green IT practices to architect and deliver business processes in the most energy-efficient way possible, for example, creating an environmentally sustainable data center and IT operations that reduce costs, while improving process quality.

However, most utilities already use robust meter, network, and customer service infrastructures designed to support processes and systems for well-defined work routines and functions. Yet in many cases, they use conventional meters with life cycles of up to 40 years – devices that worked well when energy markets were largely regulated and characterized by price regulations, easy access to energy resources, and sufficient infrastructure capacity. In that environment, organizations could rely on manual processes for everything from checking meter readings to determining future demand for electricity, without as much concern about margins, ensuring customer retention, energy efficiencies, and sustainability.

But changes in the utility industry in recent years are making it increasingly difficult to compete using traditional infrastructures and processes. Resource and infrastructure capacities are becoming more marginal, while large commercial and industrial utility customers are curbing demand for electricity in response to the challenging economic environment. Then there's a heightened focus on reducing carbon footprints.

In addition, in some parts of the world, new legislatively mandated market rules demand that utilities compete for customers on the open market, so utility executives must find new ways to differentiate their services and capture additional revenue while increasing operational efficiency. And, because customers can switch retailers relatively easily – especially in electricity markets – utilities need innovative processes to improve sales and customer service performance.

The reality is that current assets are aging, and a more adaptable infrastructure is needed going forward. For the near term, utilities must optimize current asset efficiency and availability. Downtimes must be limited to planned shutdowns and necessary overhauls only. Stringent maintenance processes can help ensure high levels of equipment reliability. Additionally, proactive planning can establish a stable, environment where resources such as personnel, contractors, parts, and tools can be optimized.

Future increases in bulk transmission capacity, however, require significant improvements in transmission grid management. A smart grid, for example, can upgrade the use of capital assets while minimizing operations and maintenance costs. Smart grids precisely limit electricity power down to the residential level. Optimized power flows reduce waste and maximize use of lowest-cost generation resources.

But how can utilities – and consumers – better understand and manage energy use and become "greener"?

Technology leads the way

Because technology in itself is seen as a critical enabler for implementing the Economic Stimulus Plan, with approximately $100 billion in funding to be spent incrementally over the next five years, it can help utilities see, think, and act more clearly as they develop and execute the necessary strategies to:

- **Optimize energy efficiencies.** New energy-grid technologies can help utilities balance supply and demand while improving the efficiency of energy delivery and consumer usage. These metering and data-exchange systems, however, require real-time communications and greater system interoperability.
- **Respond to sustainability concerns.** Increasingly, the adoption of sustainable energy practices is becoming a business imperative.

Today's utilities are challenged to take a holistic approach to sustainability that simultaneously addresses compliance, globalization, environmental impact, and energy politics. Visibility into all aspects of a utility's operations and end-to-end process control are keys to success.

- **Develop higher-performing assets**. Managing today's aging infrastructure for peak efficiency while making the energy investments that will deliver maximum value tomorrow are basic tenets of the stimulus program. Utilities must be able to maintain existing equipment, model current and future assets, and analyze complex energy scenarios.

Technology and demand management

With regard to optimizing energy efficiencies, AMI technologies can help utilities and consumers alike better understand and manage energy use. With AMI, energy consumption is recorded at regular time intervals (e.g., every 15 minutes) and then billed at different rates based on peak and off-peak hours. As a result, consumers and suppliers can collectively lower overall energy requirements and reduce carbon emissions.

With these technologies, energy providers can improve the balance between demand and supply. The data collected through AMI helps utilities better profile energy requirements during both peak and off-peak hours and predict energy usage spikes due to environmental changes. Smart-grid technologies are also supported. These improve the delivery of energy by providing greater control over load shedding, energy leakage, and outage management.

AMI technology can also help utilities stay competitive in ways that older metering and data-exchange technologies simply cannot. But without a proper IT infrastructure that enables companies to implement and work with AMI in a cost-effective manner, utilities find it difficult to deliver the flexible pricing options that the market demands. AMI requirements for data management and real-time information exchange call for improved communications and collaboration between customer and utility. It also requires far greater interoperability of systems within the utility's IT landscape and across enterprise boundaries.

Upgrading metering and data-exchange infrastructure can increase the quality of a company's sales and customer service processes. In addition, automated business-control processes can help utilities management the variations between peak and off-peak production, thus reducing the overall cost to serve while lowering the cost per kilowatt-hour.

Take, for example, Michigan-based Consumers Energy, the principal subsidiary of CMS Energy. The utility, which provides natural gas and electricity to nearly 6.5 million of Michigan's 10 million residents in all 68 Lower Peninsula counties, found that its consumers were using eight percent more electricity than a decade ago. So, Consumers Energy decided to become an early adopter of the latest smart metering software that will help the utility improve efficiencies and provide customers with timely information to help them better manage their energy usage. With this installation, Consumers Energy is also creating a platform for a future smart grid and the automation of manual processes.

The path to cleaner energy

As other utilities follow Consumers Energy's example, the thirst for energy continues to grow around the world, even as traditional sources of energy generation, such as fossil fuels, are waning. And this consumption contributes significantly to climate change and other environmental concerns. A major obstacle utilities face today is how to migrate cleaner, "greener" technologies in a cost-effective and time-efficient way.

Over the last few years, the global business climate has fundamentally changed. Protecting the environment is no longer simply a philanthropic or moral issue, but a highly relevant element of the core business. However, the primary factors driving businesses to adopt sustainability are compliance with government regulations such as the U.S. Clean Air Act; cost and profit consdierations, which drive companies to reduce costs through more efficient uses of resources; and reputation, which means companies are redefining their respective brand images to demonstrate social and environmental responsibility, and therefore, appeal to an increasingly concerned consumer base.

The push for sustainability is being seen across all levels of government and in every economic sector. For example, many U.S. Environmental Protection Agency initiatives are underway to promote more efficient energy use and to improve environmental quality without disrupting energy supplies. These efforts include programs to explore renewable energy sources and advance the sustainable production of biofuels.

Federal agencies are also helping states and local communities foster urban sustainability by supporting such initiatives as:

- Smart-growth projects that include sustainability metrics for urban development;
- Green building and infrastructure design; and,
- Energy efficiency in homes and commercial buildings.

Businesses can take a proactive approach as well. Many companies now participate in international committees working on global standards for calculating environmental impact. The Greenhouse Gas Protocol Initiative (GHG Protocol Initiative, Scope 3), for example, is drawing up a set of standardized guidelines for measuring carbon dioxide emissions for individual products and services – an initiative that has the support of the World Resource Institute and the World Business Council for Sustainable Development.

Transforming energy transmission

With utilities maintaining and/or retooling aging infrastructures to make them more adaptable to advanced technologies, utilities need to address assets in the future context.

Harmonizing local distribution with inter-regional energy flows and transmission traffic can further reduce grid congestion and bottlenecks, ultimately resulting in consumer savings. Such improvements can help create an open marketplace where alternative energy sources from many distant locations are sold easily to consumers wherever they are located. Intelligence in distribution grids can enable small producers to generate and sell electricity at a local level using alternative sources, such as rooftop photovoltaic panels, small wind turbines, and micro-hydro generators.

However, intermittent power sources require sensors and software designed to react instantaneously to imbalances to ensure system quality with such distributed generation strategies. In additional, operators and managers must have the right tools to effectively and efficiently operate a grid with an increasing number of variables. Technologies include visualization techniques that reduce large quantities of data into easily understood visual formats, software that provides multiple options when operator actions are required, and simulators for operational training and "what-if" analysis.

What lies ahead

As utilities develop and execute the necessary strategies that can help them see, think, and act more clearly to wisely spend the approximately $100 billion in economic stimulus funding over the next five years, they need to execute those strategies decisively and effectively to endure the current environmental conditions and emerge in a stronger, more competitive stance. To gain this clarity, utilities need visibility to refocus business strategies and streamline operational execution and transparency to demonstrate compliant and sustainable business practices.

Such "clear" utilities understand what is going on in every aspect of their business and business networks. They operate with increased speed, relevance, and accuracy. They are prepared for risk and uncertainty and can adjust operations nimbly as market conditions change. In short, they are transparent and accountable, lean and agile, and customer-centric and collaborative.

Emerging as such an enterprise improves every aspect of managing a utility and helps it survive and thrive -- not only in the near term, but also over the long haul. Sustainability, for example, presents both significant risks and new opportunities to improve profitability. But being sustainable is more than just knowing a carbon footprint. It requires real-time knowledge of the business and business network as well as having the confidence to share this information with customers, stockholders, and other stakeholders

So, if a utility is just beginning a sustainability plan or tweaking an existing one, the following steps may help it get the most from these efforts:

- **Assess the organization and make a plan**. Get a basic understanding of what a business case for sustainability for the utility must comprise. It should combine social, environmental, and economic considerations. With that basic understanding, a utility can see where opportunities exist for improvement and be most effective.
- **Measure business activities**. Set a baseline of data for current activities to know when and where improvements are being made. Include the utility's network of partners and suppliers in the measurement process to increase the footprint of the efforts. Customers and their usage can also be included.
- **Take action**. Execute the plan and measure every step, which includes involving employees in engagement programs, thereby making them part of the effort.
- **Monitor and adjust**. Learn from experience and look for additional means of achieving sustainability throughout the utility and its ecosystem.

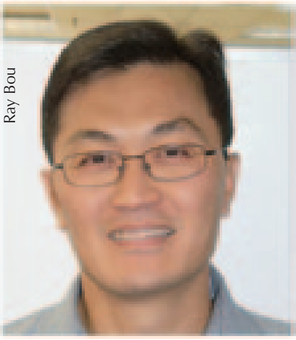
With broader insight, and more flexibility, utilities will act with greater efficiency and sustainability to face whatever challenges this dynamic environment brings. But the journey toward a sustainable future has only just begun – and green IT is but one logical step along the way. ■

About the Author

Maureen Coveney is Industry Director and Senior Principal for the Utilities Industry for SAP AG, headquartered in Walldorf, Germany.

Amy Hime

Ray Bou



Smart Technology for a Smart Utility: Enersource Simplifies Operations Center with Smart Grid Solution

Integration of utility's data into unified smart grid command-and-control environment increases efficiency and provides more reliable power

By Amy Hime, Manager, Engineering and Asset Systems, Enersource Hydro Mississauga and Ray Bou, System Control Manager, Enersource Hydro Mississauga

Enersource is one of the largest electricity distributors in Ontario, Canada, among 82 municipally owned utilities. The utility has a history in Mississauga that stretches back to 1917 with the creation of Toronto Township Hydro. Prior to 1974, the core of Mississauga was known as Toronto Township. With the formation of the City of Mississauga in 1974, Toronto Township Hydro was renamed Hydro Mississauga. Today, Enersource Hydro Mississauga Inc. is the regulated affiliate of Enersource Corporation, serving more than 187,000 customers with an electrical system that spans over 5,000 kilometers.

Enersource Hydro Mississauga focuses on quality of service for the distribution of electricity, delivery of electricity conservation programs and smart metering solutions to meet provincial government objectives. The utility has gained a national reputation for excellence during the more than 90 years it has serviced the local community and is well known for its reliability, customer satisfaction and reasonable costs.

On the reliability front, Enersource's total duration of service interruption per customer consistently performs well above the Canadian utility average. In 2008, Enersource experienced only 19.7 minutes of customer service interruption, which is considered outstanding for the sector. Enersource credits its critical infrastructure investments and strategic engineering focus with raising its reliability performance dramatically from the previous year, making 2008 one of its best years on record for providing world-class reliability to customers.

Customer satisfaction survey results are another success indicator of Enersource's continuous dedication to improving infrastructure and operations. A recent survey indicated that 90 percent of Enersource Hydro Mississauga's customers are satisfied with their service.

Enersource Hydro Mississauga crews work around the clock to uphold their track record of exceptional reliability and service.

With the goal of continuing its track record of success, Enersource is looking to the future, examining the development of distributed generation to add capacity to the Ontario supply mix and driving the conservation agenda to overall reliance on cleaner power generation.

Enersource and the province of Ontario as a whole possess a strong record in pioneering energy efficiency and conservation programs. A major driver of these efforts, Ontario is taking progressive and proactive action in the smart grid movement. While utilities and municipalities around the world are embracing the smart grid as a means of supplying more energy without further depleting the earth's resources, Ontario is on the cutting edge of this movement, mandating that all homes and businesses in the province are equipped with smart meters by 2010.

To date, Enersource has installed over 135,000 residential smart meters, and the remaining residential installations will be completed in 2010. Enersource was also one of the first local distribution companies in Ontario to complete system testing to support smart metering for small Commercial and Industrial (C&I) customers.

In addition to smart meters, Enersource has also turned to other key technologies to provide affordable, reliable service to customers while playing a significant role in Ontario's energy conservation efforts.

The company purchased its first geographic information system (GIS) in 1989 to effectively store, track and manage its assets. Today these assets account for 920,000 distribution transformers, utility poles, meters, conductors, network devices, sensors, municipal substations and other items.

In 2008, Enersource realized it needed to supplement its asset management system with a more efficient method of controlling its grid. At the time, the utility used various software products and computer consoles to manage all operations. Operators used different applications for GIS, supervisory control and data acquisition (SCADA), internal work processing and many other day-to-day electric grid management activities.

This required operators to switch among multiple systems in the control room, which increased the complexity and time required to monitor and analyze data. Having to enter information on the various overlapping systems also increases the chance of having inconsistent records.

As a result, Enersource was looking for a way to provide system operators with a consolidated user environment for all control room applications. The utility wanted to leverage its GIS data so all users could have easy, digital access to information on its hundreds of thousands of assets. This would speed the elimination of paper wallboard maps and manual processes, and streamline the flow of information across the utility.

Control room operators face further complexity as advanced smart grid technologies become more widely deployed. Smart devices generate more data points for grid operators to monitor and analyze, making it difficult to obtain a clear view and quickly make critical decisions. Enersource decided to implement a solution combining Intergraph's Smart Grid Operations Command-and-Control Center and Siemens' Distribution System Power Flow (DSPF) application to create an Integrated Operating Model (IOM). The IOM's wide range of analysis tools would make use of this ever-increasing volume of data to predict and recommend actions to the operators.

These technologies provide Enersource with the power to easily visualize the grid through a single user interface for faster, more informed decision-making. With the combined IOM capabilities, Enersource staff will have immediate information about load and voltage conditions to help them more safely, quickly and reliably reconfigure their networks and restore power.

Enersource's Integrated Operating Model (IOM) provides a clear, consolidated view of the electric network and infrastructure for faster, more informed decision-making.

The capability to easily leverage existing GIS data in the IOM was a key deciding factor in implementing the solution. Additionally, the long-term success, open architecture, flexibility and scalability of the solution set and the inclusion of outage management and mobile workforce management functionality as well as GPS tracking of field crews were also differentiating factors in the selection process.

The availability of commercial-off-the-shelf interfaces to customer information, interactive voice response and advanced meter reading systems completed Enersource's list of requirements, all met by the combined Intergraph/Siemens solution.

Enersource divided the project into two phases. During the first phase, the company implemented the outage management system (OMS), a key foundation for the Smart Grid Operations Command-and-Control Center. This allows the utility to use existing GIS information with the OMS software and provides enhanced functionality for trouble analysis, call-taking and network management, combined with status notification of changes to SCADA-controlled devices.

Specifically, the IOM allows Enersource to analyze trouble calls in real time and determine the device most likely causing an outage, as well as quickly view information about crews and their current status and pending and active jobs, among many other activities. Enersource successfully launched the first phase of the IOM in September 2008.

The project's second phase involves SCADA device control and operation, SCADA alarm management, automated switch planning and the integration of load flow analysis with power distribution software acting in concert with the OMS software. This unified command-and-control environment provides easily visualized, actionable intelligence in the form of alarms, events, work orders and other routine activities, allowing for quick detection and remediation of outages and other potential issues.

Implementation of the IOM is due to be completed in July 2010. By streamlining the work of Enersource's system operators, it will help the utility work more efficiently under both normal and storm conditions, as well as ensure that its back office and field crews have the most up-to-date and accurate information.

The Integrated Operating Model (IOM) will improve communication between the control room and field crews, allowing for safer, more efficient operations.

The robust system will allow Enersource to fully leverage its GIS system and enable the utility to model equipment not typically possible for OMS-type applications, which provides a more complete data model for analysis and will enable Enersource to fully use the system through reporting and add-on applications. Overall, the IOM will result in more reliable power for Enersource customers and improved safety for both employees and customers.

"The City of Mississauga has grown from 170,000 residents just 40 years ago to over 700,000 today," said Craig Fleming, President & CEO of Enersource. "This rapid growth challenged our ability to track the location and state of our field assets. GIS and smart grid technology have given us the tools to improve efficiency, safety and reliability."

In the future, Enersource plans to continue leveraging technology to provide more users throughout the company with geospatial data and access to the smart grid system.

"The implementation of the IOM has provided us with a good foundation to help meet the growing energy demands of tomorrow without sacrificing the excellent service and safety Enersource is known for," added Raymond Rauber, Vice President of Engineering and Operations with Enersource. "Utilizing state-of-the-art integrated solutions allows us to keep building on a quality platform that provides our utility with the confidence to deliver reliable electricity for customers now and well into the future."

Before too long, all utilities operating around the world will need to embrace smart grid strategies to survive in the future. Increasing energy demands, diminishing resources and rising environmental concerns will force all energy suppliers to seek out innovative means of serving customers and protecting the planet.

Enersource and the province of Ontario are taking proactive, pioneering steps to guarantee future success and the continued satisfaction of their customers. As more advanced technologies are incorporated into the grid, the amount of data flooding into the control room will become unmanageable without solutions that consolidate and filter the data through a single interface, creating a clear picture of actionable information from which operators can make intelligent decisions.

About the Authors

Amy Hime is currently the Manager of Engineering & Asset Systems at Enersource. Her invaluable experience with the AM/FM/GIS system dates back 20 years, and she has been in the privileged position of managing the implementation of a leading edge Integrated Operating Model for Enersource.

Amy manages the Corporate Records & Mapping department, which maintains the AM/FM/GIS system database that houses information about 920,000 items of plant and geographical items. She oversees the maintenance of electronic systems related to equipment, drawings and legal agreements, and provides security and access to 48,000 electronic and 700,000 microfiched documents.

Ray Bou, P.E., is currently the System Control Manager of Enersource Hydro Mississauga. He oversees the 24/7 system control center, from which daily operational activities are dispatched. Prior to this role, he was a Project Engineer working on the various aspects of Enersource's Integrated Operating Model project from design specification to project launch.

Ray has also managed a SCADA support team to maintain and support the SCADA system. Other notable projects include managing the protection and control and communication on the high voltage rebuild as well as the protection and control of the co-generation interconnection for the Greater Toronto Airport Authority. Prior to joining Enersource Hydro Mississauga, Ray worked in the Operations Department of Toronto Hydro, providing engineering support.

How Equipment Reliability Guides Maintenance

By Gay Gordon-Byrne
Vice President Technology & Development TekTrakker Information Systems, LLC

As utilities integrate new technology into their grids and communications links, the challenges of keeping equipment in service (i.e., maintenance) will fall hard on the unprepared. So what should managers and planners expect when "… meters are no longer meters but computers with metering applications?" – Joe Rigby, CEO & Chairman, Pepco Holdings, Inc.

SmartGrid and AMI projects are deploying electronic equipment with very little history of reliability to support service projections. Useful life is being calculated by accounting rules instead of being informed by field experience. Reliability is assumed by planners to be sufficient, but there is no empirical support. Each utility is testing and piloting new devices focused on proving that SmartGrid connections can be made to function, but without regard to the difficulties and costs of keeping millions of computers functioning in the field.

Experience with similar devices deployed in other industries already shows that concerns should be high. The most reliable of current electronic devices do not approach the stability of the old brass and glass meters they must replace. Unless utilities are extremely careful, the hidden service requirements of many AMI and Smart Grid items will easily exceed the savings potential promised in many project proposals.

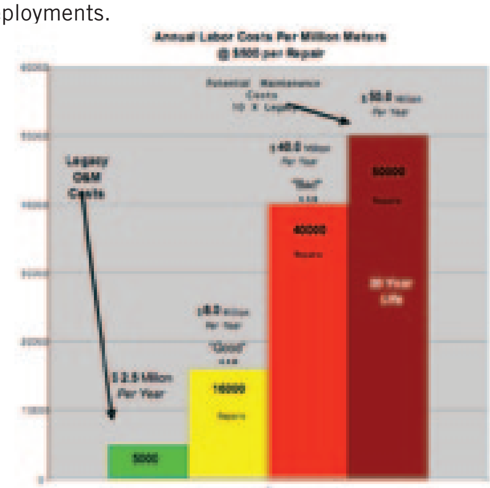
The dilemma is that utilities need to know in advance of massive deployments how well their selections perform in the field, yet all are exploring new options simultaneously. The best and most effective way to approach this information gap is to utilize the information already being collected internally by operations and maintenance departments. Tracking and reporting of repair and service issues from the maintenance teams informs the broader business and forms the backbone for improved decisions. So here are a few tips on how to take the guesswork out of the process and start making decisions based on reliable information instead…

Action Item # 1 – Calculate Current Maintenance Burden and Costs

Determining the reliability of existing products is fundamental to being able to evaluate the relative improvements that will come from deployment of new products. Planners need to be working with Operations and Maintenance departments to quantify the important baseline of current reliability and costs.

From an equipment maintenance perspective, the definition of a reliable product is one that never needs adjustments or attention. Calculating the failure rate or repair rate is therefore, a direct measurement of reliability. Once the failure rate is calculated, all new equipment choices can be compared empirically and cost projections made effectively.

Unlike the costs of initial installation, repairs of any size are costly to the organization because they arise unexpectedly; need relatively quick attention; exercise the customer service, problem reporting, and supervisory systems; and always involve warm hands (labor) to resolve. A truck roll to replace a $5 battery is just as costly as a total meter replacement. The price of the part itself is often inconsequential compared with the labor to resolve the problem. It is the impact of hundreds of thousands of relatively low-cost items requiring high levels of repair attention that can quickly unravel the business case for deployments.



In the chart below, we compare various metering product types and their general failure rates in multiple formats. We used a total cost per repair of $500 as the basis for this chart to illustrate the impact of small repairs on the overall budget. The important concept is to grasp the very wide differences across various products and appreciate the cost impact to the organization of supporting the maintenance of the poorly performing products.

This chart shows current standard meters with their industry "standard" failure rate of 0.5% as the starting point. Each of the new types of AMI meters is compared to the old style, each resulting in very different costs to maintain the same quantity of equipment.

Use Failure Rate to Project and Compare Products

Armed with the failure rate of any product, managers can project both the quantity of failures that they are likely to experience as well as the types of parts that they should stock and in what quantities. Most utilities can derive their own failure rates by utilizing tracking that is already in place for repairs to issue work orders and quantity information from asset management or fixed asset accounting systems. In cases where parts details are not readily available, calculating the device failure rate remains enormously valuable.

By combining the granular elements collected in the cost-per-repair calculation (see illustration, following) managers can project labor, warehousing, support and training needs even into departments not under direct control. Reporting generated in this step is the basis for monitoring and validating product performance over time. Keeping a history of these reports allows later comparison of failure rates, which will identify changes in patterns such as those showing degradation of performance and shorter (functional) useful life expectancies.

This methodology is effective for monitoring any device in any setting. Heavily customized items or items manufactured for unique purposes can be tracked, but the resulting statistics are unlikely to be useful due to lack of a sufficient sample size. Calculating the failure rate of 1,000 of something will quickly reveal problems even with the most highly reliable equipment. The same calculations of 10 of something may take a decade to reveal trends – a timeframe of little use in solving near-term problems.

Maintenance vs. Warranty

We have observed a tendency for planners to assume that manufacturer warranties will cover all maintenance issues. We take the position that warranty is valuable only to the extent that it covers the cost of the parts or unit.

Most electronic equipment comes with a limited time warranty (usually under a year), during which period the manufacturer will replace the item at no additional cost. Labor is rarely included unless at significant extra cost. Even if warranty part replacement is of sufficient term, returning equipment under warranty involves organizational costs rarely considered. Equipment must be packaged according to the manufacturer's instructions, a contact must be made to set up an RMA (Return Material Authorization), shipping both back and forth might not be included, and tracking of the RMA must be performed so that the replacement unit can be entered back into the asset system.

Warranty events must therefore be part of a maintenance strategy only for the value of the parts replacement. The additional organizational and labor costs to pull and replace the part or item may once again exceed the value of the initial product. A product with a high failure rate and a good warranty may be a poor choice if a more stable product is available once all costs are taken into account.

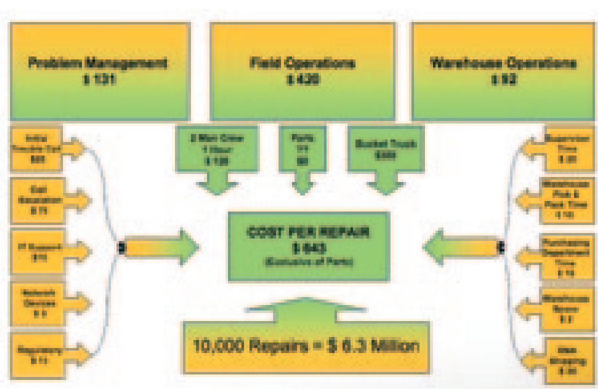
Authorization, Training & Certification

Most electronic equipment is sold with an understanding that the warranty from the manufacturer is "null and void" if repairs are made by anyone other than an authorized repair center, designated by the manufacturer. This is likely to be another area of unexpected expense. Current personnel will need some additional training to be qualified to service these new devices, and some outside services may need to be engaged to support products not easily repaired by existing staff.

Organizations already supporting hundreds of thousands of electronic devices in the field (such as large deployments of laptop and desktop computers) can provide some guidance on how maintenance support will be different for AMI and SmartGrid products than for the less complex devices that they usually replace.

Action Item # 2 – Calculate Your Own Cost-per-Repair

The attached checklist shows many of the areas commonly (and uncommonly) understood to tally in a total cost per repair analysis. Pinning down an exact number may be challenging, but an allowance needs to be included for every item on the list. Walking through a typical problem from initial call through completed repair shows why each element contributes to the hidden burden of each repair.



The initial problem is usually reported by a phone call into a call center. The call center staff attempts to rectify the problem immediately over the telephone. A large percentage of problems are issues of software or user interface and can be resolved remotely. If the problem appears to be hardware, the call center (help desk, or service desk) will escalate the problem to dispatch service personnel.

Most contracts for technician dispatch are based upon a Service Level Agreement (SLA) which dictates the minimum response time from the time the problem is confirmed by remote diagnosis. There are usually different levels of response required based on different types of severity, and contracts often include financial penalties for failure to respond with the contracted timeframe.

Once the determination has been made that a hardware problem needs attention, a technician is dispatched to diagnose, repair, or replace the problem device. This may not be the device or part identified by the call center. The service technician may require additional or more experienced assistance, different parts or devices, or remote diagnostic help to correct the problem.

One the problem has been resolved, the technician reports on the damaged parts or equipment used, makes a determination if the problem was caused by user damage (such as vandalism), and accounts for their time. The back office organization feeds the data from the technician back into an RMA (Warranty) system to have any parts under warranty replaced, or updates the equipment inventory so that the correct parts are re-stocked, and ideally closes out the ticket with a tidy description of the actual problem as well as the resolution.

Management uses reporting generated from this cycle to monitor conformity with the SLA, keep track of all expenses, monitor effectiveness of staff, and feed into upper level accounting and billing systems.

Share and Compare

Utilities have a unique opportunity in the near term to share the failure rate data collected for internal purposes and leverage it to build a database of hardware failure rates. The ability of one utility to learn about itself is limited to those projects already underway. By sharing data, each project in test, scale deployment, or production is a piece of the overall puzzle of equipment reliability.

The wider the variety of equipment experience reported from peers, the more informed the decisions. Differences between products, architectures, environments will be revealed, with the result that the entire industry can drive a focus on reliability which is essential to AMI and SmartGrid success.

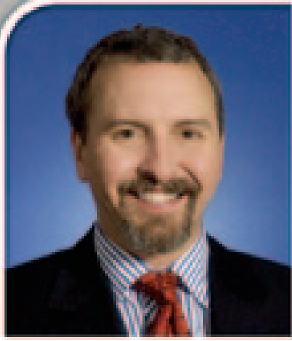
There should be a sense of urgency for this task. The pressures to create SmartGrid and AMI projects are intense and unprecedented. The funding being allocated to stimulate projects is a bounty for those vendors able to prevail in their marketing. In a very short period of time, utilities will be selecting billions of dollars in equipment in near blindness with regard to the equipment reliability. All stakeholders will benefit from good selections, and the opportunity to create the ability to make good selections exists now. Waiting only increases the period of blindness with no benefit.

Executing this type of sharing (aka benchmarking) is impossible without external help. No one utility keeps records in the same manner, and almost certainly never describes the same products in exactly the same way. Benchmarking efforts are therefore limited to single use surveys where participants submit data that already has been conformed manually to the syntax required by the survey. Manual efforts will always be too costly and limited to achieve the depth and scope a shared database should provide.

This manual reporting impasse has been resolved by this solution, in part because the methodology employed was designed to facilitate sharing of disparate and non-standard files for exactly the purpose of comparing products and peers. Moreover, data standardization, organization, calculation, security, and reporting functions for the peer group in the format of a Data Cooperative is an integral part of the solution. Members join their peers anonymously, at very modest cost, and benefit from the combined wisdom of their peers at this critical point in time. ■

About the Author

Gay Gordon-Byrne, VP Technology & Development for TekTrakker Information Systems, LLC is a 30-year veteran of the computer industry as a sales manager representing major IT suppliers. For the past three years she has served as the co-founder and principal designer of TekTrakker, the first database of hardware failure rates driven by electronic files provided in their native formats by users themselves.



Security Quality and Smart Grid: The Utilities' Dilemma

By Rob Shein, Security Architect
Hewlett Packard Company

Computer security is nothing new; the battle between hackers and defenders has gone on for decades, with iterations that have been driven by evolution on both sides of the conflict. The landscape of hacking and the nature of the threat have been changed by the availability of tools to simplify the task and the evolution of economic gain behind cybercrime. Computer technology has transformed successive industries, changing the nature of what is at risk and the potential gains to be had for an attacker.

["History doesn't repeat itself, but it does rhyme." – Mark Twain]

As these separate developments have interacted over the past few decades, those who defend against cyber attacks have cycled through the same trial-and-error phase. There has been limited application of lessons learned from the experiences of others, either from a lack of information sharing or because it was (incorrectly) believed that past experiences did not translate into best practices. However, the nature of the threat has grown steadily, both in potency and in malice, and the time has come where re-learning old lessons is not an option.

In the 1980s, hackers had to work hard and possess unique skills and tools just to gain what is now considered public information. This resulted in a small number of dedicated, knowledgeable hackers, as opposed to the vast number of unskilled hackers encountered today. In the '80s, reliable sources of information were few and far between; public access to the Internet was nonexistent, the few subscription-based information services that had numerous points of presence (i.e., local phone numbers where one could dial in via modem) were devoid of the kind of rich knowledge we now take for granted, and the cost of long distance was much higher than it is today.

A key component of hacking was "phreaking" – the hacking of telephone infrastructure. The number of useful bulletin board systems was so few, and the cost of dialing into them remotely so expensive, that getting free long distance was a crucial component of a hacker's existence. A common occurrence was for a hacker to gain control of a system, only to immediately notify the administrator of that system of how they gained access and how to prevent it in the future. A major purpose of the exercise was exploration and learning… not destruction.

Eventually, the tools developed by this first group of hackers became available to others. The advent of public Internet access and the World Wide Web resulted in a situation where knowledge became far more accessible. Thus, came the dawn of the "script kiddie," a type of hacker who had to rely on scripts and tools created by other more talented hackers, as the means to compromise systems.

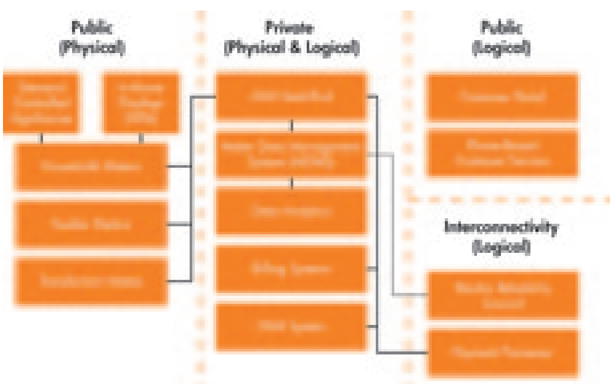
As a result, the number of attackers grew exponentially while their innate skill level declined. Website defacements for nothing more than bragging rights became the most common form of compromise, resulting in embarrassment and the expense of a cleanup, but relatively little real damage. It was eventually recognized that good network design and maintenance practice, combined with diligent patching, was sufficient to reduce the impact of the script kiddies to little more than background noise.

In the end, all security decisions are economic decisions, and in the most recent evolutionary wave of hacking it has become clear that this rule applies to the attacker as well. Criminal organizations have become a significant force in the hacking scene, seeking to turn a profit through extortion or outright theft. This threat combines the advanced technical expertise of the first-generation hacker with a malicious intent that far exceeds that of the worst script kiddie. With the addition of the latest in offensive technologies (e.g., botnets, kernel-hooking and memory-resident rootkits, application-level attacks, etc.), an increased number of resources available to criminal enterprises, and the ability to perform large-scale coordinated efforts controlled by a multi-level organization, and the current state of threat becomes truly frightening.

Against this backdrop, consider the trend of interconnectivity among critical systems, and how far that trend has progressed.

Systems that used to run as islanded networks (or without any form of a network) are now connected, albeit indirectly, to the Internet. Even more challenging, in the power industry the dawn of Smart Grid technologies promises to vastly accelerate that rate of interconnectivity, creating links in ways that present ever-growing challenges for those who wish to protect the critical grid infrastructure that powers the world.

Consider a customer-facing web portal that connects to a back-end database, which in turn, is connected to a billing system. That billing system contains private data about customers and interacts with the head-end of an AMI (Advanced Metering Infrastructure) deployment spanning millions of meters, each with a remote disconnect feature. It is not hard to imagine how a sophisticated attacker would attempt to breach the security of the web portal, compromise the database and set disconnection flags for every meter, particularly in view of the breaches that have compromised millions of credit card accounts. The resulting outage would shed load on a scale far more severe than any other incident that has occurred since the first power line was strung.



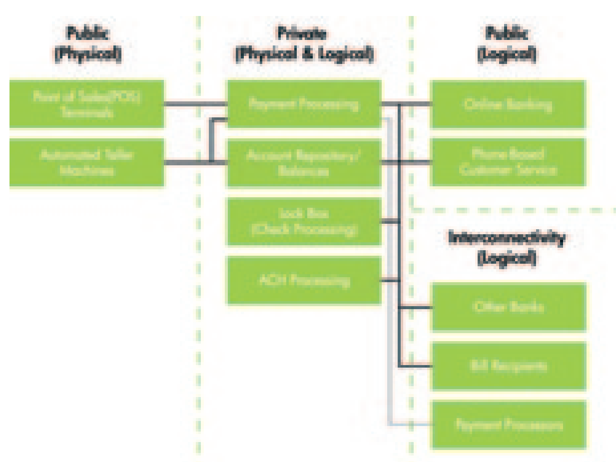
The good news is that none of this is new. Other industries have had to face this kind of threat, and worse, and there are lessons to be learned from all of their efforts. The same mistakes need not be repeated by the power industry as more modern control systems are implemented and utilities go forward with new, network-reliant technologies like AMI.

The financial industry provides a comparable example for the ways in which they automate interaction with the general public. Automated teller machines – or ATMs – provide cash, give balance information and accept deposits from the public. Those machines, in turn, need the ability to interact with the account information of not only that bank's customers, but also the customers of all other banks in near real-time.

As such, they are indirectly connected to the global banking system, even as they stand out in the public in shopping malls, dark nightclubs, and grocery stores. At the other end of the environment, online banking provides a web-based interface where customers can pay bills, transfer funds, and even open new accounts, while having direct access to privacy-sensitive data.

The banking system has always been targeted by all manner of criminal enterprises from the most short-sighted robber to large-scale crime syndicates. While the industry seems monolithic and unchanging (much as the power industry seems to outsiders, even today), it has had to deal with dramatic changes from the shift in check processing that resulted from the "Check 21 Act" to the advent of e-commerce and commonplace use of debit cards to pay for items as menial as a cup of coffee, requiring greater and more immediate interconnectivity. All of these provide opportunities for exploitation by an attacker for direct monetary gain, and all of them have been attacked for just that purpose. As with the power industry, there is heavy regulation and oversight to ensure the availability, stability, security and governance of banks.

Financial institutions like banks learned the lessons of IT security first, beginning with how to think like an attacker when securing an environment. They were the first industry to hire consultants for this purpose, relying upon hackers to help them find and fix flaws in their defenses. Fortunately, the use of "Black Hats" (i.e., former hackers, sometimes also called "crackers") is no longer necessary to accomplish the same goal. Other methods and techniques, from integrating security operations into the change control process to careful network design to control over where and how data is kept, all evolved first in the banking and financial industry as well.



But the most striking characteristic common to these institutions that became secure without disrupting operations, was that they openly embraced the task of incorporating security into their environment and processes.

To a substantial degree, that work needs to be done in the power industry, and the sooner it is tackled, the better it tends to be performed and the less pain is felt from the changes that occur. This becomes especially true when regulatory standards come into play, incurring specific deadlines. The sooner the process of seeking compliance with those standards begins, the more time there will be to involve all stakeholders and make sound decisions.

One of the most overlooked emerging security practices, however, is arguably the most important. Security of products and systems at the application level is the next place where the most positive effects can be realized, after the implementation of basic best practices. Security needs to be a driver in the design process for all vendors moving forward. It can be considered another form of reliability, only against a much nastier form of outage, resulting from undetected and/or undefended security breaches.

Nowhere is this aspect of security going to be more important than in AMI. Unlike the traditional islanded networks of past control systems, AMI involves a significant amount of infrastructure that is accessible to the general public. Wireless communications are ubiquitous, and there is no way to add security measures after the fact.

There is not – and likely never will be – a firewall, antivirus, or intrusion prevention solution that can be added to an AMI meter or collector. Even if such a solution were created, the cost of it would be prohibitive when dispersed over the millions of meters of a comprehensive solution, and management would be a nightmare. The only line of defense is that which resides within the metering solution itself; if the products in use are insecure, then that insecurity inexorably translates to the larger infrastructure.

At the Black Hat Briefings in 2009, a security researcher stood up and disclosed a long list of security vulnerabilities in AMI solutions. The specific vendors were not named, but there were four in total that were assessed, and the impression given was that none of them lacked glaring flaws. The crowning achievement of the security testing was the creation of a worm that was able to spread from meter to meter, wirelessly, until the entire infrastructure was under the control of the attacker. Some of the problems manifested in software flaws, while others were related to hardware or architectural design.

The latter two are more insidious, because they cannot be fixed with a simple software update or patch. In such cases, the cost of fixing the security holes is equivalent to, or greater than, the cost of the initial AMI rollout, as every meter must be physically upgraded, modified or replaced. This is precisely the kind of situation that every industry has faced previously, and only addressed after years of incidents eventually forced vendors to make secure design a critical part of their development processes. Unfortunately, metering implementations historically tend to last for decades, which is a sobering thought considering how long that gives attackers to find and exploit flaws.

Conclusion

For decades, security has been an afterthought that later became accepted as a needed and necessary component of any major environment or system. In the past, the process of trial and error that led to that evolution has been able to move forward without significant impact, but every iteration of the cycle has brought a higher and higher cost to the errors. With AMI in particular and Smart Grid technologies in general, there is no flexibility for a trial and error approach to the security challenge being faced today.

Meters are in fixed locations as are substations and transformers; thus, one cannot change the layout of the power grid simply because it's safer from a networking perspective when insecure products are in use. Moreover, the impact of such an incident would be enormous, far beyond what is acceptable or in some cases, imaginable. The public outrage at an incident that could be attributed to an attack would result in legislation far more stringent than anything yet seen by the power industry, but ironically, that legislation would probably do little to improve security.

Today the stakes are higher than ever, the threats are more dangerous than before, and the alternatives to integrating security into our power infrastructure are few. The best time to act is now, before the vulnerabilities and flaws that already exist become locked into our national power delivery and distribution infrastructure. ■

About the Author

Rob Shein is a Security Architect and designated Global Expert, Smart Grid Security for HP's Energy Industry, comprising Oil & Gas and Utilities, where he and his team are responsible for providing security consulting services. He is an expert in areas where information security and geopolitical issues intersect, specifically information warfare and critical infrastructure protection. Rob is an author and frequent presenter at conferences, and holds various industry certifications, including Certified Information Systems Security Professional (CISSP), Certified Information Security Manager (CISM) and the NSA Information Assessment and Evaluation Methodologies (NSA-IAM and NSA-IEM).

Optical Communications for Improving the Performance and Reliability of the Smart Grid

By: Marcelo Blatt, PhD, Director, Solutions Marketing, ECI Telecom

The electric power industry of the future will be far more information-intensive than it is today. The business model will change from the sale of energy at relatively static prices to the management of a competitive energy market providing spot pricing to customers. This will lead to a far more dynamic environment, significantly increasing demand for accurate and timely voice and data communications.

New areas, such as demand-side management, will require both customer and distributor control along with visibility. As a result, power companies will need to focus more attention on their communication networks: networks that will be characterized by higher bandwidth capacity and the deployment of Ethernet and other high-performance technologies.

The traditional approach to electric power can no longer handle the changes that have taken place over the past 10 years. This is due to several factors:

- Huge increases in bulk power shipments from one region to another
- A shift toward distributed generation, which scatters many smaller power plants closer to customers
- A shift toward renewable sources of energy, such as wind and solar
- An increasing need to regulate and control the demand side; and
- Far more stringent regulations for reliability, security, and reporting

The changes associated with this new approach to electric power generation and distribution add considerable automation and communications load to the existing network. Most of these changes are taking place in the delivery infrastructure, where the new smart grid concept employs digital technology in three important ways:

- Intelligent devices monitor and measure what is going on.
- Two-way communications allows those devices to talk to each other; and
- Advanced control systems enable computers to automatically make low-level decisions, leaving human operators to oversee and control large areas from a central station.

Changes in Generation and Distribution

Recent changes in policy mean that electricity companies are under pressure to increase the amount of electricity derived from renewable sources. This has resulted in the emergence of wind turbines, photo-voltaic cells, and tidal turbines, all of which generate power at far lower voltages and connect to the grid at lower distribution levels (not at the transmission level). For example, the Danish electrical grid, at the beginning of the 1990s, had eight generation centers. By 2006, the number grew to more than 4,000, largely through the introduction of wind farms.

The implications of these few requirements are that every distributed generator and every plant item, no matter how small, may need to be monitored and controlled remotely. For example, a village of the future may be its own micro-grid supplying its own electricity locally, and only drawing energy from the main grid in times of faults or failure of wind, sun or sea waves. Therefore, these grids will need accompanying communications technology for this monitoring.

Substation Automation: The IEC 61850 Framework

The IEC 61850 standard offers a broad framework for substation automation based on huge advances in networking technology. Technologies such as carrier Ethernet switching, high-speed wide area networks and high-performance low-cost computers are providing capabilities that could scarcely be imagined when most legacy substation automation protocols were designed.

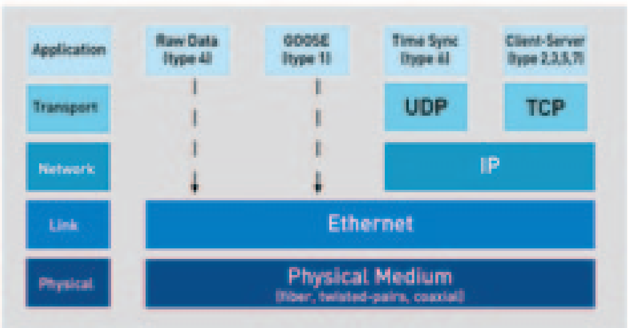


Figure 1: IEC 61850 Communications Protocol Stack

The IEC 61850 framework provides the foundation for a communications network for the next generation substation that offers higher integration, greater flexibility, and plug-and-play functionality replacing hard-wired connections. In particular, the 61850 series standardizes the mechanisms used to access and exchange data within the substation. It standardizes SCADA data and services, and encourages peer-to-peer exchange between intelligent electronic devices (IEDs).

IEC 61850 defines an interoperable communications system for the exchange of information between devices within a substation, and the structure chosen to implement this follows the ISO layer communications model. Specifically, the primary protocols chosen for the various layers include Ethernet and IP.

Since Ethernet plays a critical role in the protection and control tasks in the utility, the communications architecture, including the switches, must be designed to meet the most stringent requirements of availability and low packet latency: A packet delay of 4 milliseconds is required for peer-to-peer communication. An interesting outcome of these issues is that an optical fiber network becomes a necessity. High-speed interfaces are needed to meet the 4 msec delay requirements and all standardized interfaces above the fast Ethernet (either electrical or optical) are exclusively optical.

Dealing with Aging Infrastructure

The planning lifecycle of an electrical plant is often 40 years or more, and delaying the upgrade of an expensive plant can be massively beneficial to the distribution company's business model. An application capable of measuring plant degradation through monitoring assets for unusual activity may be able to predict failures and hence influence replacement cycles.

Similarly, temperature monitoring of circuits enables distributors to use circuits up to the maximum practical load rather than at lower theoretical thresholds, thereby allowing greater efficiency and capacity enhancements to be delayed or even avoided.

Transition toward the smart grid will be achieved gradually. It will therefore be necessary to concurrently support both legacy interfaces, such as V11, V24, and V35, along with Ethernet and other optical interfaces to maintain the current mode of operation while enabling the smooth introduction of new ones. A key feature in this context is the support of Ethernet over existing PDH and SDH radio links. This application requires a high-speed, real-time communications network that extends deep into the distribution network.

Utility Telecommunications Network Infrastructure

The communications network within the distribution company environment needs to undergo transformation. The control and communications networks must extend to all customer points if real-time demand side management is to be used effectively. Similarly, if customers are to be encouraged to become generators, an additional data stream must be aggregated to the network extending to the home. And if both distribution company and customer control are to be supported, data requirements increase even more.

At its edge, the network does not need to have very high capacity. But it must have high service penetration. One can envision a mix of technologies at the edge, with an aggregation into a core network that is built on optical fiber.

An Integrated Communications Infrastructure is a fundamental requirement for the other key technologies in the functioning of the smart grid. Most utilities have implemented very large, privately owned and operated telecommunication transport networks, supporting both fixed and mobile voice and data communications for its operational (i.e., support for grid monitoring, SCADA, remote management of substations, etc.) as well as corporate (internal telecommunications, IT, and business applications) functions. Although these two major areas typically make use of the same facilities, their needs are quite different in terms of bandwidth, traffic, availability, performance, and security and communications protocols.

In addition, these networks are supported by a variety of technologies, including microwave radio with high capacity links, trunked radio systems, mobile data radio systems, PDH, SONET/SDH, and PCM (n x 64 Kbps), which include an immense variety of interfaces such as V11, V24, and V35 for SCADA applications, IEEE C34.37 for teleprotection, FE for video surveillance, as well as PDH and SDH interfaces facing fiber and radio links. Distribution companies require fiber at aggregation points to collect information from large groups of houses, and at data centers to manage the interchange of information for real-time decision-making and control. Aggregation points may be local substations, where fiber, for example, may also be a good choice as a passive temperature and monitoring sensor for electricity cables.

IP Becomes a Unifying Technology

The Integrated Communications Infrastructure must address not only the backbone, but also the spur segments. While core utility operational networks can be based on a number of technologies, the most prevalent is Next Generation SONET/SDH also known as MultiService Provisioning Platforms (MSPPs). Packet-switched networks (PSNs) are also gaining attention in the utility telecom market. Next-generation (NG)-SDH is attractive, as it can support IP and Ethernet applications and legacy services simultaneously. In addition, NG-SDH augments the functionality of the existing SDH network and enables its evolution to IP/MPLS by providing very effective Ethernet transport over SDH. Both pure PSN and Ethernet over SDH are considered Carrier Ethernet networks.

Carrier Ethernet is a connection-oriented protocol that provides “carrier grade” performance for mission-critical applications, including high reliability, QoS, provisioning, and security. The challenge is to combine these features with the cost-effectiveness and simplicity of Ethernet.

There are two main alternatives for providing Carrier Ethernet services:

1. Ethernet over SDH (implemented by the MSPPs)
2. Packet-switched Networks (Carrier Ethernet Switch Routers)

Figure 2 illustrates the technology alternatives for implementing a Carrier Ethernet transport network.

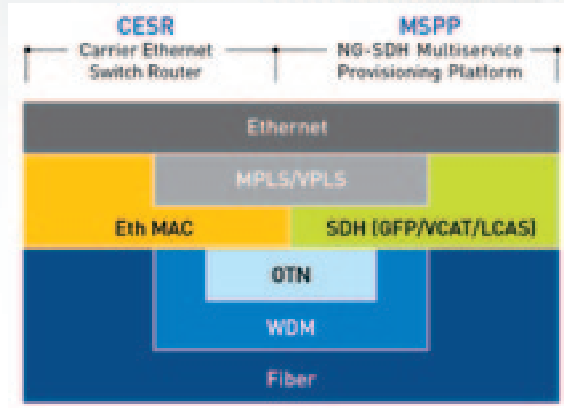


Figure 2: IP Transport Alternatives

Both solutions offer a number of advantages and disadvantages. MSPP is a proven and mature carrier-class infrastructure offering robust reliability, protection, and operations, administration and maintenance (OAM), while Carrier Ethernet routers offer higher-capacity Ethernet services. The optimal utility telecommunications network is the one that enables a combination of both.

The key technology is an MPLS-based Ethernet network that uses MPLS as a circuit-oriented layer spanning the entire carrier Ethernet and SONET/SDH network.

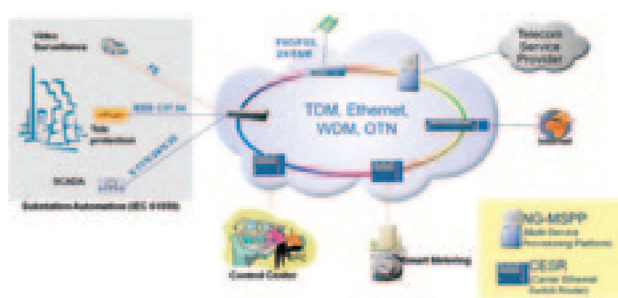


Figure 3: Example of Integrated Communications Infrastructure

The Need for Optical Communications

In addition to the IEC 61850 framework, below are two examples where an optical communications network is required as a consequence of the traffic engineering of the network – smart metering and reducing the vulnerability to intra-substation electromagnetic and radio frequency interference inherent in copper cables, as in the case of the optical IEEC C34.97 interface.

Utility Telecom Network Sizing for Smart Metering

Assume that a data rate per monitoring point of only10 Kbps is required for all applications, billing, demand side management, safety and supply continuity, and generation and distribution management.

If we consider that a distribution company serves some 2.5 million households, and if we make a further assumption that about 5% of all households will install some form of generation and that commercial generation, for example, wind farms and other ventures, gain 15% and 25% of generation at distribution points respectively, we can calculate total demand.

Because of the large number of users, it is clear that fiber is required at aggregation points. In fact, assuming that fiber and WiMAX services are currently the only reasonable option above 30 Mbps, fiber or WiMAX are needed to backhaul from every group of 3,000 houses. Since small towns of 3,000 houses often do not have broadband or effective wireless broadband data services, distribution companies may have to put their own infrastructure in place. In more heavily populated towns, it is clear that fiber is the best solution – from the aggregation point all the way back to the control center.

Distribution companies require a far greater degree of visibility and control deep within the distribution network as data collection and real-time analysis become a more fundamental part of the business model. Fiber networks play an essential role in supporting the information exchange requirements between customers, the distribution network, and the data centers carrying out the real-time analysis of the data. The aggregated volume of data is unlikely to be supported without a fiber infrastructure in some parts of the distribution network.

Low Speed Optical Communications – Eliminating Electromagnetic Interference on Data Networks

Historically, copper interfaces between the teleprotection equipment and multiplexers transfer critical information to the command center. These high-speed low-energy signal interfaces are vulnerable to intra-substation electromagnetic and radiofrequency interference (EMI and RFI), signal ground loops, and ground potential rise (GPR) – all of which considerably reduce the reliability of communications during electrical faults.

Optical fibers do not have ground paths and are immune to noise interference; making optical data links a superior interface for intra-substation communications. Replacing copper interfaces with optical fiber ensures isolation from dangerous GPR, prevents induced electrical noise, and eliminates the signal ground loops and data errors common to electrical connections.

The IEEE C37.94 standard defines an N x 64 Kbps multimode optical fiber interface between teleprotection and digital multiplexer equipment. Teleprotection equipment is used for quickly isolating faults in power transmission systems and is crucial for preventing damage to the network in the event of power outages (blackouts). Teleprotection is aggressively being deployed on communication links residing in harsh high-voltage substation environments. The optical data link replacing existing electrical interfaces in these systems provides immunity to intra-station electromagnetic interference (EMI) and reduces data errors.

Conclusion

The challenges of rising global energy demands, climate change, increasing import dependence, aging infrastructure, and higher energy prices are driving the need to deliver sustainable, secure, and competitive energy. As utilities move toward smart grids, it becomes critically important that they look toward a communications architecture that can be shared among multiple applications that can be supported by the speed, reliability, and security of the infrastructure.

Although communications is not the fundamental activity of electric utilities, a smart grid requires a communications system with the capacity to support traditional utility functions and the flexibility to adapt to new requirements, such as advanced metering, demand response, distributed generation, and more.

Since they provide highly reliable IP/Ethernet networks, the deployment of MSPPs and Carrier Ethernet switch routers to build IP utility telecommunication networks is constantly increasing. Through careful planning, designing, engineering, and application of these technologies, utilities can achieve the business objectives of a smart grid while preserving current infrastructure investments. ■

About the Author

Dr. Marcelo Blatt is Director of Solutions Marketing, Network Solutions Division, at ECI Telecom. He can be contacted at *marcelo.blatt@ecitele.com*

Washington Watch

Power Restored: NERC's Growing Electric Industry Compliance Role

By Gregory K. Lawrence, Partner;
McDermott Will & Emery LLP
(Contributing Editor)

On August 14, 2003, approximately 4:15 p.m., Eastern Time, North America experienced its worst blackout ever, as 50 million people lost power in the Northeastern and Midwestern United States and in Ontario, Canada. A special task force subsequently recommended preventing a reoccurrence by making electric reliability standards mandatory and enforceable, which became a reality four years later under the supervision of the North American Electric Reliability Corporation (NERC).

NERC is an international, independent, self-regulatory, not-for-profit organization founded in 1968 to ensure the reliability of the bulk power system serving 334 million people in North America. Its electric power industry role is to develop reliability standards, enforce compliance with those standards in a fair manner, and assess monetary and non-monetary penalties for non-compliance.

Fines and Enforcement

Although NERC is also responsible to Canadian provincial regulators, the U.S. Federal Energy Regulatory Commission (FERC) has oversight of NERC and has determined under the Energy Policy Act of 2005 and FERC Order 672 that NERC is the official U.S. Electric Reliability Organization (ERO), as of July 20, 2006. It was FERC that approved 83 of the 102 proposed NERC reliability standards (the rest are still being reviewed by FERC) that became mandatory and enforceable in the U.S. in June 2007.

FERC has delegated to NERC the authority to enforce compliance through a rigorous program of monitoring, compliance enforcement and due process (including audits and investigations), and to levy penalties of up to $1 million per violation per day for non-compliance. Penalties are gauged based on mitigation efforts and the risk and severity level posed by the reliability violation.

Indeed, NERC has a "Sanction Guidelines" to govern the assessment of penalties. Investigations can arise, for example, from audits and spot checks, self-reports, and hotline reports. From June 2008 through September 2009, however, the total of NERC fines and settlements has been about $1.3 million with remedial action and non-financial penalties used more often, reflecting FERC's goal of securing compliance, not just levying fines. As Chairman Wellinghoff stated earlier this year: "The central objective of the Commission's enforcement program is compliance."

Under FERC's Enforcement Policy Statement, commitment to compliance is one of the two most important factors in determining civil penalties, with seriousness of offense the other.

The reliability enforcement scheme established by the Energy Policy Act of 2005 is complicated, involving FERC, NERC and eight regional cross-border entities ranging from the Northeast Power Coordinating Council (New England, New York, Quebec and Ontario) to the Western Electricity Coordinating Council (Rocky Mountain and Pacific states and provinces). The members of these regional entities come from all segments of the electric industry: investor-owned utilities; federal power agencies; rural electric cooperatives; state, municipal and provincial utilities; independent power producers; power marketers; and end-use customers.

Under Order 672 and NERC rules, such industry entities that have a material impact on the bulk power system must register and certify with the NERC "Compliance Registry" and are subject to NERC's and the Regional Entities' compliance and enforcement programs and monitoring. Entities are then categorized by function; e.g., balancing authority, distribution, generator, etc., and certain exclusions may apply.

Enforcement responsibility was new to NERC and the regional entities, and while FERC has more experience in how to conduct enforcement, NERC and the regional entities have a strong understanding of system operations. Coordination among the three is thus, essential.

Auditing and Compliance

NERC and the regional entities are required by FERC to make audit standards consistent across all regions and power systems. Industry entities that can be audited include power generators, distribution owners, transmission owners, electricity trading companies and a variety of other key energy industry players. Compliance with reliability standards covers the full range of issues involving the operation of sophisticated electric power systems, including:

- Resource and demand balancing
- Protection of critical infrastructure
- Emergency preparedness and operations
- Facilities design, construction and maintenance
- Interconnection reliability
- Personnel performance, training and qualifications
- Transmission operations and planning

NERC and the regional entities monitor compliance using regularly scheduled compliance audits, random spot checks, and investigations as warranted by indications that a standard has been violated. Since 2007, NERC has received 6,400 violation notices, with 90 percent of those self-reported by regulated entities. In contrast, NERC conducted 380 audits in 2008. Whenever a possible violation is discovered, a thorough review is conducted prior to issuing a formal notice of alleged violation to the involved user, owner, or operator.

Through the entire investigation process, NERC and the regional entities work with each user, owner, or operator to resolve any reliability issues as quickly as possible. At any time, the entity being investigated has the opportunity to settle any disputes or acknowledge the allegation and accept any associated penalties. Once an agreement has been reached and approved by NERC's Board of Trustees Compliance Committee, the details are provided to FERC.

Penalties and Evolution

As noted, NERC has imposed civil penalties relatively lightly. Of 81 actions between June 2008 and September 2009, monetary penalties or settlements were imposed in just 24; the rest resulted in remediation with no additional payment. Many of the actions initiated involve alleged lapses in standards for communication, inspection, security and testing with regard to electric operating systems. More than half of the violation risk factors were classified as "high," meaning they could place the bulk electric system at an unacceptable risk of instability, separation, or cascading failures.

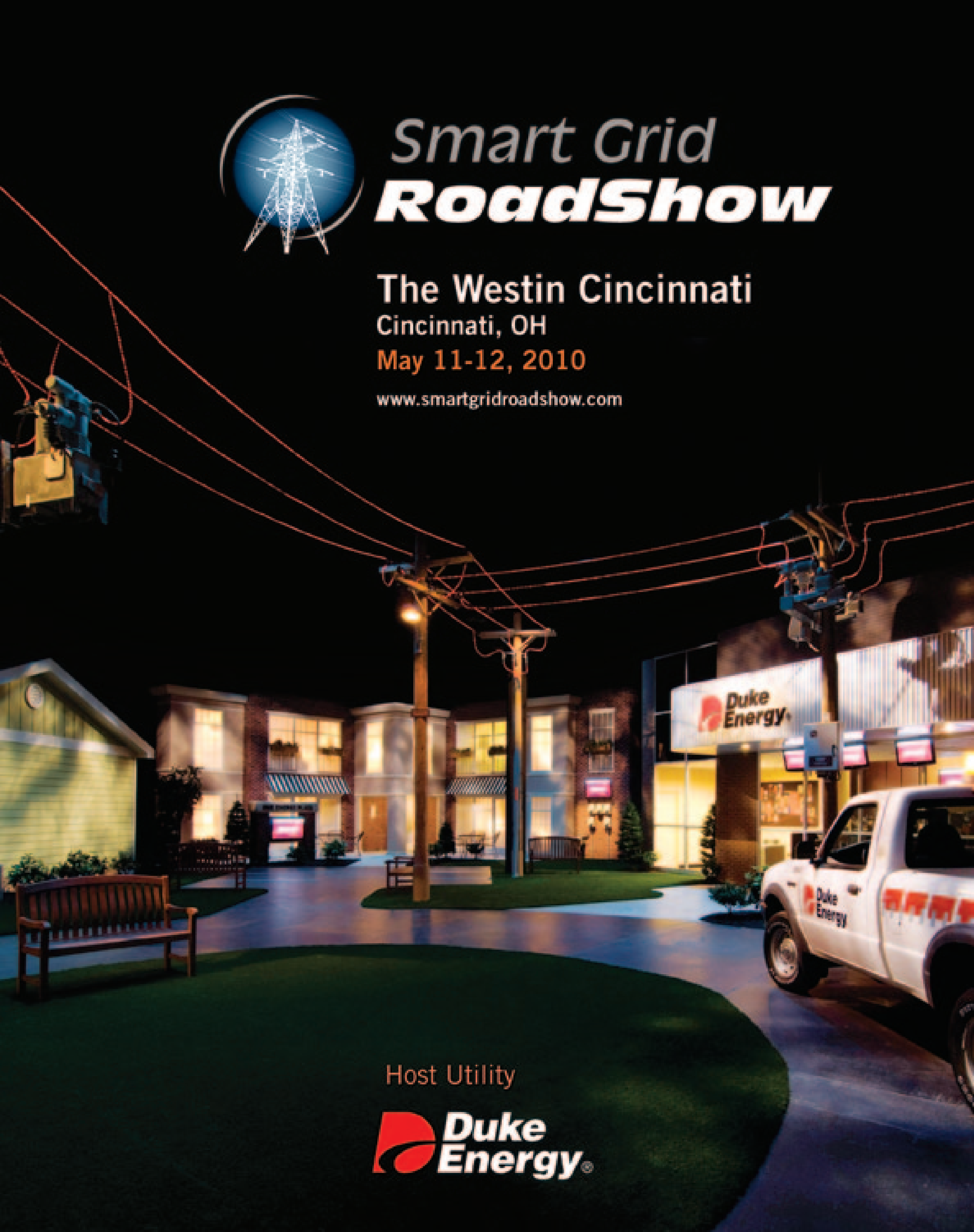
NERC's audit and enforcement capabilities continue to evolve. The organization is issuing an increased number of industry advisories that cover not only audit results but also updates to compliance standards in light of recent industry events. Entities covered by NERC rules should be aware of the advisory process and monitor new issuances on the NERC web site (www.nerc.com).

Moreover, NERC's enforcement capabilities could be profoundly tested with the increasing emphasis on intermittent renewable power sources like wind and solar. The interconnection and reliability issues that renewable energy pose for the power grid are important, and regulated entities that must meet rising renewable energy standards should do so with a sharp eye on how NERC will apply reliability standards for renewable power output. ■

About the Author

Gregory K. Lawrence is a partner in the Energy and Derivatives Markets Group of global law firm McDermott Will & Emery, and leads the firm's Global Renewable Energy, Emissions and New (GREEN) Products group. Mr. Lawrence focuses his practice on transactions, regulatory proceedings, negotiations, governmental affairs and agency litigation relating to the wholesale and retail electricity and natural gas industries.

ADVERTISERS Index


Smart Grid
RoadShow
The Westin Cincinnati
Cincinnati, OH
May 11-12, 2010
www.smartgridroadshow.com
Duke Energy
Host Utility
Duke Energy