www.electricenergyonline.com

Electric Energy T&D MAGAZINE

NOVEMBER-DECEMBER 2008 Issue 6 • Volume 12

In this Issue

Securing Utility Assets:
The Ways and Means of Critical Infrastructure Protection

comverge™

ZigBee® certified ZigBee®

Innovate AMI. Increase Reliability. Reduce Emissions.

Energy consumption concerns are on the rise, as is the demand for environmentally conscious energy. Comverge is leading the charge with innovative Clean Energy solutions. Select from Demand Response, energy efficiency, advanced metering, and grid management solutions to solve your energy demand challenges while doing your part to help protect the environment. Partner with Comverge and discover the "innovative" solutions for meeting growing demand. To learn how to achieve more with less, visit www.comverge.com or call 888.565.5525.

Come see us at DistribuTECH, San Diego, CA, Booth #320.

www.comverge.com | 888.565.5525

Circle **1** on Reader Service Card

Publisher:
Steven Desrochers: steven@electricenergyonline.com

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

Advertising Sales Manager:
Jimmy Desjardins: jimmy@electricenergyonline.com

Circulation Manager:
Janet Guay: janet@jaguar-media.com

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

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

Electric Energy Magazine is published 6 times a year by: Jaguar Media Inc.
1160 Levis, Suite 100, Terrebonne, QC Canada J6W 5S6
Tel.: (888) 332-3749 • Fax: (888) 243-4562
E-mail: jaguar@jaguar-media.com
Web: www.electricenergyonline.com

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

Post Publication mail agreement #40010982
Account #1899244

COVER PAGE IMAGE: www.istockphoto.com

Electric Energy T&D MAGAZINE

IN THIS ISSUE

Circle **25** on Reader Service Card

By Michael A. Marullo, Contributing Editor

Telecommuting… the ultimate out-of-office experience

I'm not sure exactly what got me thinking about telecommuting a few weeks ago, but whatever it was quickly took my train of thought (note the subliminal 'train' message here) down a path that just kept getting more interesting the more I thought about it. In fact, I quickly reached a point where I amazed myself with the potential implications of taking an old idea in an only somewhat new direction.

While I feel certain that I can't possibly be the only one that stumbled across this concept, I have yet to read anything even remotely suggesting that it should be deliberately and diligently pursued. But before I share more specifics of my latest stream of consciousness, let's agree on what telecommuting means in this age of instantaneous, yet inexpensive, global communications.

According to Wikipedia: *"Telecommuting, e-commuting, e-work, telework, working at home (WAH), or working from home (WFH) is a work arrangement in which employees enjoy flexibility in working location and hours. In other words, the daily commute to a central place of work is replaced by telecommunication links."*

Telecommuting is, of course, nothing new. Lots of us have been telecommuting for a very long time. In my own case, I'm one of the many remote workers who don't report to an office every day and haven't done so for years. On the contrary, it's not uncommon these days for weeks to go by without my making a personal appearance at my office, which is only a 15-mile, 20-minute jaunt. But even the one to two gallons of gas it takes to make that round trip makes a difference now, whereas a few years ago it wasn't even a consideration. Indeed, if I were to go there everyday, it would easily add another $25 to $35 dollars a week – well over a hundred dollars a month – to my overhead costs, depending on the price per gallon at any given time and the fuel efficiency of the vehicle used.

As we all know, telecommuting is largely made possible by the availability of inexpensive computers and peripherals; really cheap (practically free, actually!) telecommunications options; the Web/Internet and email; and a host of other enabling technologies, products and services. But for most workers, telecommuting is still held out as a privilege, bestowed upon a handful of select individuals that are "rewarded" by not having to come into the office all five days – each week, every week. In other cases, telecommuting is reserved for temporary situations involving out-of-office experiences like maternity leave, sabbaticals, vacations, disabilities, semi-retirement or the occasional remote task force.

Only rarely, however, have companies actively sought out ways for their staffs to telecommute on a routine basis. Sure, there might be a few organizations that have done it pro-actively as part of cost cutting measures, staff relocations or decentralization programs, but for the most part, it remains a privilege reserved for the elite or those management wants to bestow with that special kind of compensation – you know, the kind that doesn't involve an actual pay increase but that you're supposed to be really grateful for getting nonetheless!

Before we delve any deeper into this, however, perhaps little bit more background would be useful. In 2000, the most recent Census data available, the average travel time to work was 25.5 minutes, up from 21.7 minutes in 1980 and 22.4 minutes in 1990. Most workers — three out of four — were spending that time alone in their own car. And, the number of people who spend more than 90 minutes traveling to work nearly doubled between 1990 and 2000, from 1.76 million to 3.44 million, according to the Census data.

In fact, an interesting April 2006 article authored by Brandon U. Hansen, entitled, *"How To Beat Traffic Mathematically*[1]*,"* states that the average U.S. commuter spends about 100 hours a year driving just to work – 20 hours more than a typical year's supply of vacation. "This personal 'daily grind' uses more than 15,000 miles and 1,000 gallons of gas every year, which might not be so bad if much of it wasn't waste: 1.6 million hours and 8 million gallons of gas are wasted every day in traffic jams across the nation. Traffic even affects your health, raising blood pressure, increasing stress, and producing more Type-A personalities," says the article's author.

It then goes on to say: "Average traveling speed, construction and accident information are all available at the click of the mouse, but how to avoid the perpetual web of red during the morning and evening rush hours is nowhere to be found. Obvious answers such as public transportation and carpooling are legitimate, but trends show that Americans are meeting the increase in traffic by using such transportation methods less, not more."

This is all quite disheartening, considering the magnitude of the problem to say nothing of the cost, which manifests itself in ways that go well beyond the purely monetary considerations. For example, think about the wear and tear on our roads, bridges and other transportation infrastructure. And then, there's also the plethora of destination issues such as where to

[1] OmniNerd.com; April 21, 2006 (http://www.omninerd.com/articles/How_To_Beat_Traffic_Mathematically)

www.elster-eis.com

elster

Circle **4** on Reader Service Card

park all those vehicles; where to house all of the vehicles' drivers and passengers after arriving at their destinations; where and how to service the vehicles – both the preventative and the remedial maintenance issues – and, of course, the pollution issues.

But it doesn't end there. There's more – a whole lot more. It even gets into social issues, many of which have had an increasingly negative impact on our society as we became more mobile throughout the last century and into the new one. For example, if mom and/or dad are spending that "average 100 hours a year driving just to work," that's time that cannot be spent having a family meal, helping out with homework or simply being there when needed.

And how about when all that time on the road leads to an accident – as it almost inevitably does, sooner or later? Even a minor fender-bender adds expenses, lost time and other injuries whether they are physical or not. When you consider the real price we pay for the "privilege" of driving ourselves to and from an office in terms of the snowballing energy, infrastructure, financial, psychological and environmental costs, it literally boggles the mind!

So here's my proposition: What if instead of making telecommuting a privilege reserved for the few, we made it a policy to be practiced by the many? What if companies all over started deliberately looking at telecommuting as a means of cutting costs, helping the environment and improving the quality of life rather than just awarding it to a handful of key people or letting it continue to evolve passively?

I'm not suggesting that we're going to start producing automobiles and building office buildings from our homes over the Internet, but guess what… we'll need a lot fewer of all those things, even if we only apply telecommuting principles to the office workers in our midst. How many hours a week you spend in meetings that don't really require physical presence and could just as easily (more easily?) be accommodated with a teleconference, especially the kind of teleconference we can create at the click of a mouse these days. How often do you drive to an office to do work that could have been done from home – and perhaps even completed if you didn't waste 1-3 hours or more a day in the car worrying about having enough time to work on it?

Indeed, today's Web-based teleconferencing services (e.g., Webex, GoToMeeting, etc.) have finally gotten it right – or at least very close, and whatever is missing is well on its way to being satisfied with currently available technology. I recently sat in on a webinar for one of the more advanced online meeting tools and was extremely impressed with how much more capable and user-friendly these tools have become as well as their simplicity and affordability since my last experience only a couple of years ago.

And while I'm certainly not a proponent of taking the vitally important human factor out of human interaction, I do think we can do much better with how we facilitate its value. There are times when human interaction is an absolute necessity, and to suggest that it isn't would be, well, just plain silly. But there are also plenty of times when a video conference is every bit as good as being there – sometimes better since you can have all of your support materials at your fingertips and still be at your kids' soccer game by 7PM.

From a pure energy and environmental standpoint, the savings are huge, the risks low and the benefits are enormous. Think about it, and talk to your employer about telecommuting to see if the ultimate out-of-office experience is right for you. ■

Behind the Byline

Mike Marullo has been actively involved in the automation, controls and instrumentation field for more than 35 years and is a widely published author of numerous technical articles, industry directories and market research reports. An independent consultant since 1984, he is President and Director of Research & Consulting for InfoNetrix LLC, a New Orleans-based market intelligence firm focused on Utility Automation and IT markets. Inquiries or comments about this column may be directed to Mike at MAM@InfoNetrix.com.

RUGGEDCOM®
INDUSTRIAL STRENGTH NETWORKS™

Rugged Communications
Networking Solutions for Electric Utilities

- The Communications Backbone for Substation Automation and the emerging "Smart Grid"
- The Industry's Most Complete Line of Hardened Products
- Designed Specifically for Harsh Utility Environments
- The Industry's Most Comprehensive Cyber Security Solutions
- Advanced Network Management Software Solutions

RUGGED RATED

Cyber Security

Smart Grid | Substations | Wind | Power Generation

RuggedSwitch® Ethernet Switches

RuggedServer™ Serial Device Servers

RuggedRouter®
Cyber Security Appliance

RuggedWireless™
Wireless Ethernet Switches

RuggedSwitch®
IP66/67 Ethernet Switch

RuggedMC™
Media Converters

- High EMI Immunity (IEC 61850, IEEE 1613)
- Wide Temperature Range (-40°C to 85°C)
- Fast Network Fault Recovery
- High Reliability and Network Availability
- Integrated Cyber Security Features

RUGGEDNMS Network Management Software

Network Management Software

RUGGEDCOM Gauntlet

Cyber Security Solution

RuggedCom Corporate Headquarters
30 Whitmore Road, Woodbridge,
Ontario, Canada L4L 7Z4

Tel: + 1 (905) 856-5288
Fax: +1 (905) 856-1995

RuggedInfo@RuggedCom.com

www.**RuggedCom**.com

Sabre Industries, Inc. Announces New Galvanizing Facility in Alvarado, Texas

Alvarado, Texas, October 22, 2008 – Sabre Industries, Inc. announced today the opening of Sabre Galvanizing, the most efficient and environmentally-friendly general galvanizer in the United States. Located on Sabre's industrial complex along Hwy. 67 in Alvarado, Texas, this new state-of-the-art facility utilizes the latest technology in hot-dip galvanizing.

"Sabre Industries is pleased to announce the opening of our new galvanizing facility. This facility is the only one of its kind in North America, and is a lean, green operation. Sabre's galvanizing process conserves energy, reduces emissions, minimizes the operational carbon footprint, and provides zero hazardous waste generation," said James Mack, President and Chief Executive Officer of Sabre Industries, Inc., parent company of Sabre Galvanizing. "Sabre Galvanizing will set a new standard of excellence in hot dip galvanizing."

One of the largest to be found in the United States, Sabre Galvanizing is a 42,239 square foot hot dip galvanizer situated on 35 acres with ample storage and staging space. The facility houses one of the biggest operating kettles in the world, measuring 65' long x 11' deep x 9' wide and holding 2.58 million pounds of molten zinc.

David de Poincy, President of Sabre Divisions, commented, "Sabre Galvanizing has the capacity to galvanize the largest steel fabrications. Our 65' long by 11' deep kettle provides for greater heat sink reducing possible distortion and, in many instances, the need for 'double dipping'. This facility will provide regional steel fabricators with exceptional corrosion protection."

Sabre Galvanizing is the galvanizing division of Sabre Industries, Inc. Utilizing the best available technology worldwide, it produces superior quality galvanizing. Sabre Industries has manufacturing facilities located in Alvarado, Texas; Bossier City, Louisiana; and Sioux City, Iowa.

Circle 26 on Reader Service Card

Ten Year Outlook for Electric Reliability Highlights Environmental Initiatives, Transmission among Key Concerns

Princeton, N.J., October 23, 2008 – The impact of environmental initiatives and the need for transmission infrastructure are among the most important issues facing electric reliability in North America over the coming ten years, the North American Electric Reliability Corporation (NERC) announced today in its 2008 Long-Term Reliability Assessment. While the total miles of transmission additions have increased slightly over the 2007 report, generation additions are projected to significantly outpace new transmission development.

"We need more transmission resources to maintain reliability and achieve environmental goals," commented Rick Sergel, president and CEO of NERC. "Transmission lines are the critical link between new generation and customers, yet we continue to see transmission development lag behind generation additions. Faster siting, permitting, and construction of transmission resources will be vital to keeping the lights on in the coming years."

October 23rd's reports also highlight other key reliability developments, including:

Capacity Margins Generally Improved, Desert Southwest and Western Canada Require More Resources By 2010 – Lowered load forecasts for the coming ten years and new market mechanisms have contributed to generally improved capacity margins for most of North America. More resources will be required to meet target capacity margins in the Desert Southwest and Western Canada over the next two years, however.

750% Growth in Proposed Wind Generation Projected by 2017 – As state and provincial environmental regulations begin to come into effect, certain regions of North America, such as Texas, the Midwest, the Mid-Atlantic, and the Western states and provinces, are projecting large additions of wind capacity over the next ten years. Though only approximately 23,000 MW of the total 145,000 MW is projected to be available on peak, these proposed additions, if developed, would help to diversify the fuel mix in those areas and provide needed new energy resources. While progress has been made on methods to integrate these new resources into the electric grid, more work and transmission resources will be necessary to ensure reliability is maintained as these resources come online.

Demand Response Projected to Offset Nearly 80% of U.S. Peak Demand Growth in 2016; Significant Growth in Energy Efficiency Projected – Nearly 34,000 MW of demand response and 11,000 MW of energy efficiency are projected to be in place across North America by 2016, reducing total demand by 3.3%. Several regions, including Florida and the Midwest, are reporting peak demand reductions of more than six percent. These resources are providing critical reliability services, increasing the operational flexibility of the grid and complementing the addition of new variable generation resources such as wind and solar energy.

Protection System Misoperations Identified as a Leading Cause of Bulk Power System Outages in North America – Protection system performance has caused or exacerbated a growing percentage of bulk power system outages over the past several years, contributing to over 40% of these outages in 2007. This developing trend has made this issue a primary reliability concern for the coming years. NERC has begun to expand current efforts to address this issue through its standards and technical analyses.

The 2008 Long-Term Reliability Assessment is available at: *http://www.nerc.com/files/LTRA2008.pdf*

Circle 27 on Reader Service Card

Olameter Acquires MeterSmart's Meter Data Management Division

Montreal, Quebec – Olameter Inc. announced that it has acquired the Meter Data Management division of MeterSmart L.P. The terms of the deal between these two private companies were not disclosed.

As a result of this acquisition, Olameter has expanded their suite of solutions to become a leading supplier of professional and reliable advanced meter reading and energy services to the utility industry. Olameter continues to provide an array of utility-focused IT solutions, consulting, field services, and meter shop services, but will now add meter data management, verification, estimation, and editing (VEE), and settlement services to their service portfolio.

MeterSmart will remain in operation to provide services surrounding their advanced customer program management platform, Encentra.

To ensure a comprehensive and seamless service transition, Olameter has acquired all associated MeterSmart resources and retained existing employees. Olameter has established its US corporate headquarters in Arlington, Texas, including a complete data center. This acquisition will strengthen Olameter's North American market position to include over 100 clients within 36 US States, four Canadian Provinces, and Mexico.

"The products and services that MeterSmart provided were well known and respected throughout the market," commented Jan Peeters, Olameter's CEO. "Given the relationship to Olameter's existing core competencies, we are certain of our position to provide these clients with quality service, and that this acquisition will allow us to expand our offerings to meet a wider array of industry requirements."

Optimize System Voltage

With the SEL-2431 Voltage Regulator Control

- *Plug-in compatibility with all popular voltage regulators*
- *Easy front-panel navigation and application settings*
- *Quick information retrieval with remote communication options*

Learn more about

SEL-2431 Voltage Regulator Controls

at www.selinc.com/eetd11

SEL®

Making Electric Power Safer, More Reliable, and More Economical®

www.selinc.com • info@selinc.com • +1.509.332.1890

WORLDWIDE 10 years WARRANTY

John Feltis, Olameter's Vice President of Business Development and Meter Services added, "This acquisition not only enhances our portfolio, but aligns with our corporate objective of expansion across North America. We are also fortunate to be able to retain existing staff and their years of industry experience and client relationships."

About Olameter

As a leading independent meter service company, Olameter offers a full range of telemetry and back-office systems for electric, gas, and water utilities and retailers. In addition to the abovementioned service additions, Olameter provides AMI system monitoring & integration (via their inView application), ASP data collection, workforce management (via their onService application), consumer web-presentment, integration consulting, ASP billing/CIS applications, call centre and back-office operations support, meter reading and field services (including meter installations), and meter service and sales. Olameter solutions are designed to maximize business returns through a proven implementation model that minimizes impact on the client, and assists in achieving deliverables such as improved cash flow, reduced costs, and enhanced customer loyalty.

Circle 28 on Reader Service Card

Substation Related Automation and Integration Program Spending Plans remain "Cautiously Optimistic" by Major North American Utilities

More Than 80% of Respondents Claim to Have Substation Automation and Integration Programs Underway in Mid-2008; Cyber Security Initiatives and Upgrading of Infrastructure to Improve Reliability Seen as Key Drivers to Future Growth

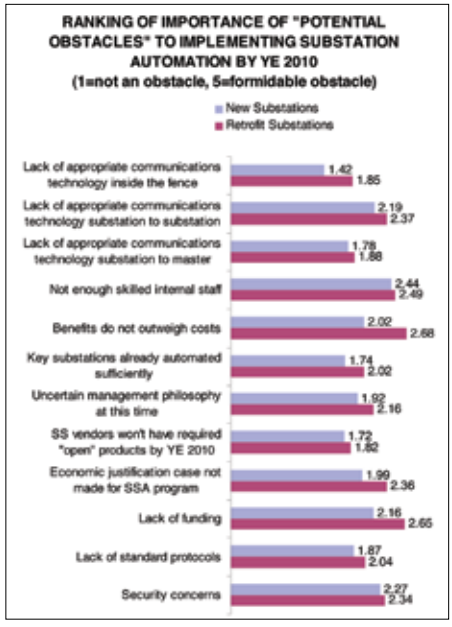
October 10, 2008 – Ellicott City, Maryland. The Newton-Evans Research Company has released research findings from its mid-year study of North American utility substation officials. More than 100 large and mid-size electric utility organizations, accounting for more than one-third of substations, customers and revenues, participated in this new mid-year study.

North American utilities accounting for nearly one-third of all utility owned transmission and distribution substations indicated plans to spend about $130-150 million this year on substation A&I activities. In turn, this suggests that more than $350 million is being spent by the entire community of more than 3000 electric power utilities this year for substation-related integration and automation programs.

Many of the large North American utilities participating in this year's study continue to buy from what they believe to be "best in class" suppliers, whether these are global corporations, or smaller substation A&I market specialists. Others are buying individual components, equipment and products and providing their own substation software development and integration rather than outsourcing this effort to construction and engineering firms. The North American strategy is in sharp contrast to many international regions, wherein utility spending for substation programs is often purchased on a "turnkey" basis from a single supplier.

Among other highlights in the North American study are the following:

- 81% of the respondents have substation automation and integration programs underway in mid-2008. This is a substantially higher rate than was observed in five earlier studies conducted since 1996. Potential obstacles (see image) to substation automation and integration programs are ranked higher for retrofit programs than for new construction, but both have moderated over the past decade.
- DNP remains as the most widely used protocol within North American substations, with strong likelihood that users will migrate from a serial to a LAN-based DNP version over the next two years. Modbus was second in popularity, and Modbus Plus came in third.
- Plans among North American electric utilities to adopt the IEC 61850 protocol (and architecture) remain at a low level, compared with European utility plans and plans noted in some (not all) other regions. The outlook beyond 2010 points to some increased adoption of IEC 61850, at least among a handful of the 100 largest North American utilities.
- Utilities are making use of outside service firms to provide training services (72%), distribution field device configuration support (52%), and engineering drawing support (46%).
- Cyber security issues are being actively addressed by North American substation engineering and operations both in response to industry and federal directives, and in line with prudent utility operational planning guidance. The adoption rate of encrypted protocols, communications port security measures and additional intrusion prevention measures continues to increase.



A total of 22 question groups were included in the survey instrument, accounting for more than 85 individual topical questions.

Additional topics being covered in the series of substation studies include overall substation communications architecture, voltage ranges used to power substation automation equipment, external systems linkages to and from the substation, listings of preferred equipment suppliers, and an assessment of where North America's substations are positioned along a five-phase path to complete automation.

VIRELEC LTD.

From Concept to Commissioning

Virelec has delivered systems for many utilities and industrials across Canada and in the USA. Let our team of knowledgeable professionals help you with your P&C or SCADA project.

Protection, Control and SCADA Systems

Virelec is an experienced supplier to the industry, offering engineering design, procurement, panel manufacture, system integration, testing and site commissioning.

System Engineering

In addition to detailed protection design, Virelec offers power system load flow, short circuit and relay co-ordination studies.

Drop-in Control Houses

Virelec offers this new method of delivering P&C systems. The complete building envelope containing panels, AC/DC distribution, batteries and auxiliaries is cabled, tested and pre-commissioned at Virelec's factory ready for field equipment cabling.

IED Engineering and Support

Virelec's experienced team has expertise in integrating IEDs into substation automation systems, including the IEC 61850 standard. Virelec also provides relay settings and programming, as well as site commissioning.

Call us at 905-569-8030
E-mail: info@virelec.com
Website: www.virelec.com
Virelec Ltd., Mississauga, Ontario

A parallel study is currently being finalized with the international electric power delivery community of utilities. The international study includes participation from utilities in more than 35 countries around the world.

Additional information on the four volume study "Worldwide Market for Substation Automation and Integration Programs in Electric Utilities: 2008-2010" is available from Newton-Evans Research Company, 10176 Baltimore National Pike, Suite 204, Ellicott City, Maryland 21042. Phone 1-410-465-7316 or visit *www.newton-evans.com*.

Liz Forrest can be reached at *eforrest@newton-evans.com* and Eric Leivo can be reached at *eleivo@newton-evans.com* .

Circle 29 on Reader Service Card

Detectent Changes the Game in Energy Efficiency

Escondido, Calif. – Industry pioneer in the application of advanced Customer Intelligence Solutions for utilities, Detectent, Inc. announces the launch of their Energy Efficiency Solution, which delivers new techniques to maximize the potential of utilities' energy efficiency programs.

The Energy Efficiency Solution delivers program managers the tools and services they need to radically change the way programs are delivered to meet rising energy efficiency targets.

Detectent's Energy Efficiency Solution enables utilities to:

- Align customers to programs based on energy profiles
- Rank customers based on potential efficiency gain
- Apply behavior analytics to determine likelihood of program acceptance
- Reach customers with the most effective program messages

The Energy Efficiency Solution is built upon Detectent's proprietary enhanced customer information warehouse. The enhanced customer information warehouse contains the knowledge and understanding of each individual customer far exceeding the information to which utilities normally have access. Detectent's advanced analytics and behavior modeling enables the creation of a prioritized list of customers that are more likely to participate in a given program. Individualized customer outreach strategies, unique to each program, ensure specific messages are communicated with the maximum impact. Together these components form a solution that enable utilities to meet rising energy efficiency targets.

"Detectent's approach to identifying target customers for Energy Efficiency programs will continue to grow in importance as efficiency targets increase for utilities," said Vincent Graziano, President of RISE Engineering, one of the oldest and most established providers of energy efficiency services in North America. "Furthermore, as more efficiency measures are adopted by the market, the task of identifying new prospective customers will only become more difficult," added Graziano.
With more than thirty years' experience implementing energy efficiency solutions for commercial and residential customers in New England, Mr. Graziano understands the challenges of continuing to grow such programs in a territory that has been focused on energy efficiency for decades. "In a very short time, Detectent's approach proved capable of making a dramatic increases in the effectiveness of our marketing efforts and customer acceptance of the energy efficiency programs," said Graziano.

"Our Energy Efficiency Solution represents another milestone for Detectent," said Michael Madrazo, President of Detectent Inc. "It is the result of collaboration between our customers, their industry partners and our team. The solution is built upon the knowledge Detectent has gathered in our enhanced customer information warehouse and continues to prove that there is much value yet to be extracted from this wealth of information."

Circle 30 on Reader Service Card

Hubbell Power Systems Distribution Center Celebrates 10th Anniversary

Centralia, MO employees will celebrate the operation of the Company's 381,562 square foot Distribution Center (DC). Since 1998, the DC has supplied HUBBELL products to utilities and other customers around the globe. Nearly $3,000,000,000 in products has been shipped using an estimated 39,110 outbound trucks to fulfill 1,317,581 customer orders. Employees have worked 2,498 days during the period, totaling 1,283,302 hours.

During hurricanes Gustav, Hanna and Ike earlier this year, the DC was a core contributor to the HUBBELL ability to ship almost 2.5 million connectors, fittings and hardware, 195,000 cutouts and fuse links, 78,000 insulators and arresters as well as 10,000 tools and more than 33,000 anchors, fiberglass construction products and overhead switches to the storm-ravaged areas of the country. 153 trucks were used by the DC and other HUBBELL plants to get the material to utility customers and distributors.

The DC is noted for its ability to rapidly respond to storm emergencies. Emergency material stocks are regularly monitored at the facility in preparation for potential storm disasters. When storms approach, whether hurricanes, ice storms or tornados, truck carriers are alerted 48 hours prior to projected damage areas and in-transit products are expedited to delivery points before storms hit.

The DC provides a centralized shipping point for most Hubbell Power products.

Circle 31 on Reader Service Card

Securing Utility Assets

The Ways and Means of Critical Infrastructure Protection

By Electric Energy T&D Magazine Editorial Staff

In Part 1 of this 2-part series on security, our goal is to provide a broad purview of what most would probably agree is a complex and rapidly evolving topic. To do that, we asked several industry experts to give us their views on where they feel security is today and where it is headed – all in the context of physical and cyber-security for the energy and utilities industry.

We were indeed very fortunate to have had ready access to a stellar panel of experts drawn from the Special Security Panel convened at the Smart Grid RoadShow[1], held recently in Toronto, Canada. This panel – drawn from a cross section of acknowledged security experts in the energy/utility automation and controls field – represents a core group of knowledgeable and experienced individuals who deal with security on a day-in, day-out basis. Their comments, observations and recommendations are presented here as the initial installment.

Then, in Part 2, our January/February 2009 issue will round out the perspectives and add balance with viewpoints from other industry leaders, each having relevant commitments to security for the energy and utilities sector. We believe the following text represents an excellent baseline of information for anyone charged partially or wholly with a security-centric mission.

The Smart Grid Initiative is destined to take grid optimization to new levels, yet all of the new capabilities – and the new devices, systems and subsystems that will be needed to support them – create fallout that could potentially add nearly as much to the challenge as these tools ultimately alleviate.

Several of our experts are quick to note that security is both a current and a future challenge. Specifically, they caution that we cannot focus exclusively on securing legacy installations any more than we can focus all of our attention on designing new levels of protection/detection into future solutions, thereby ignoring latent threats that exist in the installed base. Security – whether physical or technology-focused – must be viewed holistically, and as we trust this article underscores, it must be viewed as a "both/and" remedy rather than an "either/or" ultimatum.

Editor's Note: Besides the continuation (Part 2) of this article in the Jan/Feb 2009 issue of EET&D, we will be revisiting security as an issue of importance throughout the coming year, culminating with a similar article in our Nov/Dec 2009 issue.

There has been much written about security recently – and will probably (rightfully) continue to be for along time to come. These days, security is top of mind in many aspects of our daily lives, whether it involves shipping, travel, information management or – for those of us in the utility space – critical infrastructure protection. By contrast, security was hardly ever mentioned prior to the September 11th attacks, except perhaps among special interest groups already focused on security as a business. This dramatic shift illustrates just how much our thinking about security has changed in less than a decade.

Although some would say that seven years seems like a long time for contemplation, it really isn't in the traditional utility vernacular. Indeed, it's probably just enough time to get our arms around a challenge of such huge proportions and potentially ubiquitous consequences. Indeed, besides being a major issue itself, security is also caught up in the transformation of the grid – commonly referred to as the Smart Grid Initiative – from a relatively passive, 1-way network into a highly intelligent 2-way, self-healing architecture of which security is a fundamentally vital part.

It is also well known that the realization of current and future SGI goals and objectives will require an unprecedented level of capital-intensive infrastructure investment by virtually every utility from the smallest to the largest load-serving entities. There are so many different dimensions of security these days that it's hard to even know where to begin.

[1] The *Smart Grid RoadShow* is a conference series created by Electric Energy Publications and produced by Jaguar Expo Inc. For more information, please visit: http://www.SmartGridRoadShow.com)

Panel of Experts Speaks Out On Security…

Ernie Rakaczky
Invensys Process Systems

Ernest Rakaczky has played an active role within the Process Control arena for over 31 years. He is currently the Principal Security Architect for Invensys Process Systems (*www.ips.invensys.com*) and a key member of the Control Security Team in this position.

Rakaczky participates in the efforts under way at ISA within SP99, NIST within PCSRF, MSMUG and plays an active role in the various Security initiatives with DOE, DHS, INL, NRC, IAEA, Process Control Systems Forum (PCSF) and Sandia Labs, most recently being appointed to the PCSF Governing Board as the control vendor community representative.

He is a founding member to the Canadian Industrial Cyber Security Council and was most recently appointed by Public Safety Canada to chair an active working group to define the Cyber Security Requirements for the Canadian Critical Infrastructure. With the formation of the ISA Security Compliance Institute, ISCI, has been elected as the Marketing Chair of the initial Governing Board.

Jonathan Pollet
Industrial Defender

Jonathan Pollet, VP of North American Operations at Industrial Defender, Inc. (*www.industrialdefender.com*), brings a blended history of more than ten years of experience in supervisory control and data acquisition systems (SCADA), distributed control systems (DCS) and cyber-security solutions in both disciplines to the company. In recent years, Pollet has led combined physical security and cyber security teams on over 100 SCADA and DCS vulnerability assessments for critical infrastructure facilities.

Steve Rubin
Longwatch

Stephen Rubin, Longwatch (*www.Longwatch.com*) President & CEO, has over 30 years experience in the software industry. Rubin was the founder and CEO of Intellution, Incorporated, a worldwide leader in the development and application of process control software for personal computers. Elected a Fellow of the International Systems and Automation Society (ISA), he is a graduate of the Worcester Polytechnic Institute where he also serves as a member of the WPI Board of Trustees.

Tony Clem
Hewlett-Packard

Anthony Clem is a Senior Security Architect for the Hewlett Packard Americas Security Practice (*www.HP.com*). Anthony has focused on compliance consulting for HP for the past eight years in the retail, financial, and energy markets for SOX, PCI and NERC-CIP. Anthony has over twelve years in security experience and 15 years experience in IT. He previously worked in security for U.S. government agencies and was also involved in building early Internet banking architectures.

Andrew Wright
N-Dimension Solutions

Andrew Wright holds a Ph.D. in Computer Science from Rice University. Dr. Wright is the Chief Technical Officer for N-Dimension Solutions (www.n-dimension.com), responsible for technical product strategy and direction. He is also working with IEEE working group 1711 to make AGA-12 an IEEE standard, with Idaho National Lab to develop best practices for securing industrial control networks, and with ISA's SP99 Working Group 4 on secure control system requirements. He has published over 20 technical papers and has 16 years of experience in industrial research and development.

Prior to joining n-Dimension Solutions, Dr. Wright was a Technical Leader in Cisco's Critical Infrastructure Assurance Group (CIAG), where he developed cyber security solutions for critical infrastructure, and particularly for Industrial Control Systems and SCADA. He established the Cisco Secure Control Systems lab in Austin TX, was the key architect of the AGA-12 serial SCADA encryption protocol, and was a founding developer of CVSS, the Common Vulnerability Scoring System.

Deryk Yuill
Bow Networks

Deryk Yuill received his Bachelor's degree in Electrical Engineering from the University of British Columbia in 1984. He has spent his career in a variety of product development and management roles in the telecommunications and utility automation industries. Deryk joined Bow Networks (*www.bownetworks.com*) in December 2001, where he serves as Vice President of Technology and is responsible for the definition, sales and marketing of the Company's substation communications, security and data integration products.

In 2006, the North American Electric Reliability Corporation (NERC) adopted a set of critical infrastructure protection (CIP) standards with their primary mission being to protect the nation's bulk power system against cyber attacks that could potentially disrupt the provisioning and operation of the electric power grid. As Chairman Kelliher's comments (below) suggest, security and smart grid initiatives are inextricably intertwined.

> *"The need for vigilance may increase as new technologies are added to the bulk power system. For example, "smart grid" technology may provide significant benefits in the use of electricity. These include the ability to manage not only energy sources, but also energy consumption, in the reliable operation of the Nation's electric grid.*
>
> *However, smart grid technology will also introduce many potential access points to the computer systems used by the electric industry to operate the electric grid. Security features must be an integral consideration."*
>
> ***The Honorable Joseph T. Kelliher, Chairman***
> ***Federal Energy Regulatory Commission (September 11, 2008)***

In January 2008, these NERC-CIP standards were approved by the Federal Energy Regulatory Commission (FERC), making them mandatory and enforceable with significant sanctions and penalties for

non-compliance. These standards establish the minimum requirements for cyber-security protection and are a good framework and foundation to build a more solid protection against cyber-security breaches. Like all current Cyber Security Guidelines/Practices/Standards there is a common set of requirements in the implementation and management of a successful cyber-security program.

Synopsis of NERC-CIP Guidelines & Focus

NERC Guideline	Brief Description of Standard
CIP-001	***Sabotage Reporting*** Disturbances or unusual occurrences, suspected or determined to be caused by sabotage, shall be reported to the appropriate systems, governmental agencies, and regulatory bodies.
CIP-002	***Critical Cyber Asset Identification*** Identification through the application of a risk-based assessment and documentation of the Critical Cyber Assets associated with the Critical Assets that support the reliable operation of the Bulk Electric System.
CIP-003	***Security Management Control*** Responsible Entities have minimum-security management controls in place to protect Critical Cyber Assets.
CIP-004	***Personnel & Training*** Personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets, including contractors and service vendors, have an appropriate level of personnel risk assessment, training, and security awareness.
CIP-005	***Electronic Security Perimeters*** Requires the identification and protection of the Electronic Security Perimeter(s) inside which all Critical Cyber Assets reside, as well as all access points on the perimeter.
CIP-006	***Physical Security of Critical Cyber Assets*** Intended to ensure the implementation of a physical security program for the protection of Critical Cyber Assets
CIP-007	***Systems Security Management*** Responsible Entities are required to define methods, processes, and procedures for securing those systems determined to be Critical Cyber Assets, as well as the non-critical Cyber Assets within the Electronic Security Perimeter(s).
CIP-008	***Incident Reporting and Response Planning*** Ensures the identification, classification, response, and reporting of Cyber Security Incidents related to Critical Cyber Assets.
CIP-009	***Recovery Plans for Critical Cyber Assets*** Ensures that recovery plan(s) are put in place for Critical Cyber Assets and that these plans follow established business continuity and disaster recovery techniques and practices.

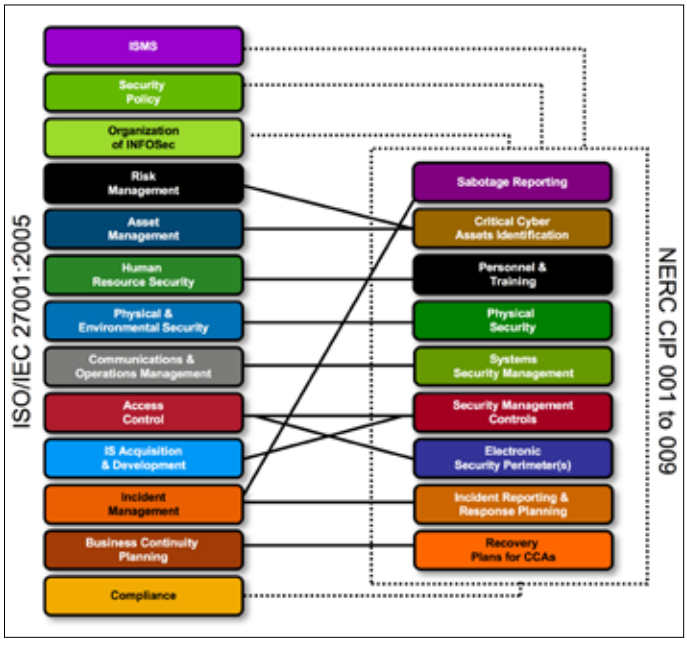
With fines up to $1 million per day – per NERC CIP violation – electric utilities must be prepared to support these compliance requirements.

Dr. Andrew Wright, Chief Technology Officer for n-Dimension Solutions, is quick to point out that there is no "silver bullet" to address all cyber security problems – a view that is shared by substantially all of the security experts we interviewed for this article. For many organizations with critical infrastructure to protect – presently focused on utilities involved generation or transmission of energy at the BES (Bulk Electric Supply) level, which has traditionally been set at or above 100 kV – achieving the level of cyber-security protection required by NERC-CIP can be a daunting task.

Figure 1 illlustrates the correlation between NERC-CIP compliance requirements and the established ISO/IEC standard. The overall implementation of the cyber-security program will require a very strong collaboration across all standards and elements within the operational environment, but perhaps even more important, long-term success will depend on the awareness, understanding, acceptance and adaptation to the new set of behaviors that any successful program will require.

"Keeping in mind that there is no one single product that can meet all the stringent requirements imposed by the NERC-CIP standards, an organization should not base their cyber-security protection solely on a single device – or class/category of devices – such as firewalls. Comprehensive cyber-security is achieved through a combination of physical, technological and human elements that must work together to arrive at a complete 'best practice' solution," according to Wright.

Figure 1: Reference Model Taxonomy: ISO/IEC 27001-2005 & NERC-CIP 001-009 (Diagram Courtesy of Hewlett-Packard)



Based on their research, NERC has stated that the *Top 10 Cyber-security Vulnerabilities* facing the industry are:

1. Inadequate policies, procedures & culture
2. Insufficient defense mechanisms
3. Lack of control at remote access points
4. System admin mechanisms
5. Wireless networks/communications
6. Shared communications channels
7. Lack of tools, forensic and audit methods
8. Installation of inappropriate applications
9. Unauthenticated control systems command and control data
10. Inadequately managed, designed, or implemented critical support infrastructure

"Our company and our partners know the industry and know the challenges that an operator faces," Wright continued. "The provisioning of a wide range of cyber-security solutions in both products and services is to accomplish one objective; that is, to assist critical infrastructure organizations of any size anywhere to achieve the highest standards in cyber security and conform to industry regulations."

Industrial Defender's **Jonathan Pollet** agrees with Wright that there is no panacea solution when it comes to cyber-security: "A truly secure Smart Grid should defend itself at multiple points throughout

the system and should use active defense systems like firewalls or universal threat management (UTM) devices to actively stop attacks at the touch points. Also, Intrusion Detection and Intrusion Prevention technology should backup the firewalls and UTM devices to add another layer of protection.

All devices and system components should create security events and logs with the logs centrally collected for event correlation, incident response, forensics and audit trail. Core system components should have redundancy so that system continues to work, even while under attack. And to prevent any fraudulent activities, the system should use strong encryption and authentication methodology.

"Open systems are now commonplace," Pollet notes, "but when it comes to open systems utilities should rethink the 'open' model where all meters can be read by everyone and data shared openly. If the utilities own the system, they also own the risk. So before opening up the system, it is prudent to consider a model where participants push data out on a prescribed basis using a secure protocol."

Pollet also stresses that it is far easier to design security into the system up front: "We need to think about basic architecture and security standards such as ISA99 (refer to **Figure 2**) and NERC-CIP well ahead of the implementation curve," Pollet warns.

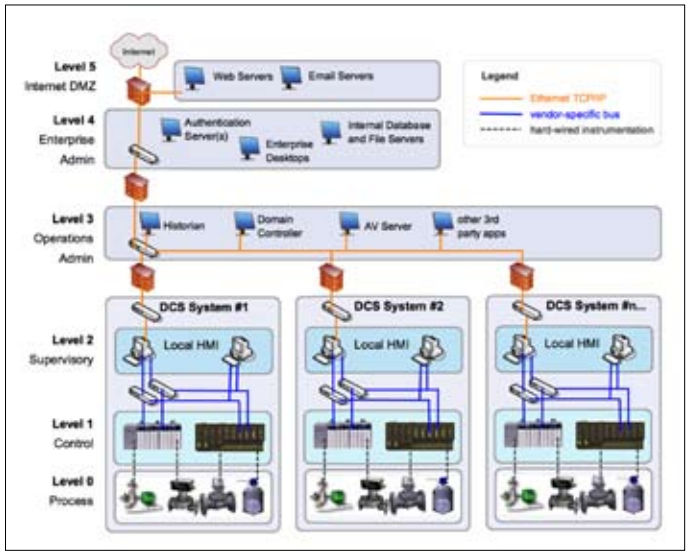
Ernie Rakaczky of Invensys Process Systems reminds us that Pollet's view regarding Smart Grid impact on existing connectivity models also extends to legacy installations of critical control systems. "Over the past decade, suppliers of critical control systems have made tremendous efforts to ensure they will operate in an environment that is open, interoperable and continue to take huge steps in defining a more secure operating environment for these systems," Rakaczky points out.

"The reality is that within our current grid infrastructure we have an operating environment of control systems that could easily date back a decade or more. We are now facing one of our first big challenges in creating a Smart Grid environment, so as we begin to put our modernization plans into place those plans must also include the modernization of these critical control systems," Rakaczky warns, "for it is only through that modernization will we be able to take advantage of the full requirements and benefits of the Smart Grid."

Indeed, one of the big issues that will have to be faced is the traditional 15- to 20-year life cycle estimate for control systems. That figure will probably have to be shortened since an increasing number of elements within these systems – such as the embedded operating system software upon which these systems are based – will have abbreviated life cycles as they adapt to rising numbers and types of security threats as well as for various other reasons. Moreover, it will be critical that all existing control systems be supported for all security issues for as long as these systems are installed and operating.

Rakaczky also agrees with Pollet when it comes to the secure transfer of information across critical control system networks: "The other key element for the control systems within the Smart Grid environment will be the ability to more effectively manage the overall cyber-security profiles of their interconnected networks and the protective technologies that will be in-place (i.e., policies, procedures, firewalls, IDS/IPS, etc.). If not already, this will quickly become a full-time (24x7x365) management requirement," Rakaczky warns.

Figure 2: ISA99 Standard Defines Security Levels for Defense In Depth (Courtesy of Industrial Defender, Inc.)



"And unlike today – where this environment is usually predictable, repetitive and fairly simplistic – requirements dictated by the new Smart Grid environment will likely create obstacles not unlike those encountered in banking, information management and other business environments where this characteristic of network change is quite prevalent. Determination of whom and/or what has authorized access; what category, class and type of information is needed; and which devices within the networks should be accessible must all be assessed and must all be decided well in advance of access being granted," Rakaczky continues.

"From the outset, the key to success will be to start building a fully functional security operation center (SOC) for each Smart Grid operation that will have a full cyber-security responsibility for the actual control devices, systems and networks as well as the overall security infrastructure," advises Rakaczky.

Steve Rubin, President of Longwatch, notes that important steps need to be taken to secure physical assets as well as those in cyberspace. Moreover, Rubin envisions emerging intelligent grid initiatives promising greater system reliability, uptime, safety and security. Achieving incremental improvements, reducing operating expenses and minimizing capital expenditures, while extending the value of installed infrastructure are but a few of the many objectives that Rubin believes will be logical outcomes of the transformation to an intelligent grid.

"Integrated, widespread video can deliver much of the information needed to support and help achieve those objectives," Rubin states. "Recent advances in video technology and software make it possible to transmit digital video over a power plant's existing network, such as Ethernet or wireless, and to put the video images on HMI/SCADA workstations in the control room," says Rubin. "This technology allows high-resolution video to be stored at the remote site for up to 30 days, and low-resolution 'video clips' can be sent to the HMI/SCADA system whenever an event occurs. Each clip can also be configured to

show footage before, during and after the event. And, the operator can switch to a live video feed at any time, and pan and zoom the camera remotely," Rubin explains.

Rubin goes on to say: "Some plants are already using digital video clips to monitor multiple sites using a pre-scheduled scan period, presenting the operator with updated still images of each remote site. Up to 24 video images can be put on a single screen and updated at speeds up to once per minute, depending on the bandwidth available. By using the existing plant network, as many cameras as needed can be installed around a given facility – be it a substation, generating plant or other type of asset installation – without the need for dedicated cable, with all video from that location easily brought into the HMI/SCADA system for display."

"Intruders can still be detected by conventional devices such as door switches, motion detectors or other types of sensors, but the video software can also detect an intruder entering through analysis of the video image itself. Then, after security has been alerted and the police called, high-resolution video can be downloaded from the remote site and used as evidence in criminal proceedings," Rubin notes.

Equally important, video can be used by operators to monitor power equipment, investigate the cause of a control problem, or verify that procedures such as startup or shutdown are being carried out properly. For example, if a problem occurs at a remote substation, technicians will know whether they need a shotgun or a toolbox to fix the problem. With video on HMI screens, operators can see what is happening anywhere in the facility, 24/7/365.

Deryk Yuill, VP of Technology at Bow Networks, also focuses much of his attention on securing the installed base. "It's natural that much of the discussion around cyber-security involves new technology," says Yuill. "These discussions are useful to have, but the massive installed base of equipment is frequently neglected, as a practical matter. It will take years – if not decades – before even a substantial portion of legacy installations can be upgraded or replaced, as Ernie Pointed out," Yuill agreed.

"In talking to a large number of utilities about NERC-CIP compliance, it has been interesting to observe their response to it and the two main threats that accompany it," Yuill continues. "The primary threat is that of a cyber-attack, whether accidental or malicious. The secondary threat is that of fines, which can be levied on non-compliant utilities."

"There is quite a variety of attitudes about this, Yuill says, ranging from those who are primarily concerned by the security threat to those appearing to be more concerned by the threat of punitive fines for non-compliance. The good news," says Yuill, "is that there are reasonable ways of securing most of the systems utilities have in service today."

"Utilities that are committed to security and focus on these fundamentals should find that cyber-security is an attainable goal," Yuill continues. "I believe that for a utility that has built a good security program, the compliance burden can be substantially minimized. Furthermore, as the bar is raised on NERC-CIP compliance – a virtual certainty – those utilities that have focused on security first will be best prepared to adapt to the more stringent requirements."

HP's **Anthony Clem** believes that after achieving security compliance, utilities must document security controls extensively to prove compliance. "NERC-CIP mandates require security event monitoring, incident alerting, forensic analysis and event data retention," Clem contends. "Therefore, it is no longer practical or operationally feasible to assemble and store records manually. That's because utility companies will likely need to manage many documents to meet compliance and collect log files from multiple applications and servers. With sanctions, significant fines, more frequent audits, and increased federal oversight, can any utility afford the ramifications of non-compliance?" Clem asks.

Besides acting as an additional line of defense against cyber-security threats, a complete security solution should also help automate compliance tasks, which can be tedious and time-consuming.

"As others have already said, the energy and utilities industry is experiencing unprecedented pressures to transform the way it delivers energy and interacts with its customers," Clem observes.

"Going forward, the Smart Grid will increasingly rely on advanced technologies, which besides bringing better power management and automation to the meter, new services and business opportunities for utilities and industry alike will also be created. The Smart Grid will manage and distribute electricity and operational information through an extensible, reliable, digitally managed network. This fully two-way communication environment will deliver asset optimization and efficiency opportunities for utilities," Clem explains.

The new expanded network also brings emergent risks associated with advanced technologies. Subsequently, utility providers must ensure that appropriate measures are in place to protect the extensive information flow and control signals intrinsic to the Smart Grid. Protecting both the operations/control network and enterprise network is paramount, as sophisticated cyber attacks are on the rise and increasingly targeted toward critical infrastructures. ■

A Final Note…

Of course, there are many ways to approach security, but it seems clear that most if not all of the experts agree that adoption of a comprehensive, holistic approach that embraces both new and legacy installations as well as both cyber and physical security is the easiest, fastest and least expensive way to achieve compliance.

Complying with the tide of mandates creates greater overhead expenses and data-management headaches. Therefore, to address these new cyber-security requirements, it is imperative that an overall security approach not only address the compliance standards, but also leverage the tools, processes and investments made to support the broadest and most comprehensive security vision possible.

[These and related topics will be addressed in Part 2 of this article, appearing in our Jan/Feb 2009 issue.]

We know infrared.

We invented this industry.

FLIR brought the first infrared camera to the commercial marketplace in the early 1960's. Today we are the only company worldwide totally dedicated to finding and fixing problems through infrared imaging.

Our commitment to infrared runs wide and deep.

Nobody offers a wider selection of IR cameras. Nobody comes close to employing more infrared engineers – now over 350 strong. No other company spends what we do on R&D (over $231 million since 2005!). Nobody offers the training we do, with a school so comprehensive and so respected it's attended regularly even by people who buy competitive brands. No other company has piled up more industry firsts.

Add it all up and it's no surprise that FLIR infrared cameras have saved companies millions of dollars outright, and many more millions avoiding serious losses. As a result, FLIR's reputation for product excellence and industry leadership is one that nobody can touch, let alone match.

Yes, we know infrared. Like nobody else.

Over 40 Years of Infrared Firsts!

First: Commercial System – Mid 1960's
First: Portable System
First: TV Compatible System
First: Image Fusion – Mid 1970's
First: Focal Plane Array
First: Onboard Temperature Measurement
First: Windows-Based System
First: Uncooled Microbolometer System
First: 640x512 Resolution Scientific Camera
First: Camera with Digital Storage
First: Under 2 lb. Camera
First: Portable PdM High Definition Camera
First: Visual/Voice and Text System
First: Megapixel IR Science Grade Camera

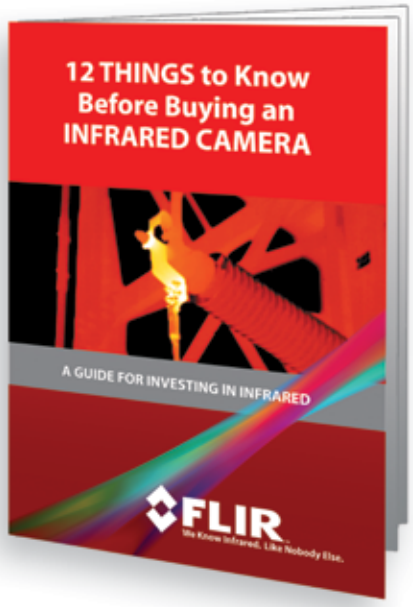
FLIR engineers working on one of the first infrared cameras. Circa 1968.

Free ITC training valued at $1,750 USD ($1,900 CDN) applies to purchase of a new P-series. Save $875 USD when you buy a new T-series or A-series. Offer does not apply to GasFindIR or I-Series. Valid for orders placed between September 1 – December 15, 2008. Images/content used for illustration purposes only. Not valid with other offers. Offer valid in the USA & Canada only. Other restrictions may apply. Please call for details.

Like nobody else.

Don't Buy an Infrared Camera or Thermal Imager
BEFORE YOU READ THIS!

Don't make costly mistakes when you buy an infrared camera. Take a look at our easy-to-read guide filled with tips and the comprehensive information you need to make a smart buying decision.



Download for FREE!

- > What features are must-haves?
- > Which features can help your business grow?
- > What are the price vs. functionality trade-offs?
- > Why is thermal sensitivity critical?
- > What is the most overlooked spec?

Download for FREE today!
12 Things to Know Before You Buy an Infrared Camera
Get it now at: **goinfrared.com/ee6** | **1 800 GO INFRARED** (464 6372)

FREE TRAINING!
*Go to school on us**

Buy an infrared camera before December 15, 2008 and get **ITC training FREE** – Save up to $1,750!

**offer varies by camera model*

FLIR®

The Global Leader in Infrared Cameras

Circle **6** on Reader Service Card

Paul J. Yarka

The 2008 Automation/IT Leadership Series

Accenture

Paul J. Yarka
Partner, Global T&D Asset Management Practice
Greg Bradley, Senior Manager
T&D Asset Management Practice (Europe, Africa & Latin America)

Greg Bradley

Since the inception of this Automation/IT Leadership Series in 2007 we have concentrated almost exclusively on companies providing product/system solutions. However, it is important to also recognize the considerable knowledge, experience, skills and immeasurable value that services organizations bring to the table, especially during these times of unprecedented challenges in our industry.

In this issue, we are very pleased to address this vital services component with an interview with Accenture, one of the pre-eminent companies serving the electric energy marketplace that has skillfully and successfully bonded the business, technological, operational and financial relationships of automation/IT products, systems and services. Over the past decade, the firm has established a reputation for leading some of the largest and most influential trends in various facets of the electric utility industry, perhaps most notably in the field of outsourcing.

This interview, however, focuses on the growing need for huge capital investments by utilities at a time when aging infrastructure continues to decline and our most experienced human resources are moving toward retirement in large and increasing numbers. With many utilities still reluctant to commit large sums to asset replacements or revitalization without definitive cost recovery assurances from regulators, Accenture shares with our readers some refreshingly upbeat scenarios for coping with these formidable challenges.

– Mike Marullo, Automation/IT Editor

EET&D: Let's begin with a bit of background. The Edison Foundation estimates that $1.5 trillion of investment is needed in US electric utility transmission and distribution infrastructure between now and 2030 to meet growing demand, manage risk, and maintain operations. Similar needs exist in the natural gas and water utility industries. With the ongoing financial and credit market crisis, the need for greatly improved capital investment management capabilities is significant, so how can utilities best prepare themselves for such an enormous task?

Yarka: That's correct, Mike, the task that we face as an industry regarding asset modernization is indeed a daunting one. Substantially all utilities – not just here in North America but the world over – will be increasingly challenged on several levels in this current market. The need to manage capital and O&M spending, align spending with multiple drivers and constraints, provide clarity and transparency regarding justification for individual investments, and demonstrate that the specific projects implemented actually deliver on their forecasted outcomes has never been more apparent or more urgently in need of attention. I think Greg would probably agree that this is a global challenge and one that all utilities must eventually overcome regardless of utility size, type or geographical location.

Bradley: Yes, there's absolutely no question that this is a universal issue. Therefore, a comprehensive adjustment to a utility's asset investment planning and management process and the introduction of a next generation decision-support capability can be essential in helping utilities address those challenges.

EET&D: Conceptually, that sounds like a good idea, but perhaps you could elaborate some on exactly what you mean by that?

Yarka: Sure, let's begin by looking at traditional utility practices in this area of capital expenditures. Utilities are always looking for additional decision support methods, but in the meantime they continue to employ their traditional approach of identifying and tracking large capital projects along with capital program and O&M program blankets, frequently aggregating capital and O&M expenditures without necessarily capturing bottoms-up work or project-level detail. A frequent process improvement is to enhance an organization's bottoms-up definition of most if not all identified and planned work.

Refinements to this process and enabling technology can also be achieved through the incorporation of additional steps and components of their end-to-end investment management process. Some organizations have linked basic investment management process steps and enabling decision support technology with associated processes and systems for risk management definition, asset strategy development, budgeting, and post investment review. Typically though, a limited subset of planning and investment analysis capabilities has been implemented when what is really needed is a comprehensive T&D asset investment planning and management process.

EET&D: What would you say are the key elements of such a process?

Yarka: There are really two things that a utility must be prepared to commit to for this process to work as intended. First, they must commit to moving toward an increasingly standardized combination of business process, business collaboration, technology, systems integration and organizational change. The latter element – organizational change – can be very difficult and usually takes the most time to achieve, but that is being somewhat accelerated by the aging workforce issues that are actually helping in some ways to break down the barriers to organizational change.

Second, they must be willing to embrace and encourage a more automated process that enables fact-based, data-driven, decision-making to optimize capital and expense spending.

EET&D: I'd like to pursue this issue of organizational change before we move on because I think it represents a potentially huge impediment to putting the future of the electric power industry on the right track. What do you feel are the most important elements of getting past the organizational logjam so that we can move ahead with the repurposing and redevelopment of the grid?

Yarka: There are a number of issues that need to be addressed head on if we're going to move things forward. Perhaps most important is the need for clarity and transparency. Many utilities have gotten comfortable with the culture of horse-trading – and a little horse-trading now and then can be beneficial from a company culture and business perspective – when it comes to budgeting, in particular. But to be successful in getting control of fiscal policy and maintaining control, they need to adopt a much broader mindset that addresses the interests of all stakeholders. This means moving away from the notion that there is no need to provide detailed project definition for projects having less than what is usually a rather "unscientifically" calculated minimum threshold value.

How the organization defines non-discretionary funding, abandoning the widespread use of blanket budgets, and the idea that projects can be sufficiently scoped and budgeted with only minimal information and without a high level of financial awareness across the entire operating organization are all critical considerations. All too often, there is no official consensus on these matters; they just become S.O.P.

EET&D: Assuming that these organizational impediments can be overcome, what are some of the benefits to adopting this plan for utilities willing to follow it through to its conclusion?

Yarka: The benefits are several and quite tangible. Among other things, they will see both immediate and long-term improvements and operational efficiencies once the plan is adopted and put into motion. Specifically, project identification and the post-investment review process will be streamlined for better project and portfolio management. This immediately leads to improved spending management and trade-off analysis. Senior management attains clarity, transparency, and decision-making involvement in the planning and budgeting process.

And, because the process ultimately requires input from field operations, system operations, supply chain, finance, and others to those who actually plan and identify projects and programs, delivery of and accountability for forecast impacts and outcomes are better

defined, and hence, more achievable. A lot of this might seem like common sense, but you have to realize that traditional ways of doing things are difficult to change in almost any business, and utilities are certainly no exception. This process simply gives them a roadmap that is fairly easy to understand and follow once the initial barriers are broken down.

EET&D: What might a utility expect to see in the longer view, once these changes are well under way?

Yarka: The first thing that comes to mind is being able to actually accomplish their longer-term goals and objectives in the areas of resource management, contractor management, material management, and portfolio management. Poor planning and visualization have historically derailed these long-term aspirations up front, followed by erratic or non-existent execution of the short-term objectives that were needed to support the longer view. As a result, the longer-term objectives only rarely were realized.

EET&D: One of the key dimensions of the Smart Grid Initiative that is rapidly gathering momentum all across the industry is the notion that there is a true paradigm shift under way as regards the way that utilities plan and carry out their budgeting process. That shift appears to be underscored by movement toward a much more centralized, top-down approach, as contrasted with the bottom-up, piecemeal approach that has traditionally characterized the utility budgeting process. Is the process you have outlined here compatible with that trend?

Yarka: This process most definitely embraces a budgeting process that is more centralized and standardized than what we have seen in the past. Reduced planning and tracking time, improved estimating accuracy and the ability to create a level playing field and consistent investment guidelines for all involved in the business planning process will help tremendously to further that trend. Moreover, the ability to keep project and portfolio information current and implement a consistent risk framework across this process will directly help utility managers elevate the organization's overall project and program understanding and collaboration.

EET&D: Where and how does technology fit into all of this – or does it?

Yarka: As asset investment planning and management decision support tools evolve, a variety of additional functional capabilities are still needed. Apart from providing a tool to compile, manage, and prioritize investments, tools of today – and in the future – are being developed by several different industry groups including large ERP software providers. These companies, as well as some engineering-oriented firms with experience in T&D asset strategy decision support tools, are extending their platforms to support various aspects of investment management. And, some relatively new firms are developing multi-user decision support tools that support several aspects of the end-to-end investment management process.

EET&D: What do you feel are some of the capabilities that utilities want and need for risk management, asset strategy development, budgeting and post investment review?

Yarka: On an enterprise level, integration with top ERP and EAM platforms to access actual capital construction expenditure data, maintenance cost and equipment history data, and asset register data is essential. But there are also other important factors that must be taken into account on a more detailed level. Perhaps Greg would like to elaborate further on the core elements that we have both seen in our respective geographical markets.

Bradley: Yes, I think we are both seeing and hearing many of the same needs and requests by utilities, regardless of which continent – or continents – their service territories cover. Some of the most important ones involve the ability to develop, analyze, save and adjust "what if" investment scenarios; the ability to assemble, compare, analyze, prioritize and optimize investments across the enterprise; the ability to support a multi-user collaborative environment across multiple lines of utility business in all facets of work identification,

risk assessment, comparison, analysis, prioritization, and optimization; the ability to forecast and manage a five-year capital and O&M plan; and finally, the ability to model asset class-specific, end-of-life/replacement plans based on failure models.

EET&D: While it certainly makes sense that there would be some similarities, should we expect to see some or all of these trends materializing in North America at some point as well?

Bradley: There are many other capabilities that utilities seek in next generation asset investment planning and management tools. Across Europe, we are observing an increased level of scrutiny from regulators and infrastructure-owner consortia acting as asset owners. Both require better visibility of long-term investment plans, which justify both the volume of capital work proposed as well as the cost for executing it. Work volumes for asset replacement need to be justified in terms of their linkage to network performance and reduced risk, whilst the budget associated with the works need to demonstrate capital efficiency.

But let me be clear that I'm referring here primarily to regulators in the UK and the increasing trend toward consolidation of asset ownership by large players such as Suez, GDF, Veolia as well as infrastructure funds like Macquarie. These companies – as well as others – are investing in "network businesses" to secure a stable level of return on capital, in effect guaranteed by the regulatory or government-set tariffs. We've already seen some of this trend in North America as well. The recent investments by Warren Buffet's Mid-American Energy in PacifiCorp – and more recently BG&E/ Constellation Energy – as well as Macquarie's investment in Duquesne Light & Power are some examples of this, I think.

Yarka: I would also add that in some cases, these plans are linked transparently to customers to test their "willingness to pay" for the level of service offered by the utility for a given level of cost. This growing trend requires utilities to be able to articulate these linkages in ways, which they previously were unable to and also requires extensive integration of systems, data and business processes.

EET&D: A lot of these measures sound rather long-term in nature. What – if anything – is keeping utilities from realizing the value sooner rather than later?

Bradley: One of the key constraints that European utilities encounter is the availability of data to support these systems and modeling requirements. Often, there are gaps in the asset register or in the attribute data associated with the assets. Similarly, the data can often be stored in multiple systems in multiple formats, which makes integration for investment planning complex and limits the ability to generate rolling, dynamic plans that can easily be reforecast or updated to meet emerging business priorities, overcome unexpected constraints, or provide an update to a regulatory review. Yet even with a strong commitment to the process and steady investments in information infrastructure, it will definitely take time to overcome these impediments. Meanwhile, there is clearly an opportunity to realize incremental benefits along the way – virtually from day one – with proper planning and execution.

EET&D: Is it fair to say that these constraints also apply here in North America, or are they different?

Yarka: Although there are certainly some regional differences due to the dissimilar regulatory environments between North America and other parts of the world, I think the data availability constraint is widely relevant. As Greg points out, it will indeed take time to overcome, but of course, the best way to shorten the path to seeing real progress and tangible results is to get started today. ■

Overcoming the 'Knowing–Doing' Gap in Safety

By Carl Potter, CSP, CMC and
Deb Potter, PhD, CMC

One of the biggest mysteries in hazardous work is why well-trained people do not follow their company's safe work practices. The utility industry is no exception. Utilities and their contractors, for the most part, go to great lengths to ensure that workers know the rules, have the proper personal protective equipment, and have the tools they need to do their jobs safely. Yet every year fatalities and injuries occur at alarming rates. After years of research, the answer is clear: the gap between knowing and not doing is much bigger than the gap between knowing and not knowing.

It's quite simple to observe that the gap between knowing and not knowing is easily overcome through training and education. Utilities provide some of the best education of any industry, yet we continue to see example after example of devastating situations where people do not apply what they know. It makes any workplace or job a risky one when this occurs.

It's not hard to see examples of the 'knowing – doing' gap in the workplace. On September 12, 2008, a train engineer in southern California ran a red warning light causing a head on collision with the Metrolink and a Union Pacific train, killing 25 and injuring hundreds of others. The contributing factor was that the engineer was text messaging while on duty. The engineer was presumably well-trained, yet ignored a basic safety procedure, ultimately causing human loss and suffering. Rarely does a week go by when we don't hear about a serious injury in a power plant or utility field operation.

Unfortunately, the gap becomes all too real in investigations of a workplace fatality in which the injured person failed to follow basic safe work practices that could have easily prevented the incident. For instance, a recent review of a burn incident that occurred during restoration after a storm in 2008 showed that, although a proper pre-job briefing took place, the involved employees did not follow the steps that were determined to be the safest way to restore service – a prime example of the 'knowing-doing' gap. We've got to train people to be aware of the gap between what they know and what they do and why it's important to close that gap.

If you've ever been to London and used the underground transit system, you've no doubt heard the recorded voice loudly proclaim, "mind the gap – mind the gap" to remind embarking and disembarking train passengers about the space between the platform and the train. What if we had a voice remind us to mind the gap between our knowledge and our actual performance? The problem is we all have 'knowing-doing' gaps. It's part of human nature. For example, most of us know that exercise and proper nutrition will keep us healthy and help us live longer, more fulfilling lives. Yet, a majority of us don't adhere to what we know to be true. It takes work to stay mindful of the gap and to know how to make choices to close it.

It's essential that leaders recognize, and then do something about the gap. Think about your own workplace and answer the following questions:

1. What evidence of a gap in worker knowledge and application exists? Often leaders don't look for the gap and therefore don't know that it exists. Learn to observe workers, even your fellow workers, to determine if they understand and apply pertinent rules.

2. How are supervisors trained to deal with situations where workers aren't accurately applying safe work practices? Remember that supervisors are often people who have come from the workforce and may not be trained in how to handle certain situations. Ensure that leaders from the front line all the way to the top of the organization know the safe work practices and how to deal with employees who choose not to follow them.

3. When is the last time your organization's safe work practice training curriculum was reviewed for relevance and interest? Outdated and uninteresting training can create apathy toward learning and will lessen the opportunity for appropriate application of safe work practices. If you are responsible for training others, take time to review materials and make sure they are up to date and relevant for your workers. If you aren't in charge of training, volunteer to review material and provide feedback.

Understanding and dealing with the gaps will help you recognize the mental models that individuals have that widen the gap between knowing and doing. Sometimes the gap results in tragedy and human suffering.

When it comes to safety, far too often workers, supervisors, and managers put up mental barriers to safety and they don't even realize it . Yet, adopting an approach of readiness will help overcome -- and even remove -- many of the obstacles we have in our minds. Take a moment to understand what keeps you or your team from being mentally ready for the job.

Identifying the Mental Roadblocks to Safety

Consider the following five barriers found in employees' minds, regardless of their levels in the organization:

1. **"Accidents are just going to happen."** It's surprising how many intelligent managers, supervisors, and employees have this barrier. This fatalistic belief creates an obstacle to organizational learning about safety. This attitude of hopelessness stifles creativity and improvement in the organization's safety process.

2. **"It won't happen to me."** This barrier is a polar opposite to the previous one. This attitude prevents employees from taking responsibility for safety. This mental barrier to safety puts everyone around in danger – the employee, co-workers and sometimes customers or members of the public.

3. **"I have enough experience or skill to take shortcuts."** This egotistical nature of this barrier causes individuals to resist coaching, feedback, and training that can help them work safe. This danger of this obstacle is that it often exists in the minds of more senior or experienced workers who set a poor example to those who are less experienced. It's difficult to detect this barrier. When employees make excuses for not following the company's safe work practices, this behavior sets a poor example for less experienced workers.

4. **"I'll do it just this once."** These words may be the last words of a fool. How often have you said this yourself or heard others say it? This phrase should be a big red flag to stop and assess the situation.

5. **"Zero is impossible."** This is the mother of all safety barriers. This statement is an indicator of a huge barrier to an injury-free workplace. Ask yourself why you'd work where it's not possible to work without injury. This barrier affects individuals and the entire organization because it shuts down efforts to create a zero injury culture.

Carefully consider these mental barriers to safety. You may find that you recognize them, or other obstacles, in yourself or your workgroup. These barriers pop up at different times, for various reasons. If you find yourself in a safety meeting thinking that you have already heard about the topic so many times, you just don't want to hear it again – check your mental barriers. Or, you may notice a barrier pop up when you're in a hurry. If so, stop and assess your mental readiness. Sometimes a barrier is a permanent one, so ingrained in our thinking that we don't even recognize it. That's why it's important to first recognize the barriers, then work to understand the concept of mental readiness.

Four Guidelines to Close the Gap

1. Involve a cross-section of employees in a review of your current safety rule documentation. Ask them what rules are unclear or are difficult to apply or which ones they simply choose to ignore.

2. Get a copy of your safety manual or accident prevention book and a yellow highlighter. Mark every instance of the words "shall" and "will". These words, while similar, carry different weights. The word "shall" means "without deviation" and the word "will" generally indicates a guideline. Can workers reasonably follow the rules that contain the word "shall"? Be sure that you ask the involved workers.

3. Use a safety expert to review the OSHA rules that are applicable to your industry. Does your safety manual include all these rules and, more importantly, are your employees aware of the proper application of these rules and the safe work practices for your organization?

4. Establish employee-management safety councils in your organization. Employee participants represent their peers and have access to management to discuss safety concerns. When management demonstrates their commitment to listen to and address issues promptly, such groups can be highly effective.

Engaging employees in these activities is a key factor for success. It will help them to "show up" mentally and physically, and bring their best efforts to work. One of the most important jobs of a leader – whether a crew leader or a company president – is to guide people to appropriately apply knowledge. Take time to first consider if you're applying what you know about safety, then look around. Ask yourself what you can to do help others apply what they know. The result is that by closing the knowing-doing gap, you are reducing risk to employees, the public, and the company. ■

About the Authors

***Carl Potter**, CSP, CMC, CSP…The Safety Strategist℠…works with organizations that want to create an environment where nobody gets hurt. He is the author of the newly released book "I Am Safe – Closing the Gap Between Knowing and Doing." As an advocate for zero-injury workplaces, he is a nationally-renowned safety speaker, author, and advisor to industry.*

***Deb Potter**, PhD, CMC is a researcher, author, and speaker in the area of safety management. She is the author of "Simply Seamless Safety."*

For information about their programs and products, see www.potterandassociates.com or contact them at Potter and Associates International, Inc. 800-259-6209 or carl@potterandassociates.com.

Smart Grid RoadShow

Denver Marriott City Center
DENVER, COLORADO
APRIL 6-7 2009

Bringing the Smart Grid Marketplace to Your Door!

If you are a Smart Grid participant — whether as a user, supplier, consultant or in a related capacity — and would like to share your knowledge and experience with a tightly focused audience of professionals seeking information and solutions to a wide range of Smart Grid initiatives, then the Smart Grid RoadShow Program Committee wants to hear from you!

We are currently soliciting presentations and abstracts for special sessions for SGRS venues across North America. So don't delay… **visit the SGRS website to download the Call For Papers or contact us for more information today!**

888.332.3749 x222

Host Utility: Xcel Energy

Produced by: JAGUAR EXPO

Presented by: Electric Energy T&D MAGAZINE

www.smartgridroadshow.com

Circle **21** on Reader Service Card

"Extreme IT Makeover" Transforms Georgia Utility

By Bob Arnett, Vice President-Technology Systems
Cobb Energy | Marietta, Georgia

Two short paragraphs sum up an incredible three years in the lives of dozens of people in Marietta, Georgia:

Six months prior to "go-live" of a two-year technological overhaul to replace an aging legacy environment and reduce outside contractor support costs of the billing system by 50 percent, Cobb Electric Membership Corporation (Cobb EMC) purchased Southern Company Gas. Cobb Energy – an aggregator of services for Cobb EMC – needed to immediately dissolve its previous gas marketing partnership with SCANA Energy and transfer back accounts. Likewise, Southern Company Gas (now Gas South) also required a billing system conversion from its platform by a fixed date. This created an additional conversion from a different platform and a change order resulting in a 12-month extension, a 74 percent budget increase, and extensive re-planning of the project.

It was a very emotional three years with widespread user involvement and executive support for the project, which resulted in projected annual benefits of more than $3 million. Both the IT staff and business people are performing more value-added tasks since the IT transformation has taken place. Turnaround time on user requests has dramatically improved. Cobb EMC has improved its accuracy metrics and decreased its reporting requirements from 6,000 reports to 300 in the new environment. Everyone in the entire IT organization and most of the business people has received training on new applications and tools, and they survived to tell about it!

Behind that brief description, in which the organizers of the CS Week Conference explained why they gave Cobb Energy the "Expanding Excellence Award for Best CIS Implementation," is a story that typifies the obstacles many utilities face when they resolve to improve services to their communities. It is a story of how teamwork, perseverance, a lot of smarts, and a touch of luck can transform the way a utility does business.

Need for Change

In today's world, where utilities are focused on environmental concerns, resource constraints, and intelligent grids, it is sometimes hard to remember that in the mid-Nineties, the word of the day was "deregulation." Some co-ops decided to remain on the periphery, but Cobb EMC determined that it could best serve its members by reorganizing to prepare for deregulation and protect its assets. It formed Cobb Energy in 1997 in an effort to manage its costs more efficiently while allowing this new affiliate the ability to provide services to other utilities.

By the early 2000s, it was clear Cobb Energy was on the right track, given the specific market conditions and member needs. Cobb Energy provided the billing services for Cobb EMC's electric customers, and also for 110,000 SCANA natural gas customers. These gas customers in Georgia's deregulated market signed up through partnerships with Cobb EMC and four additional co-ops. Cobb Energy produced the gas bills for the other co-ops and created "combo-bills" (electric and gas on one bill) for select Cobb EMC customers. The organization also established small footholds in telecommunications, security, surge protection, and tree trimming services, along with beachheads in mortgage financing and prepaid health cards.

"We selected Oracle over nine other bidders based on the company's industry expertise and the application's functionality, usability, flexibility and ability to integrate with other software. Before we implemented Oracle, we needed to gather information from multiple screens to assist customers. Oracle Utilities Customer Care and Billing delivers the information needed to assist our customers to the fingertips of our employees. Our infrastructure and application transformation has touched every Cobb Energy department and affiliate, and we will leverage this platform for many years to come."

Robert Arnett, Cobb Energy
Vice President, Technology Systems

"We migrated from a monolithic architecture to a multi-tier architecture that allows us to 'grow' our computing capacity either vertically or horizontally… our choice! "We can also utilize one vendor or multiple vendors because the application is not dependent upon one particular operating system or database. And, we can now consistently complete our nightly billing processes before 1am. Before, billing often ran until mid-morning; often later and into the next business day."

Tom Bland, Cobb Energy
IS Operations & Services Manager

Existing technology was good enough to get the job done, but it was becoming more expensive to operate and expand every year. It was not flexible enough to accommodate such a diverse and expanding business. Cobb Energy had not upgraded its billing software in more than five years, since obtaining the source code and beginning to customize it heavily.

On top of that, it was difficult to respond to everyone's needs. The requests seemed to get more creative every day. A favorite quote was also the IT team's greatest challenge. David Johnson, chief operating officer (COO) of Cobb Energy once said, "If I can think it, you should be able to program it!" That should give any IT person a few chill bumps! The team received requests to set up new rates in the system on a regular basis. It took the team six months to design, code, and test one rate before implementing in the system.

The overall technology environment seemed to handcuff the team at every turn. Progress was plagued by 189 complex, point-to-point interfaces, cumbersome testing, overwhelming needs for user training, high turnover in the call-center, and a huge dependency on contractors three time zones away. The batch processing window sometimes ran 36 hours, not catching up until the weekend. The connection between customer service and engineering was printed paper.

Moreover, the tools for project planning, code management, issue and risk management, and testing just did not exist. All of this resulted in the business people losing patience with the IT department. There were so many report requests in the queue that departments were double- and triple-keying data into spreadsheets and Microsoft Access databases. The marketing department alone had 29 MS-Access databases. Sound familiar?

Change

After some analysis, Cobb Energy discovered that it spent more than $2.3 million annually on external resources and an additional $1.5 million on manual processes that should have been automated, just to manage and operate the legacy billing system.

Late in 2003, after a three-month selection process, Cobb Energy chose a new CIS application—what is now known as Oracle Utilities Customer Care and Billing (CC&B). Oracle acquired the application's vendor – SPL WorldGroup – in 2007.

Competition was fierce among the nine vendors considered. But in the end, it was essential to select on factors that would ensure future success—an application with advanced functions and a lot of flexibility, plus the ability to integrate with other software. CC&B was the software that would carry Cobb Energy through the changes—expected and unexpected—that would occur as the business evolved.

Then "Pandora's Box" opened. Since the legacy system was mostly monolithic and contained more than just the billing functions, Cobb Energy conducted a similar selection process for enterprise resource planning (ERP) and human resources planning (HRP) applications. This "best-of-breed" approach dictated the need for an enterprise application integration (EAI) strategy to pull it all together. If it was not complicated already, now it was extremely so.

With the projects well under way, the need for enterprise-wide communication and change control was overwhelming. Cobb Energy reorganized its IT department in an effort to manage two distinct areas of responsibility: Infrastructure/Operations and IS Programs. Strategically, the organization changed the department name "IT," to "IS" to emphasize the focus on *"Services"*.

Cobb Energy created a formal Project Management Office (PMO) to coordinate all three projects: customer information system (CIS), ERP, and HRP. Project Managers and Stakeholders met often to share progress and iron out common issues.

As the PMO made progress, Cobb Energy identified the need for formal ITIL-based processes and the organization developed its own *Foundation Processes*.

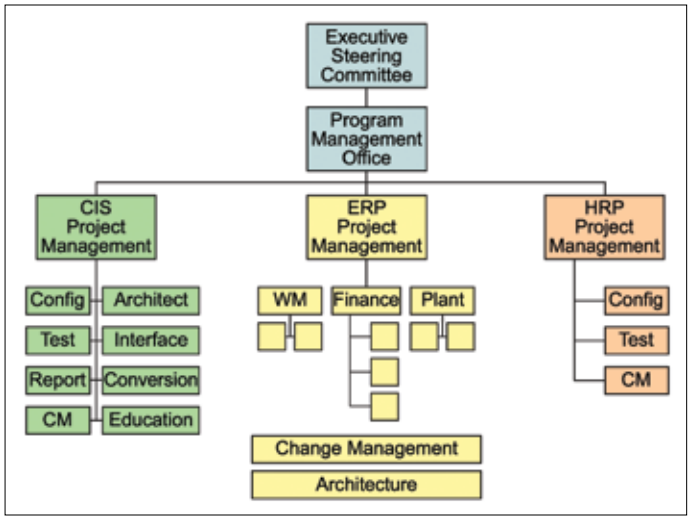


Figure 1: Cobb's CIS implementation took place within the context of two additional projects to replace the ERP and HR systems. The Project Management Office – where managers could discuss and collaborate on issues affecting all projects – coordinated all activity.

Figure 2: Crowded conditions plague almost every major implementation. The number of resources and the length of Cobb's project was a challenge for the Facilities management department.

(Clockwise from top; the conference room converted to a test lab, new doublewide for project resources, renovation of existing office space.)

These eight processes help manage the bulk of the work performed today. They are well documented and are continually reinforced throughout the enterprise. These Foundation Processes are: Project Management, Change Management, Resolution Management, Configuration Management, Software Management, QA & Test Management, Education Management, and Release Management.

A highlight of current operations is the Change Control Board (CCB), which is comprised of vice presidents and COOs from most departments. As part of the Change Management Process, the CCB meets every other week to discuss change requests that meet certain criteria. It approves and prioritizes the requests given to the IS department. This team is the reason the IS department's alignment with the business is so successful.

Cobb Energy kicked off the CIS implementation in March 2004 with a target completion date of November 2005.

The Monkey Wrenches

Six months before the target go-live date, "IT" hit the fan! In the heat of CIS testing and training, the business landscape started to change. Cobb Energy terminated its existing natural gas agreement with SCANA Natural Gas, and Cobb EMC announced it was acquiring Southern Company Gas (now Gas South). For all the right reasons, this was a huge change order to the CIS project.

Cobb Energy reorganized the CIS project into three separate efforts: testing continued where possible, Cobb Energy unwound the SCANA configuration and transferred back its accounts, and work began from scratch on the new gas company requirements. The new gas company acquisition added 12 intense months to the project by incorporating a completely different platform conversion on top of the one for Cobb EMC.

In addition to this huge change order, other distractions to the project required management. They included:

"In order to be an enterprise service provider that values quality and commitment above all else, we had to transform learning into action across the IS organization by implementing a series of foundation processes and change control procedures. This allowed us the opportunity to become a highly efficient project management-oriented service provider. Our success has been attributed to high performance and customer focus."

Tim D. Jarrell
IS Programs Manager
Cobb Energy

- The legacy support company folded. Retaining key resources that understood the old data model and application intricacies was a challenge.
- The contract firm writing the conversion modules changed names and management.
- Hiring a strategic branding agency resulted in a new corporate logo and branding efforts – requiring Cobb Energy to update Web sites, checks, and invoices.
- Nearly half of the IS department had to relocate to a new doublewide trailer while a facility renovation took place. Currently, the "temporary" units are still in use!
- The IS group was tasked with supporting the creation and building of a disaster recovery center.
- The main systems integrator was acquired by a huge company.
- The CIS software company, SPL WorldGroup, was acquired by Oracle.
- And of course, there existed all the staffing problems of any long-term project like this one—people took new jobs, people got married, people had babies, people had serious medical problems, and more people had babies—nine in all.

Fortunately, advanced planning resulted in a strong management team that was able to furnish the Steering Committee with cost-benefit analyses that helped guide major decisions, such as acquisitions. The executive level support allowed the necessary adjustments along the way.

Eventually, there was a light at the end of the tunnel. But with so much riding on a long weekend and a "big bang" double conversion, the light could have been a train approaching at top speed.

Nearing Go-Live

In preparation for go-live, the challenge was to determine whether or not all parts of the project would come together simultaneously. The objective was to achieve a high level of confidence across the organization and affiliates that ensured everyone and everything (infrastructure) was ready. In this case, a "gut feeling" was not sufficient.

Cobb Energy created many documents, checklists, and models to measure the go-live "readiness," but it really boiled down to these three questions:

- Is the IS department ready?
- Are the business units ready?
- Can we maintain operational stability once we say "GO!"?

To reach this high level of confidence, Cobb Energy planned a series of "mock conversions." Each one would have reasonable goals and would build upon the previous one. Cobb Energy established the reasonable goals both to allow the team to see its accomplishments and to enable management to gauge the progress. The organization developed and managed this plan as follows:

- Six mock runs would start four months before go-live, with the last three spaced 20 days apart.
- The team established goals in two areas with many sub-components, including:
- Stakeholder Acceptance
  - Application Functionality. 322 separate items to ensure that application functions were working as designed and data was converted accurately.
  - Application Integration. 126 items to test data integration points.

- Technical Architecture. 73 items to ensure that the architecture would be stable in a production environment.
- Organizational Readiness. 155 items measuring whether or not IS and business groups were ready to convert, use, and support the application.

- Critical Success factors:
  - Will billing be accurate?
  - Can payments be posted?
  - Can deregulation transactions be processed?
  - Can the users access the system reliably?
  - Is the architecture up to the challenge?

Implementation by the Numbers

- Number of customers at start of project: **258,000**
- Number of customers at end of project: **338,813**
- Number of internal IS staff assigned to project: **12**
- Number of business people assigned to project: **18**
- Number of contractors (on and off-shore): **70**
- Time to Implement: **3 years**, including one major redesign/ redevelopment to accommodate Cobb EMC's acquisition of Gas South and termination of previous agreement with SCANA, plus the forward thinking to configure the system to work in an ASP billing services environment.

With so many inputs and components to measure, Cobb Energy needed a quantifiable and measurable system to calculate go-live readiness. For Stakeholder Acceptance, the organization measured current status vs. the ultimate goal using this scale:

- 1 - Ready.
- 2 - Ready but risky.
- 3 - Not ready, with critical work to do.

Go Live Rating:	2.41				
Application Functionality					
Go Live Status Summary	*Average*	*(1) Ready for Go Live*	*(2) Risk for Go Live*	*(3) Not Ready for Go Live*	*Total Items*
Overall	2.26	67	38	101	206
Base Functions	2.31	10	0	19	29
Business Process	1.70	57	13	28	98
Reporting	2.42	0	0	9	9
Conversion	2.61	0	25	45	70

Figure 3: This chart shows how Cobb evaluated its application functionality readiness four months before go-live. The chart's groupings permit managers to identify not just individual problems but entire areas needing significant attention. Color coding further enhances managers' ability to see the big picture.

Measurements for the Critical Success Factors were different. The team established a separate goal for success of each mock run to be able to judge whether or not the progress was acceptable. For instance, 120 days from go-live, Cobb Energy decided that it could achieve a 60 percent bill generation rate. Then it raised the bar higher and higher for each succeeding mock run.

Project

Critical Success Factors-Mock 2

Go Live Status	*Score*	*Success Criteria*	*Current Status*	*Additional Comments*
Overall	1.90			
Ability to Bill	1.00	60% Bill Generation 54% Billing Accuracy	See Accuracy Results	Bill Print issues outstanding
Ability to Accept Payments	1.00	80% Payments Applied Accurately	See Accuracy Results	
Ability to Process AGL Transactions	2.50	65%+ of Consumption (CONS) processed	See Accuracy Results	Some issues with exception situations. Unable to test certain transactions in full volume environment.
CSR Access to Application	2.00	300 concurrent users with average sub 5 second response time.	Tested successfully with 300 concurrent users.	Adjusting architecture settings alleviated timeout problem. Need to monitor at go live.
Stable Technical Architecture	3.00	Full Volume Processing of all batch and online processes.		CC&B Batch window at approximately 10 hours.

Figure 4: This chart shows Cobb's progress on critical success factors 120 days before go-live. Note that for these evaluations, scoring and color-coding represent measurements against the goal for the specific mock run, not against an ultimate desired outcome.

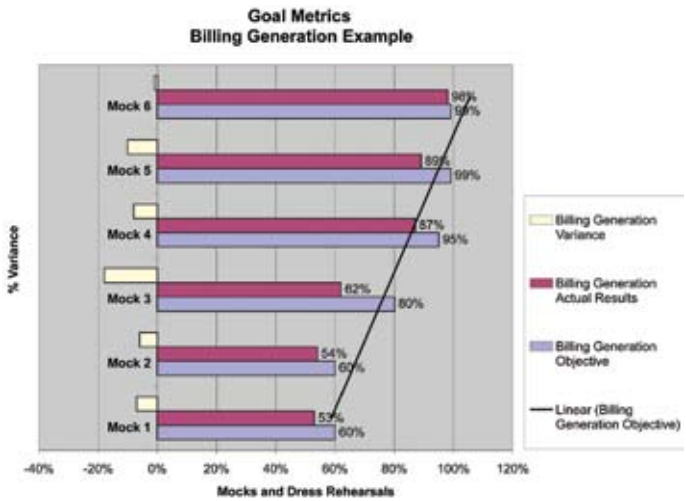


Figure 5: Establishing different goals for each mock run permitted Cobb stakeholders to determine which groups were making adequate progress toward the goal and which were falling behind. In this example, while the billing generation team made progress between mock runs two and three, managers using this chart could immediately identify the need to step up the pace following mock run three.

The final mock run was a resounding success. The team had set very high goals and achieved every one of them. The level of confidence was high enough to pull the trigger on the go-live conversion weekend.

Measuring Success

After a year of operating in the newly overhauled environment, the team took a look back to measure how accurate the estimated savings and productivity improvements truly were. Some of the results include:

- Improved operational efficiency. Cobb has reduced the time needed to complete nightly batch processes, including uploading meter reads, payments, and bill creation, by nearly 80 percent—from 36 hours to seven hours. The organization can clone a separate reporting environment during this window as well.
- Introduction of Web self-service. Customers can now change their profiles, sign up for bank draft payments or electronic billing, view previous and current bills, and request starts and stops of service.
- Combo billing—now done in minutes, not days, with customer-specific messages and bill structure.

- Better communication of the entire severance process. Today, customer service representatives (CSRs) can see all collections activities. They know when letters, calls, etc. are going out. They also know how to use different collection criteria for different customers.
- On-demand billing for immediate bill creation vs. next day.
- Interactive Pay Plan management that lets CSRs analyze customer history and easily determine eligibility. Today, Cobb can achieve better Pay Plan compliance and it has eliminated the majority of escalations.
- Better sales and marketing. Today, Cobb can quickly configure, test, and deploy new rates. CSRs can quickly determine customer rate eligibility for any of Cobb Energy's products and services. The organization has decreased new-order entry time by more than 50 percent and has completely eliminated incorrect rate setup. Cobb has achieved all of this without a separate customer relationship management (CRM) package.
- Reduction in the Cancel/Re-bill time by 80 percent.
- Reductions in the quality assurance team by four people, allowing Cobb to reassign staff to more value-added tasks (i.e. formal testing team, the new Business Intelligence team).
- Elimination of weekend system operators.
- Reduced training requirements from six months to one month, due in large measure to the requirement for staff to take four custom, Web-based training classes before attending an instructor-led class.
- Replacement of manual and paper interfaces with programmed integration with field service, asset management, outage management, and geographic information systems (GIS) applications.
- Standardization across all departments. Enterprise-wide use of Oracle databases and Java development. The reduction from 6,000 reports, letters, forms, and queries to only 300 now.
- Bringing bill and letter design in-house. As a result, the internal staff is able to tailor communications to the customer while also increasing the quality of the bill and literature. Cobb has significantly reduced errors in the final products that previously resulted from miscommunications with third-party vendors.
- Transformation of the application environment from predominately programming to a highly flexible configuration engine. This eliminated the dependency upon more than a dozen contract programmers and allowed the three internal programmers to take on more value-added responsibilities.

Project
Critical Success Factors

Go Live Status	Score	Success Criteria	Current Status
Overall	**1.00**		
Ability to Bill	1.00	99% Bill Generation 99% Billing Accuracy	See Accuracy Results
Ability to Accept Payments	1.00	99% Payments Applied Accurately	See Accuracy Results
Ability to Process AGL Transactions	1.00	99%+ of Consumption (CONS) processed 90% of all other transactions processed	See Accuracy Results
CSR Access to Application	1.00	300 concurrent users with average sub 5 second transaction response time.	Tested successfully with 300 concurrent users averaging less than 2 seconds.
Stable Technical Architecture	1.00	Full Volume Processing of all batch and online processes. Six Hour Primary Batch Window	No reported issues. Batch window well within required time.

Figure 5: The "all green" status gave Cobb management and staff complete confidence that they were ready for go-live.

"With Oracle Utilities Customer Care and Billing, we satisfied approximately 90 percent of our requirements 'out of the box.' We are expecting many years of functional and economic benefits from our new customer care system."

David Johnson, Cobb Energy, COO
(Formerly Manager of Customer Service, Billing & Meter Reading)

As for the ongoing results of the Critical Success Factors, Cobb Energy is maintaining:

- 99+ percent billing accuracy.
- 99+ percent accuracy in payment processing and posting.
- 99+ percent transaction processing accuracy.
- 97.9 percent application up time (excluding scheduled maintenance). Note that since stabilization and a recent upgrade occurred, the application has averaged 99+ percent uptime. Similarly, the network and database uptimes have averaged 99+ percent.

Conclusion

Every IT professional has an implementation war story. Cobb Energy's is undoubtedly not the longest or the most difficult. But what made it all worthwhile was the outstanding success of the results. Everyone on the team knew that all those hours, all those weekends, evenings, and missed family events were worth it. Many people went through the Kübler-Ross grief cycle multiple times. Finally, it has been very gratifying to retrain staff and put employees in ro les where they can have significant job satisfaction – all while providing a quick and rewarding return on investment to Cobb Energy.

Having this success acknowledged at the 2008 CS Week Conference with the Expanding Excellence Award was a tribute to the hard work from many people, including the support from upper management.

But, right when everything seems to be going smoothly, someone throws a new Change Request into the mix. To date, none of the requests have been as large as the ones already completed. They will come, and Cobb Energy's team will be ready for them. ■

About the Author

Bob Arnett *is a North Carolina native, and graduated from Appalachian State University with a degree in Information Systems. Bob has worked in a variety of roles in the IT industry during his career including operators, programmers, practice managers, sales support reps, and VP of Sales. Prior to working with Cobb Energy, Bob spent over 20 years in the IT industry with a number of companies, including 15 years with Digital Equipment and 2 years with Ernst & Young. Bob was hired by Cobb Energy in 2003.*

In 2007, Bob was named the "CIO of the Year" by the Sierra Energy Group, an international award presented to Utility executives. In May of 2008, his team accepted the "Best CIS Implementation" award for their complex installation of Oracle Utilities Customer Care & Billing application.

New Perspectives on NERC CIP Access Management

By John Shaw, Executive VP
GarrettCom, Inc.

A major objective of NERC CIP cyber security standards is to ensure that only specifically authorized people are able to electronically access control systems and Intelligent Electronic Devices (IEDs) that can affect critical power grid operations. To demonstrate NERC compliance, utilities must be able to prove that related protections are in place and vigilantly observed.

As utilities move from learning about CIP standards and related technologies, to the planning and now the implementation phase for CIP processes, CIP teams are gaining additional perspectives into the scope, interrelationships and evolving requirements of secure access management. These perspectives may be grouped into three areas:

Real world implementation

NERC CIP standards are intentionally unspecific in many areas, allowing some interpretation and customization to the current environments of each utility. While there are many important mandates, each utility has the flexibility to adapt implementation specifics to take into account local variations such as existing IT infrastructure, substation communications, control system capabilities, and operating procedures.

Preparation for "Life under NERC CIP"

NERC CIP compliance is not a static achievement. Becoming compliant is not just getting to "done", but rather getting into position to execute ongoing procedures. Successful compliance includes looking ahead and implementing tools and processes that are the least burdensome to sustain over time.

Anticipation of ongoing change

Cyber security is a dynamic landscape, continually altered by new threats, developing technology and inevitable changes to NERC CIP requirements as they undergo refinements of technology and of the definition of critical assets. Current implementations must remain flexible enough to accommodate a changing technological and regulatory environment.

Successful management of each of these perspectives affects system architecture, network architecture and operations processes.

Implementation in the Real World

The basic elements of access management for CIP include:

- Identifying Critical Cyber Assets (CCAs) -- applicable to all of NERC CIP,
- Establishing an Electronic Security Perimeter around CCAs,
- Identifying and screening key personnel,
- Defining user profiles for each person, i.e., limit what they are allowed to access,
- Establishing a 2-factor authentication mechanism for users,
- Authorizing each permitted access event against individual user profiles,
- Logging all accesses and provide related reports and audits,
- Identifying, logging and alerting on all exception events,
- Supporting ongoing changes to users, CCAs, the network and device passwords, and
- Providing back-up and recovery tools for access management systems and processes.

These specific requirements can be met in a variety of ways, but an overall goal is to tailor the implementation to limit the disruption to the current operating environment and to simplify the overall project.

Many utilities already have a user authentication infrastructure within their Enterprise IT environment. Common technologies include Microsoft Active Directory, used for coordinating user authentication over multiple systems, and RSA SecurID servers, used to provide two-factor authentication, i.e., a password (something you know) and an RSA token (something you have). Most current IEDs or older control systems do not support these services directly.

Access Management Systems Can Integrate IT and Substation Networking

A new CIP Access Management System (AMS) can bridge the substation world with current IT tools both by functioning as the secure gateway for legacy devices and by interoperating with existing Enterprise authentication services.

One possible system architecture for initial implementations is shown in **Figure 1**. The basic steps for user access to IEDs in this architecture would be:

- The end user activates a secure access client software application on their PC.
- The end user is transparently connected to the AMS server, which obtains credentials from the end user and interrogates Active Directory and/or RSA SecurID servers as well as its internal security profile data base to authenticate the user and validate authorized target devices.

- The end user clicks on a desktop directory icon for the authorized target IED.
- In active coordination with the router/firewall/gateway at the substation, the AMS establishes a secure connection to the target IED and connects the end user to the IED, as if to the IED's front panel port.
- AMS client software on the end user PC selects and initiates the appropriate vendor-specific application program on the PC for use with this IED, if applicable.
- The AMS server logs every access event and, optionally, all activity during the user session.
- The AMS retrieves additional event logs periodically from the substation router/firewall/gateway and receives any exception alerts for additional security monitoring and audits.

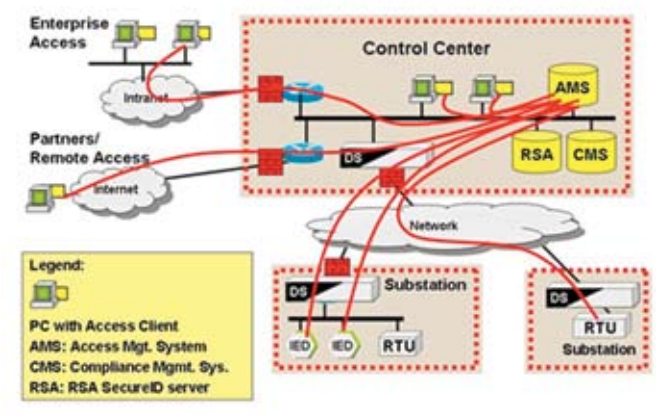


Figure 1: Access Management Architecture

Some utility cyber security implementations have additional active mechanisms in place to detect and alert on forms of attack that are more complex than a direct login attempt. An example is an Intrusion Detection System (IDS) that looks for patterns of attack such as aggressive transmissions to exposed protocol ports or other vulnerabilities in host operating systems. IP Firewalls at the control center and at substations may also detect basic network attacks (or simply misguided packets) that also constitute security events.

To manage these diverse sources it is desirable to link firewall events, AMS events and IDS events to a common Security Event Management console, as shown in **Figure 1**.

Access Management must also integrate with the substation network itself. For ease of initial implementation, an AMS may interoperate with a wide variety of substation gateway devices on a secure basis. Possible substation gateways may include existing serial communications processors (e.g., SEL 2020/2030), WAN router/firewalls, some serial-IP terminal servers, telephone-line-sharing switches, and other vendor-specific devices.

While there may be many devices that interoperate with an AMS for interfacing to serial IEDs, some may fail to provide either a complete Electronic Security Perimeter function for the substation (e.g., firewall non-AMS-related SCADA connections) or the required level of event logging. A comprehensive substation access gateway would incorporate:

- WAN connectivity,
- IP routing,
- Stateful ("TCP connection-aware") IP firewall,
- IPsec VPN,
- Direct connectivity for serial devices, Ethernet devices and Ethernet LAN, and
- Secure connection management with the AMS for both serial and IP sessions including logging of sessions and alerting of any exceptions.

Many utilities will end up with more than one configuration type for substation communications, accommodating different situations. Variations include use of an integrated router/firewall/gateway, use of a secure telephone-line-sharing switch for dial-up substations, and the use of multiple devices in series, such as a router/firewall with a serial communications processor. (**Figure 1** shows how an AMS architecture can work with this variability.)

Living in a NERC CIP World

Utilities may complete implementation of a CIP-compliant framework by the appointed ready date, July 1, 2009, but compliance will never be truly completed. Compliance requires keeping security technologies current and diligence at administrative tasks of record keeping, change management and periodic audits. It is critical that tools be put in place to minimize this administrative overhead.

One such tool is an Access Management System that also supports additional compliance management tasks beyond pure access control. An AMS can be used to automate the maintenance of records in ways that promote flexibility and reconfiguration. For example:

- The AMS holds an inventory of all the IEDS and systems that users may have access to. By flagging those devices designated as Critical Cyber Assets (CCAs), the AMS becomes a repository of the current CCA inventory information and can be used to produce audit reports and to manage changes to the official CCA list.
- An authorized user list may be used as a control point for physical access control systems and other personnel-related CIP functions.
- An AMS can provide scheduled updates of individual or related groups of IEDs – or of specific IEDs when special concerns arise, in compliance with the CIP requirement that all IED and system passwords be periodically changed.
- An AMS can pull log files from remote gateways and archive these automatically on a regular basis for audit purposes, without operator intervention.
- An AMS can manage other file types, such as configuration files and IED logs, and assist with administering and updating software for selected substation devices.

Secure access procedures designed to keep intruders out can also make access difficult for authorized users. A well-implemented AMS architecture can reverse this effect and make remote access even easier than before CIP.

By using an AMS, such as the Crossbow™ Secure Access Manager, which is purpose-built for the substation environment rather than using generic IT access tools that do not understand the protocols, devices and software applications common to utilities, it is possible to enhance end user productivity in ways such as:

- Organizing the IEDs that are relevant to that particular user -- essentially only those that the user is allowed to access -- into graphic-assisted directories, grouped into various combinations of region, substation or device type.
- -Supporting PC software that provides click-through access to the target IEDs, making the network connection and session logging functions transparent to the user.
- Associating the appropriate vendor-specific software application on the user's PC, such as AcSELerator, WinECP or Enervista, with each target IED, enabling AMS client software to automatically launch this application, further simplifying on-demand IED access.

Anticipation…

NERC CIP standards have been criticized for not going far enough in securing the power grid from sophisticated attacks. Researchers have made considerable efforts to identify and demonstrate potential security breaches, revealing vulnerabilities that the minimum CIP standards may not remedy. Also, the current standards only apply to the relatively small percentage of overall utility assets considered "critical" under the definitions of the standard. While the primary transmission grid is addressed, billions of dollars of utility assets are left unprotected.

Regulators have signaled that the CIP standards will likely be expanded. This will include technical details from additional expert stakeholders to strengthen defenses and to react to the evolving nature of cyber threats. The standards will also likely spread to more utilities and substations, if not by regulation, than at least by "best practices" as IT influences extend more into substations and as utilities become generally accustomed to cyber protections as the normal way of business.

Implementers are already taking steps to prepare for such change. At a detailed level, an AMS and remote gateways may be selected that have a wide variety of embedded security technologies. As standards evolve, there will be flexibility in implementing one or a combination of technologies, such as IPsec Virtual Private Networks (VPNs) with various strong encryption and key exchange algorithms, SSH port forwarding, Secure FTP, and SSL protocols applied to both serial and IP-based end devices. There is no need to rely on one specific technique becoming the preferred standard, since highly flexible devices are available.

Similarly, the server technology for centralized server elements of the AMS can be built on standard IT platforms so that they benefit from evolving major vendor tools and standard IT security practices.

Substation networking flexibility becomes even more important as more substations, including more distributed and smaller substations, fall within the utilities' cyber security plans. While some access management architectures feature a single vendor-specific substation gateway option, other AMS architectures utilize a wide variety of remote gateway types. Options may include multiple gateway form factors, support for different WAN network services, preferred partner products for complementary requirements, and a generally open secure network architecture to integrate additional products as required over time.

Additionally, more enhanced cyber security functionality will be required locally within major substations over time. This may include local IDS systems or user authentication services within the substation, with databases and administration tied into central AMS servers and processes. Deployment should include a roadmap supporting a substation-based IDS/authentication server.

Choose Adaptive Technologies and Keep Moving Forward

The clock is ticking. Utilities are only several months from the mandatory NERC CIP compliance date. Implementation is accelerating, even while the learning curve continues for many. Fortunately, utilities have many potential technologies and partners to work with, including access management solutions created specifically for the world of substation operations.

Project teams can find flexible, proven access management technologies that can adapt to particular utility environments to make implementation simpler, less disruptive, less risky and less costly. Ongoing processes can be highly automated to reduce administrative overhead and system interfaces can be designed for ease-of-use to increase end-user productivity accessing remote substations.

And, while it is hard to anticipate all the new cyber security threats and regulations that may emerge, it is possible to implement open-ended solutions that cover many extra bases and leave future options open. The common theme for overall success is to pick a substation-centered security solution that is highly adaptive, simplifying the initial project and facilitating long-term operations. ■

About the Author

John M. Shaw *is Executive Vice President of GarrettCom, Inc., a leading supplier of substation-hardened networking products. Shaw leads GarrettCom's planning for NERC CIP cyber security compliance solutions and is an active speaker and writer on network security. He has more than 25 years experience in planning utility- and carrier-grade data networks, telecommunications technical marketing and executive management, including positions at Tellabs, Newbridge Networks (now Alcatel-Lucent) and NYNEX (now Verizon).*

Contact him at jshaw@garrettcom.com

The Intelligent Communications Platform, or Putting the 'Smart" in the Smart Grid

By Paul Karr, Vice President of Market Management
Trilliant Incorporated

The Wakeup Call Has Sounded

The energy grid wakeup call rang loudly after decades of growing energy use and a false confidence that the grid would somehow always find a way to serve its users. The 2003 blackout in the northeast United States and Canada that affected more than 50 million people gave both users and providers a message that status quo wasn't good enough.

Since then there has been a growing push for improving the North American power grid toward what we now call a Smart Grid; one that introduces pervasive communications and embedded intelligence while providing for much broader consumer engagement, and more diverse operating requirements.

In fact, legislation in both the U.S. and Canada has pushed infrastructure investments in technologies intended to put the 'smart' in Smart Grid and thereby address critical energy issues. The Energy Policy Act (EPAct) of 2005 mandated that each state evaluate the business case for advanced metering infrastructure. In Ontario, the Energy Conservation Responsibility Act of 2006 mandated deployment of smart meters to all consumers by 2010. The U.S. Energy Independence and Security Act of 2007 (see **Figure 1**) expands support from the U.S. government for investments in Smart Grid technologies while further emphasizing the need for the power industry to play a leadership role in addressing carbon dioxide emissions affecting climate change.

Recent state-level legislation and growing consumer sentiment suggest an increasing appetite for making investments in distributed clean technology energy solutions. Distributed generation technologies such as solar, wind, and biodiesel are becoming more readily available and have the potential to significantly improve grid operations and reliability while reducing carbon emissions.

1. Increase use of digital information and controls technology to improve reliability, security, and efficiency of the electric grid.
2. Dynamically optimize grid operations and resources with full cyber-security.
3. Deploy and integrate distributed resources and generation, including renewable resources.
4. Develop and incorporate demand response, demand-side resources, and energy-efficiency resources.
5. Deploy "smart" technologies – real-time, automated, interactive technologies that optimize the physical operation of appliances and consumer devices – for metering, communications concerning grid operations and status, and distribution automation.
6. Integrate "smart" appliances and consumer devices.
7. Deploy and integrate advanced electricity storage and peak-shaving technologies, including plug-in electric and hybrid electric vehicles, and thermal-storage air conditioning.
8. Provide timely information and control options to consumers.
9. Develop standards for communication and interoperability of appliances and equipment connected to the electric grid, including the infrastructure serving the grid.
10. Identify and lower unreasonable or unnecessary barriers to adoption of Smart Grid technologies, practices, and services.

Figure 1: Smart Grid capabilities defined by the Energy Independence and Security Act of 2007. More than half of the ten elements that define the Smart Grid directly relate to or involve advanced communications or an intelligent communications platform.

What is the Nervous System for the Smart Grid?

While the electric power distribution grid today provides a critical role in the delivery of energy services, it does so with limited visibility into system performance and customer behavior. A Smart Grid requires a sophisticated nervous system that will provide increased reliability, interoperability, two-way communications, risk-managed services, and will support changes to the grid as new power resources are added while empowering consumers to be able to better address their energy and financial needs. To be intelligent, the grid's nervous system must answer the need for pervasive communications.

Today the Smart Grid industry is largely nascent and proprietary while the future demands solutions that are fast, interoperable, reliable, and able to mitigate risk while accelerating benefits, operating efficiency, and customer satisfaction. The Smart Grid's intelligence lies in the interconnection of communications technology including voice, mobile, and fixed data and intelligent standards, for plug-and-play networks on a global scale.

As the Smart Grid evolves, every device added to the communications network has the potential to add intelligence to the system overall, providing for new network-based applications in addition to traditional point solutions. A core business driver for the adoption of an intelligent communications platform is to support smart metering applications, also referred to as advanced metering infrastructure (AMI). AMI involves automated measurement of time-of-use

energy consumption – hourly, 15-minute or 5-minute intervals – and provides for new time-of-use rates that encourage consumers to use energy during off peak hours when generation costs are low, rather than peak periods when generation costs are high and the grid is under stress.

With time-of-use rates, consumers may continue to use power during high peak periods but will pay a higher price to do so. AMI may also include remote service disconnect functionality that can reduce costs associated with site visits otherwise required to manage move-out/move-ins or to support pre-payment programs.

Other Smart Grid capabilities that may be realized through the deployment of intelligent communications include improved outage management detection and restoration monitoring, revenue assurance, and virtual metering of distribution assets achieved through associating and aggregating metering data.

As Ahmad Faruqui of The Brattle Group – a firm that provides consulting and expert testimony in economics, finance, and regulation to corporations, law firms, and governments around the world – has underscored, "The need for two-way communication between the utility and its customers lies at the heart of all Smart Grid initiatives. Such communication allows dynamic pricing to be transmitted to customers and it also enables customers to automatically curtail usage during critical hours and to shift energy consumption from high-priced peak periods to low-priced off-peak periods. In this fashion, both parties work synergistically to manage the cost, delivery and environmental impact of power generation and energy services delivery."

Intelligent Communications Network Basics

Modern communications network solutions leverage standards-based technology, such as IEEE 802.15.4, thus providing robust two-way wireless mesh network communications to a broad range of sensor and control devices. An intelligent communications platform provides for much greater ability to market new offerings to targeted customers based on their energy consumption profiles while also empowering consumers with new tools and access to information providing for a greater control over energy costs and improved satisfaction.

The intelligent communications platform should provide for remote firmware upgrades to connected devices and be capable of leveraging Internet protocol (IP) based communications across multiple wide area network (WAN) platforms (**Figure 2**).

Also critical for leveraging a communications infrastructure investment is support for broad interoperability and interconnectivity, as embraced by the following guidelines.

- Interoperability for AMI applications means supporting a broad range of options for metering devices.
- A communications platform should be meter-manufacturer independent, empowering choice for utilities. This provides for current and future competitiveness for the meter itself, which is one of the more expensive elements of the smart metering solution.
- Interconnectivity for communications platforms refers to the ability to support a broad range of functions, both end point devices as well as systems at the head end.
- To support demand side management and energy efficiency initiatives, an intelligent communications should support programmable communicating thermostats (PCT), in-home displays (IHD) and load control switches. Ultimately, an intelligent communications platform should support a model whereby third-party manufacturers can develop solutions that operate on the network providing competitive options for utilities.
- For enterprise system interconnectivity an AMI, demand side management or other Smart Grid head-end application should be developed using service oriented architecture (SOA) principles and Web technologies.
- These applications should also support modern Web services-based solutions, providing published simple object access protocol (SOAP)-based APIs. Utilizing this approach provides for easier integration to existing enterprise systems as well as simplifying the process of adding functionality, either through enhancements provided by the vendor or add-ons delivered by third parties or developed by the utility.

Finally, the value of an intelligent communications platform deployment is driven by the ability of other enterprise applications and processes to utilize the vast amount of new data received through the AMI, demand side management and Smart Grid applications.

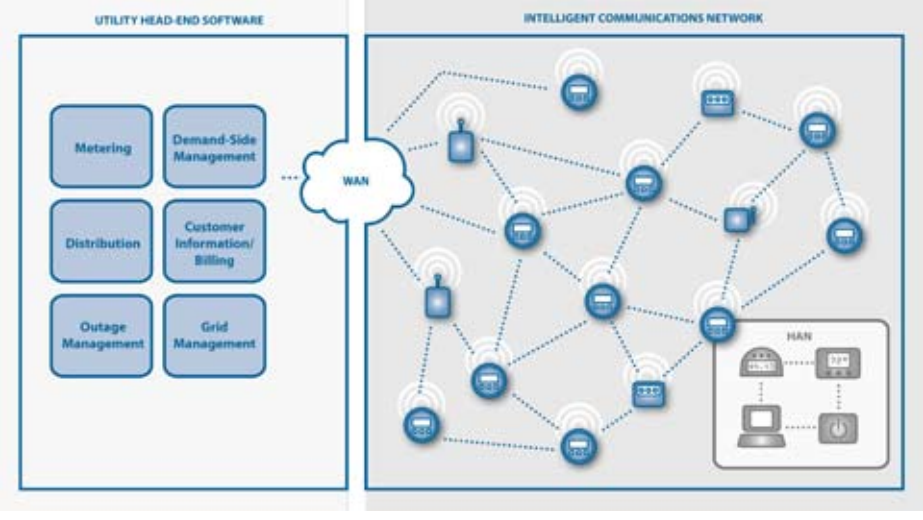


Figure 2: A mesh network configuration provides an intelligent communications platform.

Core areas of extended value include integration with:

- Customer information systems
- Call center processes
- Outage management systems
- Work management systems.

How Utilities and Customers Employ the Smart Grid

While the Smart Grid encompasses a combination of hardware and software built atop an intelligent communications infrastructure, it also requires tools for consumers and utility companies alike to help manage, monitor, and respond to energy requirements. The flow of electricity from utility to consumer becomes a two-way conversation, saving consumers' money, delivering more transparency about end-user usage to the utilities, and reducing carbon emissions. In some cases, consumers could even be compensated for their efforts to minimize their carbon footprint, even to the point where consumers can sell the energy generated through renewable sources at home back to utility companies.

E.ON U.S. subsidiary Louisville Gas & Electric (LG&E) serves nearly 400,000 electric customers in the greater Louisville area. LG&E is currently working with Trilliant on a responsive pricing program that incorporates time-of-use pricing with a real-time, critical peak pricing component, as well as Demand Side Management (DSM) tools for those customers who choose to participate in responsive pricing.

The implementation of this variable rate structure is possible through the use of an intelligent communications platform that integrates smart meters (electric and gas), energy use information displays and DSM equipment such as programmable thermostats and load control switches for customers in some homes and small businesses. Automation of major energy appliances empowers participants to shift usage in response to rate changes without manual intervention.

Figure 3: LG&E Smart Grid Equipment Display helps customers understand usage, configuration and benefits.

The power usage management program is designed to learn about whether keeping customers informed about electric rates and their own consumption will spur them to use power more judiciously. The communications platform supporting the program utilizes a wireless mesh network based on the IEEE 802.15.4 standard.

Devices that interact on the network include programmable thermostats, load control switches, in-home energy use displays, as well as electric and gas interval meters. The mesh network utilizes multiple wide area network (WAN) backhaul options including Wi-Fi, digital cellular and fiber, providing for selection according to least cost and best performance.

According to Greg Fergason, Demand-side Management Program Manager at E.ON U.S., the question that LG&E wants to answer is whether giving customers more information and greater control over energy usage will encourage them to use less power or shift usage to periods of lower demand. The goal is to make it easy for the consumer to do the right thing with respect to their energy usage. They will get their answers through the improved information management provided by this framework.

At Hydro One, one of the ten largest transmission and distribution utility companies in North America, and the largest electricity delivery company in Ontario, Canada's most populous province, they are well on their way to installing smart meters in all homes and small businesses by 2010. The Smart Meter Project is part of a larger undertaking in Ontario that will mean building almost a whole new electricity system by 2025, including replacing 85% of its current generating systems as they retire over time, and expanding the system to meet future growth.

To do this, Hydro One has built an award-winning smart meter solution based on a 2.4 GHz RF mesh intelligent communications network foundation. This Smart Grid plan is designed to maximize flexibility and interoperability in a customer base that is a mix of urban, rural and remote customers. Some of the latter are accessible only by air, rail, boat, or snowmobile.

According to Myles D'Arcey, Senior Vice President, Customer Operations at Hydro One, the utility sees the Smart Grid as representing the future of energy management for the company and for its customers. The company

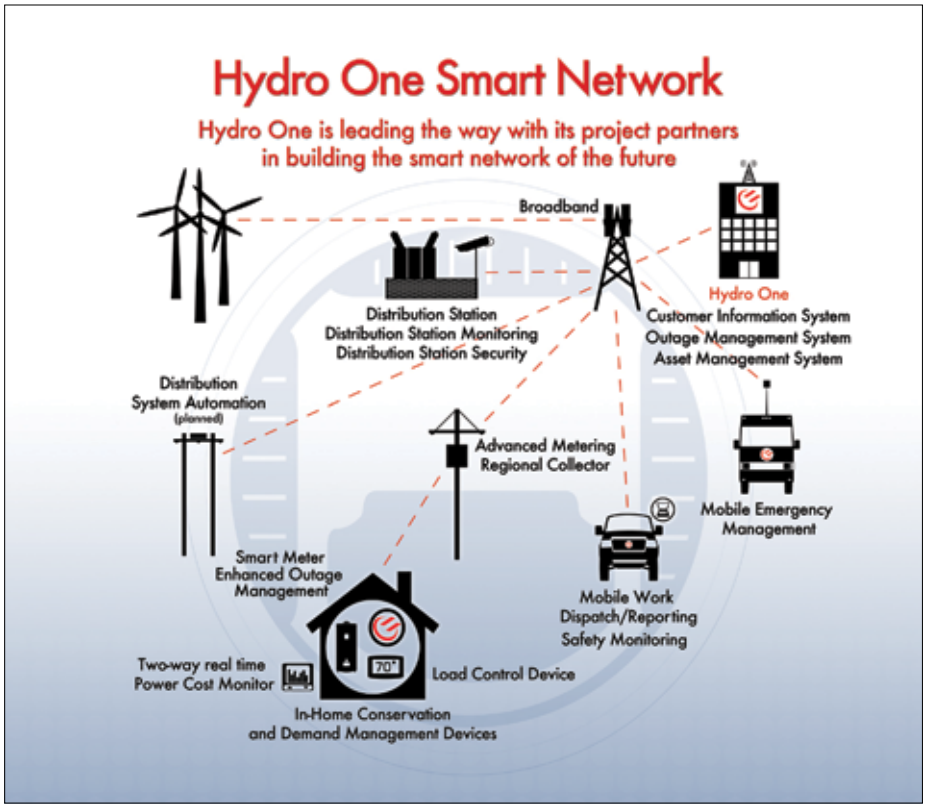


Figure 4: The Hydro One Smart Network.

is close to its target of installing a total of 610,000 meters by the end of 2008 and 1.3 million meters by 2010.

Ontario's Smart Grid includes a two-way self-healing mesh intelligent communications infrastructure that is based on non-proprietary, high bandwidth enabling industry standards (2.4 GHz IEEE 802.15.4) that enable use of data from many types of devices from a broad range of manufacturers for meters, load control, in-home displays, distribution monitoring and control, and head-end software applications. The information is available on customer information, outage management, asset management, geographic information and work execution systems.

One unique feature of the province's smart meter deployments is its centralized Meter Data Management Repository (MDMR), including a paperless change meter order process that handles the needs of all local distribution companies across the province and its geographically dispersed work force. The system is designed to transition customers from conventional rates to time-of-use pricing in the near future.

Integration of Distributed Generation Resources into the Smart Grid

While reliability and lower-cost electricity remain the key functions in the Smart Grid, deployment and integration of distributed generation, including renewable resources, are important supply side elements of the Smart Grid vision and should not be overlooked. These may include installation of arrays of solar photovoltaic panels on home and office roofs, solar carports, small wind (3-5kVA) turbines, small biogas turbines, and fuel cells.

By integrating these resources into a common communications platform, utilities have the opportunity to develop solutions that achieve a much greater result than simply the sum of independent systems. For example, intelligent plug-in hybrid electric vehicles (PHEV) connected to a smart solar carport may choose when to purchase power for charging the car or even to sell power back to the grid in a vehicle-to-grid (V2G) model based on dynamic price signals received through the communications platform. And, by maintaining intelligence at the edge of the grid, consumers and distributed resource owners can be empowered to manage to their own energy usage and benefit the grid as a whole.

Global climate challenges and system reliability are providing the drive, but technology, legislation and consumer interest will provide the extra stimulus to drive Smart Grid infrastructure investments in the coming decades.

With the realities of global warming and the concern of system reliability, there is a growing sense of urgency to take action. A future without a Smart Grid equals increasing power outages, severe strains on the grid, and uninformed and 'un-empowered' users. An intelligent communications platform underpinning the Smart Grid provides an important foundation capable of supporting multiple devices in multiple environments – commercial, industrial and residential – working seamlessly together in a single unified network.

All the technical assets of a Smart Grid can be managed holistically rather than as isolated or poorly connected parts. The power of a network grows geometrically according to the amount of resources and assets actively connected to it. It is the future of the Smart Grid, and it is available today – making this the time to embark on realizing the vision of a Smart Grid. ■

About the Author

Paul Karr *has more than 20 years of experience across marketing, sales, and business development. Before joining Trilliant he held executive positions in marketing and product management at Sun Microsystems where he played an instrumental role in the successful integration of SeeBeyond Corporation. Prior to Sun, Karr was Director of Strategic Alliances at CellNet Data Systems where he helped guide strategy through the acquisition by Schlumberger. Karr has a Master of International Business degree from Seattle University and a BSEE from the University of Washington.*

Long-term Memory Loss: Where did the time go?

By Kevin McCarty, Co-Founder and Executive Vice President
West Monroe Partners

The Wakeup Call Has Sounded

The United States Department of Labor claims nearly half of the energy utilities workforce consists of Baby Boomers. As many will be reaching retirement during the next 10 years, a manpower shortage looms. Forward-thinking energy utilities have the opportunity to plan initiatives now to address this impending problem in the future, while separating themselves from sheer tactical competitors. This article offers an overview of critical issues… and some possible approaches.

The aging workforce in the energy utility industry has been well documented, and the fear of losing skilled labor is very serious and real. According to the United States Department of Labor, the energy utility industry averages the second-highest average employee age among 54 industries studied. Nearly one-fifth (19.2 percent) of industry workers are within five to seven years of retirement. Perhaps the most alarming statistic involves age distribution, as illustrated in the chart below. The average age of an energy utility employee is steadily rising; since 1995, the number of industry workers aged 55 and older has increased by 225 percent.

How did this happen?

With the threat of new competition at bay, deregulation spurred a movement for consolidation of operations throughout the industry. Organizations employed cost reduction tactics such as hiring freezes and downsizing. Efforts to recruit college graduates and early- to mid-level employees ceased while natural downsizing favored more experienced, longer tenured employees. In addition, the industry experiences little voluntary turnover as a whole. Promotions are often made from within, and oftentimes years, if not decades, of on-the-job training are invested in each senior employee.

I guess this is goodbye…?

The first concern that comes to mind is loss of physical headcount. Average age, average tenure and age distribution statistics indicate that energy utilities are either not actively recruiting or retaining young talent successfully. Certainly, public perceptions of an "antiquated" industry do not aid these efforts. Customers don't perceive the industry to lead in technological innovation—after all, power is power, and it is a commodity, so what has changed about it over the years, right? And, issues such as pollution and high or increasing energy price rates tend to project the image of industry staffers to be the unenviable equivalent of an Internal Revenue Service agent.

On the positive side, once an individual is employed by an energy utility, he/she stays. Promises of frequent promotion potential and competitive pay and benefits packages tend to keep employees on board. In 2006, the energy utility industry boasted a median tenure of 10.4 years—the highest average by more than three years among industries analyzed by the United States Department of Labor, Bureau of Labor and Statistics.

On the flip side, longer tenure signifies a higher capacity for industry-specific skill sets and critical intellectual capital that individuals possess. It is the loss of this technical know-how and critical knowledge that dominates the minds of executives—more so than the dwindling of sheer manpower numbers. In addition to addressing a potential labor shortage, energy utilities must find ways to collect retiring workers' institutional knowledge before that knowledge leaves the organization entirely.

Forward-thinking energy utilities have the opportunity to plan initiatives now to address this looming problem in the future, while separating themselves from sheer tactical competitors. Through strategic re-branding efforts and technological investment, energy utilities can obtain, mentor and train the young, technically savvy talent saviors from Baby-Boomer retirement doom.

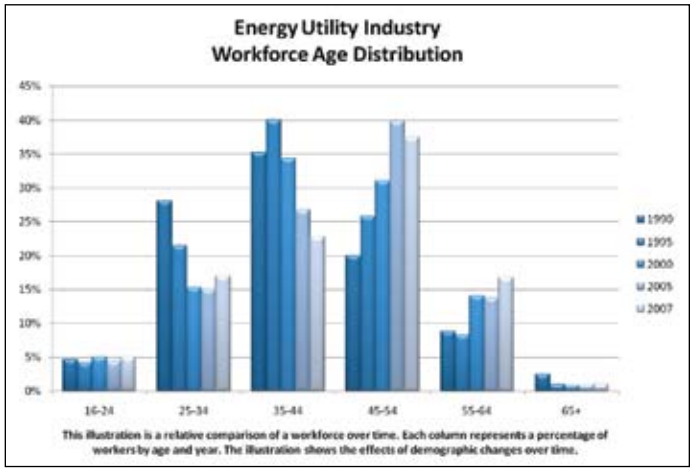


Chart Source: United States Department of Labor, Bureau of Labor and Statistics

Extreme makeover

Hiring young talent offers the most potential for addressing this issue. But, there is a major barrier: young workers today have little desire to work for energy utilities. Indeed, these younger generations view the industry as old, antiquated, and archaic. They seek vibrant cultures, challenging opportunities with tremendous upward mobility potential, diverse environments, and cutting-edge ideas and technology usage. Many don't equate a utility company with a place where they can obtain that kind of working environment.

Have you ever seen the show *Extreme Makeover*? Welcome to the "energy utility" episode. If they are to overcome these built-in biases, the industry must address its image problem by looking in the mirror and changing virtually everything that does not appeal to Millennials. Or, at least, it must change Millennials' *perception* of the industry.

The banking industry offers an appropriate role model for this effort. In an industry once known for stodgy, pale colored interiors and as a career destination for "lifers" who never expected to change jobs or climb the corporate ladder, pioneering banks took some key steps. They made things fun and lively, promoting diversity, collaboration, and career development. They changed everything from the career model to the physical structure to appeal to young talent. A prime example of creating such an environment is Umpqua Bank's exceptional growth from a 40-person community bank to a 128-branch entity with a strong western United States presence.

In his book *Leading for Growth: How Umpqua Bank Got Cool and Created a Culture of Greatness*, Ray Davis (co-written by Alan Shrader) explains how his creative leadership approach facilitated this success, including hiring a cutting-edge design firm to revamp the retail layout and modernize its appeal.

Employees were required to answer the phone with a cheery "World's Greatest Bank," which invoked a fair amount of criticism amongst industry counterparts. However, this gesture was just one small step in the transition into a positive, winning corporate culture. Far from the conventional methods for training bank tellers, Davis sent his employees to Ritz-Carlton to learn customer service. His appreciation for employees and dedication to change re-defined the retail banking world. While this is an industry-specific example, the basic premise behind Davis' approach was to challenge the current thinking, find new ways to motivate employees and, ultimately, attract customers.

Energy utilities will also need to address the Millennials' dedication to preserving the environment. Millennials are passionate about saving the Earth. One recent study shows that 78 percent of Millennials believe that companies have a responsibility to join them in efforts to better the environment, and nearly 80 percent of Millennials want to work for a company that cares about how it contributes to society.

Energy utilities must promote their investments in technologies that preserve the environment, not to mention their efforts to generate an increasing portion of their energy portfolio through renewable sources. Millennials may at first dismiss the notion of such companies contributing to a greener planet (and can you blame them with the historic dependence upon fossil fuels?), but they can be convinced. If they want to dedicate themselves to a job where they can contribute to the environment, then they can become a utilities team member who builds business cases to increase investment in renewable energy sources.

Can't we all just get along? Bridging the gap

Once young talent has been recruited, they must be retained and a massive transfer of technical- and industry-specific knowledge must occur before the Boomers retire. Ideologies, preferences, motivations and general attitudes differ greatly between Millennials and Baby Boomers. Closing this divide is critical to successfully transitioning key information.

Management must nurture a close-knit interaction between the two groups, and career-hungry Millennials will need to pick the brains of Baby Boomers. Without a doubt, facilitating a dynamic, new culture will require a serious change management effort.

This change effort must increase the awareness of differences between Millennials and Boomers, enable each group to appreciate the strengths of the other, and manage the differences effectively. For Millennials, companies may consider redesigning office space to encourage collaboration, assigning projects to groups of employees who are evaluated as a group for reaching a goal, and establishing a mentoring program. At the same time, companies must continue to connect with boomers through steps such as emphasizing the importance of respect, facilitating face-to-face conversations, and re-teaching the corporate history to all employees.

Millennials are eager to absorb industry knowledge. With a newly created comfort level between the two groups as well as some coaching, they can effectively drill in to the business processes and key "secrets" of the Boomers' daily operations, thus capturing industry knowledge before the mass retirement movement.

The future is technological empowerment

Once Millennials and Boomers have bridged the gap, the company can extract core and previously undocumented business processes from workers' minds and then analyze and streamline them to reduce costs and create efficiencies. Tools such as enterprise content management applications can help to preserve intellectual capital, socialize process changes, and bring other advantages to the table.

New technologies also back up companies' commitments to preserve the environment:

- Smart Grid consists of a transformed electricity transmission and distribution network that uses two-way, communications, advanced sensors and computers to improve the efficiency, reliability and safety of power delivery and use.
- AMI is a system to measure, collect and analyze energy usage, from advanced devices such as electricity meters, gas meters and/or water meters, through various communications media on request or on a predefined schedule. Among other benefits, it reduces gas emissions by requiring fewer trucks dispatched to read meters.
- Renewable energy solutions have become popular as concerns rise about the exhaustion of fossil fuels, as well as environmental, social and political risks associated with continued extensive use of fossil fuels and nuclear energy. Efforts to extract oil from even deeper reservoirs are increasing and the costs of renewable energy technology have been shown to fall with increased investment and capacity expansion.

Alternative solutions

Consolidation with similar organizations also provides a path for addressing aging workforce issues. While it does not offset the need to recruit and retain young talent, consolidation gives companies the opportunity to address the loss of utility-specific labor and intellectual capital by pulling the best parts from multiple entities—lessening the blow of the retirement boom.

In fact, the industry currently is experiencing some consolidation due to rising fossil fuel prices and increased competition brought about by deregulation. But, every major industry player faces aging workforce issues; even if one company acquires another and doubles the size of its employee base, it is essentially doubling its amount of Boomers and its potential for mass retirement.

A final option is importing young talent from beyond domestic borders. If young local workers do not want to work in the energy utilities industry, then the only other opportunity to add young talent is through broadened international initiatives. On a global scale, the opportunity to work for a U.S.-based corporation continues to be a very attractive one, regardless of industry perception, and advantages exist with lower salary expectations, at least in some cases. This strategy, however, presents the same need to "bridge the gap" that exists with Millennials—and combining potential cultural issues with political attitudes in this traditionally conservative industry means the gap could be as wide as the Grand Canyon.

Close the drain, and fill the sink back up!

All signs point to a mass retirement movement within the energy and utilities industry, but top-tier organizations have an excellent opportunity to minimize the exodus of industry-specific talent and critical knowledge. Those that maintain a strategic vision to integrate intelligent solutions into their core operational procedures, prepare their people to succeed in a new environment, and maximize technology to support the enterprise will be in the best position to face and overcome these looming obstacles. ■

About the Author

***Kevin McCarty**, co-Founder and Executive Vice President of West Monroe Partners, offers more than 15 years of global business and technology consulting experience across multiple industries. He serves clients as a Solutions Executive and Architect combining strategy, financial, people, process, and technology elements to deliver technology-enabled business change. West Monroe Partners helps organizations address cultural changes and prepare workforces to achieve business objectives. For more information, please contact Kevin McCarty, kmccarty@westmonroepartners.com.*

Secure Super Grids Boost Reliability and Capacity of T&D Assets

By Jack McCall, Director of Business Development
T&D Systems, American Superconductor

About Superconducting Cables…

The need for modernization of the electric power grid is well documented. This effort will entail not only construction of new cross-country transmission lines, but also increasing the reliability and supporting the growth of more concentrated urban loads. Both will require a robust and stable transmission and distribution infrastructure. American Superconductor Corporation (AMSC) introduced a unique technology in 2007 as a secure, system-level superconductor cabling solution that increases both the capacity of T&D infrastructure and the fault current handling capability of dense urban circuits.

High-capacity, very low impedance superconductor cables that offer significant power density advantage over traditional copper-based cables have been well demonstrated at electric utilities and are now being deployed in the grid. Three of these cables have been energized in the United States over the past two years. Stand-alone fault current limiters based on superconducting materials also offer a new vista in grid security and technical control of system operating parameters.

AMSC's Secure Super Grids (SSG) technology combines the benefits of both superconductor technologies. This proprietary, system-level, 'intelligent grid' solution utilizes customized superconductor power cables and ancillary controls to deliver up to ten times more power than conventional copper cables while at the same time suppressing power surges - or fault currents - that can disrupt service. This unique technology allows for the construction of multiple paths for electricity flow in metropolitan power grids to ensure system redundancy when individual circuits are disrupted due to severe weather, traffic accidents or willful destruction. As such, this technology provides electric utilities with a powerful and secure means to simultaneously address rising electricity demands and steadily increasing fault current levels.

Providing Power to Congested Urban Grids

High temperature superconductor (HTS) cable systems are an ideal retrofit in existing urban utility infrastructure where space is at a premium. Very low impedance HTS cables can be located in proximity to other infrastructure without disturbance because they emit no magnetic fields and are unaffected by the thermal considerations that affect traditional cables. Moreover, HTS cables can be retrofitted into existing ducts or placed in narrow trenches.

While placement concerns are vital considerations, the central benefit of HTS cables – and the main reason why global industries invested over 20 years of R&D commercializing them – is their ability to carry up to ten times the power density of conventional cables. Keeping up with power requirements in areas such as Manhattan, and countless other metropolitan centers, demands a power-dense solution. Today, HTS cables by Southwire carry up to 3,000 A_{rms} at 13.2 kV in the grid that American Electric Power manages in Columbus, Ohio. Long Island Power Authority (LIPA) has installed a Nexans 138kV HTS cable system running nearly a half-mile in length. Rated at 574 megawatts (MW), this system is able to serve 300,000 residents and businesses in New York's Nassau and Suffolk counties.

Managing Fault Current Magnitudes

SSG's technology takes the high power handling ability of HTS cables and adds inherent fault current limiting capabilities, further increasing the application options in the power network. In many urban areas, fault currents now approach the limits of conventional equipment and, given the increasing demand for electricity, such currents will likely continue to rise.

All of the new transmission and distribution equipment commonly installed to meet load growth and connect to new sources of generation contributes to increasing fault current levels. Fault currents now exceed 60,000 A in some transmission substations and reach 40,000 A in certain distribution substations. These values approach the limit of today's circuit breaker ratings. Given the unrelenting expansion of grids, a new solution is necessary.

While higher capacity fault-handling equipment is available, the economics of implementing a large-scale upgrade are not favorable. SSG technology takes advantage of a feature inherent to AMSC's second generation HTS wire that permits the design of a cable that is able to carry massive amounts of power one minute and then automatically turn into a resistor – a fault current limiter - when an over-current occurs on the system (i.e., beyond a pre-determined level).

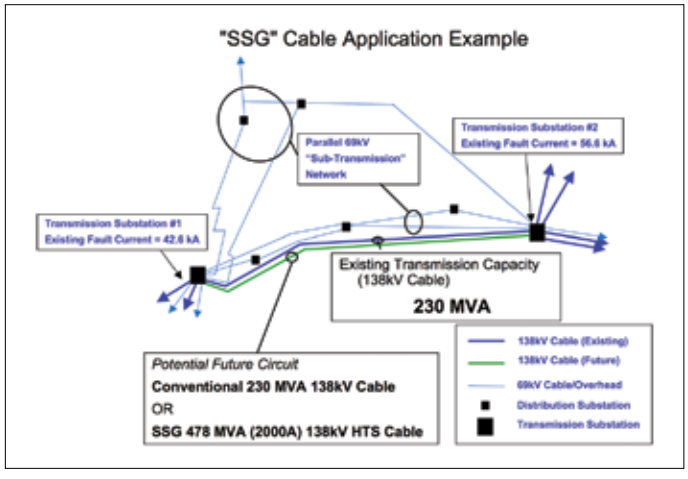
This fault current limiting ability hinges on a fundamental property of HTS materials: above a critical current, their superconductivity is quenched and their electron transport characteristics become resistive. It is for this reason that high temperature superconductors have been termed "smart materials," switching rapidly whenever a fault current exceeds the superconductor's critical current magnitude. The result is a new tool to enhance the capacity, reliability and security of the power grid.

Applications of cable-based or stand-alone superconductor fault current limiting equipment are diverse and range from enabling normally closed bus-ties, interconnecting substation secondaries to improve reliability, enabling IPP interconnections, and making possible the construction of a more tightly meshed grid to relieve congestion.

The slate of economic benefits is broad and includes: avoiding equipment damage, deferring or eliminating the need for equipment replacement, enabling the use of lower fault-rated equipment, eliminating the losses of series reactors, achieving higher system reliability, facilitating use of lower impedance transformers and enhancing grid stability. Given these compelling advantages, the United States Department of Energy has estimated a potential U.S. market for fault current limiting devices to be on the order of several billion dollars over the next 15 years.

Modeling Illustrates Sizable Fault Current Reductions

The following schematic shows configuration of an existing utility grid used to model behavior of a SSG installation (green line) between two transmission substations.



In this example, a single transmission circuit (i.e., 115kV/138kV cable) and a fairly extensive 69kV "sub-transmission" network connect two major transmission substations. The 115kV/138kV cable has the capacity to transfer up to 230 MVA from one transmission substation to the other, but the 69kV sub-transmission system primarily exists to serve the various distribution substations in the area, and it is not designed as a path to transfer bulk power.

When a significant power source near transmission substation #2 is installed due to ongoing load growth, the utility will have a significant financial incentive to increase the amount of power that can be transferred in the direction of transmission substation #2, which can provide power to neighboring regions or sold to a neighboring utility. In this example, approximately doubling the amount of transfer capability would meet the system owner's goals.

One potential solution to increase the power transfer capability is to add a second 115kV/138kV conventional cable that is electrically identical to the first between the two transmission substations. This approach would effectively meet the goal of doubling transmission capability. However, the existing fault current levels at both transmission substations are already at a very high level, and the addition of a new conventional circuit will result in even higher fault current levels. Any significant increase in fault current above initial levels would likely require a tremendous investment to replace circuit breakers, transformers and other fault current sensitive substation equipment.

An alternate solution would be to install a 138 kV Secure Super Grid cable system. With a single SSG cable circuit, the power transfer level can be raised to meet the increased power transfer goal. For the purposes of this study, a 2000A, 478 MVA cable was considered. This SSG cable has more than twice the power carrying capability of the existing 230 MVA conventional circuits.

Because the SSG cable alone can supply the desired level of transfer capability, the system owner would have the option of opening the existing conventional 138kV cable, leaving the SSG cable as the only in-service transmission path. This approach would result in fault current reductions of over 27% at transmission substation #1 and over 6% at transmission substation #2 from initial levels. Comparing the SSG solution against the conventional solution option, the reductions in fault current are over 36% and 9% at transmission substations #1 and #2, respectively, with similar increases in power transfer capability.

The impact these various scenarios have on fault currents is summarized in **Table 1**.

		Fault Current Level Change	
Scenario	**MVA Transfer Capacity Increase**	**Sub#1**	**Sub #2**
Base Case	230 MVA Base	42 kA	56 kA
2nd Conventional Cable	+230 MVA	12%	4%
Replacement HTS Cable	+248 MVA	-29%	-5%
HTS Cable + Original Cable	+478 MVA	2%	0

Table 1: Fault currents calculated in the utility network simulated in schematic above.

These data affirm the conclusion that Secure Super Grid technology can be applied in a manner that significantly increases power transfer capability while lowering fault current levels.

This solution offers a major value proposition for electric utilities worldwide in dealing with the need to provide increased power capacity in a rapidly growing economic environment. This new system is easily installed and brings increased underground capacity, fault current protection, reliability and security to densely populated urban and metropolitan area power grids.

Consolidated Edison to Deploy SSG Solution

Consolidated Edison, one of the nation's largest investor-owned energy companies, provides electric service to nearly all of New York City, serving the island of Manhattan over a distribution system organized as shown in **Figure 1**.

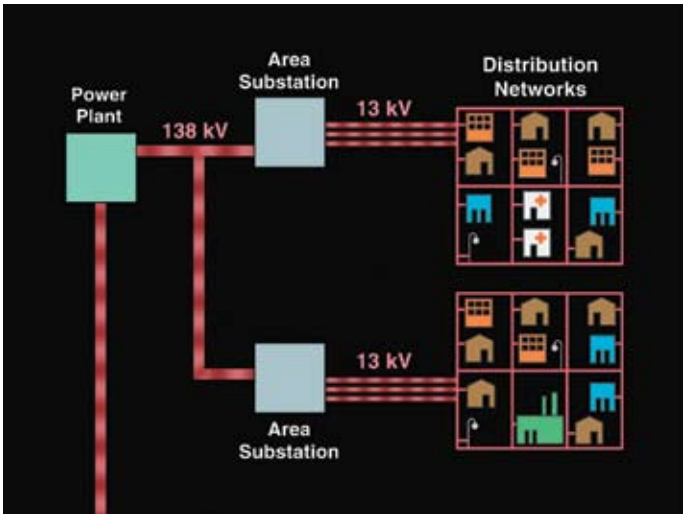


Figure 1: "Islanded" electric distribution networks serving residential and commercial customers in Manhattan today. (Courtesy of Con Edison)

The utility operates individual load islands of 100 MW to 300 MW that it serves at 13 kV, using multiple underground feeds from an area substation. Typically, a substation consists of five 65 MVA 138-13 kV transformers, serving about 150 MW of load. Consolidated Edison's security standards mandate N-2 contingency capabilities; that is, no loss of load-serving capacity, even after two substation transformers go down.

The utility has publicly discussed its desire to overhaul New York City's power grid over the next few decades to provide greater reliability and security.

As shown in **Figure 2**, the utility's concept is to connect area substations to provide power redundancy while also breaking distribution networks down into smaller compact networks, thereby minimizing the affect of blackouts. The space constraints under the streets of New York and the fault current levels that would result from realizing this vision, however, necessitate the use of SSG technology.

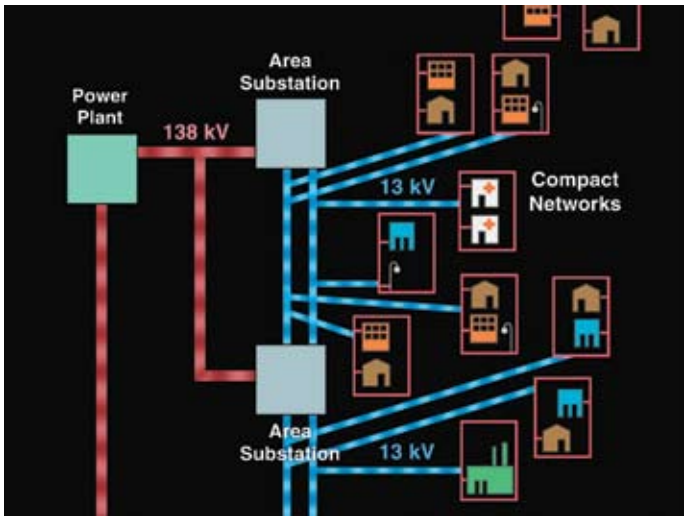


Figure 2: Area substations are connected via superconductor cables and network "islands" are broken down into smaller compact networks. (Courtesy of Con Edison)

Under a program funded in part by the U.S. Department of Homeland Security, Consolidated Edison is installing a first substation-to-substation link in Manhattan. Since the 13 kV interties have the potential to increase fault currents beyond the interrupting capability of existing substation equipment, superconductor cables themselves will be relied upon to manage fault currents.

Normally a certain minimum length of SSG cable is required to achieve the desired fault current limiting effect. This installation also demonstrates how even a very short SSG cable, placed in parallel with a small shunt conventional cable, can lower fault current levels.

The system operates as follows: Under normal operating conditions, the impedance of the superconductor cable is of order 1/6 or less compared to that of the shunt conventional cable (and optionally a series reactor), so that the dominant portion of the current flows through the high capacity superconductor cable and there is no voltage sag from the conventional cable or its series reactor. When a fault occurs, the superconductor cable switches immediately to a resistive state, limiting the fault current.

The superconductor cable with its HTS wire is designed in such a way that the resistance is large compared to the impedance of the conventional cable, so that the remaining fault current is diverted to the conventional cable (and its series inductor) and is finally limited by the total shunt impedance. After four cycles, a fast switch opens, allowing the superconductor cable to recover to its superconducting state, which occurs in only minutes.

During this time, if the fault has cleared, the conventional cable carries the power based on its overload rating. After a few minutes, the recovered superconductor cable is reconnected to the circuit by closing the fast switch and it again picks up the majority of the

power flow. If the fault does not clear during this time, the system circuit breaker opens to initiate the utilities' standard protection procedures.

Alternatively, the system can be designed to allow two full faults of up to four cycles, so that a first re-closure of the fast switch can be carried out within seconds, compatible with standard utility protection schemes. The parallel conventional copper cable is not necessary in all situations. For instance, longer cable runs could provide enough superconductor wire to absorb the fault energy of the full fault hold time without overheating until existing circuit breakers open.

In shorter runs such as ConEd's deployment, the parallel cable or an existing parallel connection is necessary to allow the fast switch to open and still maintain current flow to mesh with the existing utility protection procedures. In many cases, parallel cable connections already exist in the meshed utility network. In the special situations where a new conventional cable is required, it is important to note that this cable does not need to be rated for full continuous-duty capacity, but only to be able to carry the larger fault power flow under overload conditions for short durations. ■

About the Author

Jack McCall *is the Director of Business Development T&D Systems for American Superconductor with responsibility for superconductor cable systems, static VAR compensators and related FACTS (Flexible AC Transmission Systems) solutions. He has more than 25 years experience in the utility T&D business, holding a variety of product engineering, product management, system engineering, business development, marketing, and strategic planning roles.*

McCall holds a Master degree in Electric Power Engineering from Rensselaer Polytechnic Institute and a Bachelor of Science degree in Electrical Engineering from Gannon University. He is a member of the Institute of Electrical and Electronics Engineers (IEEE) and the International Council on Large Electric Systems (CIGRE).

For further information, contact: Jack McCall, American Superconductor Corp. (www.amsc.com), 15775 W. Schaefer Court New Berlin, WI 53151 Tel.: 262-901-6016
Email: jmccall@amsc.com.

Preparing for the Storm:
How a Computer-Based Emergency Management System Can Help Utilities Improve Incident Response During Hurricane Season

By Akhlesh Kaushiva Vice President, Commercial IT Services and Anil Jayavarapu, Director-Business Process Management Avineon Inc.

Hurricane Katrina taught us many things, most importantly that the nation's emergency preparedness procedures needed a great deal of improvement. New measurements are needed on a local, state, and federal level to ensure that no other city or region suffers through a similar situation. In the wake of the devastation, the federal government has recently launched a number of emergency initiatives. These include:

- The National Response Framework, which provides a blueprint for dealing with disasters;
- The National Emergency Communications Plan that seeks to connect first responders from around the country; and,
- The National Shelter System, which contains maps and data for more than 45,000 shelters nationwide.

While these are steps in the right direction, utility companies need their own emergency management plans to handle specific disaster responses should another hurricane of Katrina's size and magnitude come knocking at our door. Just this year, Gustav and Ike packed a one-two punch for residents along the Gulf of Mexico, leaving millions without power for days or weeks.

In fact, although the height of hurricane season runs from June to November, utility companies must remain in a state of perpetual readiness for natural disasters throughout the year. Experts agree that having access to information is key, but companies should establish common operating procedures and emergency response plans based on the most up-to-date and accurate data. Part of this readiness is the overall outage management process, which involves pre-event emergency preparedness and incident management during and after a major outage event.

Emergency Management Initiatives

By now, most companies are familiar with emergency management. Its two main components – emergency preparedness and incident management – help companies prepare for any number of disasters and manage responses to various incidents. Most utility companies have some form of emergency preparedness and incident management process in place, which should follow guidelines set forth in the National Incident Management System (NIMS).

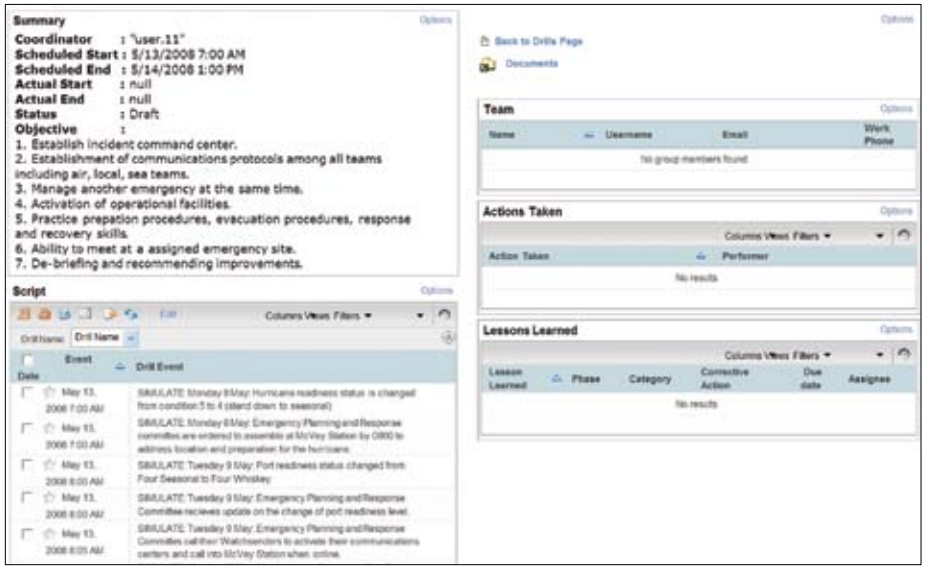
A version of NIMS has been in use since the 1970s when it was primarily used to help streamline communications during responses to wildfires. Then in 2004, prior to Hurricane Katrina's landfall in August 2005, the Secretary of Homeland Security, at the request of the President, federalized NIMS and mandated its use by emergency responders. NIMS is a comprehensive system that improves emergency response operations through the use of the Incident Command System (ICS) and the application of standardized procedures and preparedness measures. These tools promote development of cross-jurisdictional, statewide, and interstate regional mechanisms for coordinating response and obtaining assistance during a large-scale or complex incident such as a major hurricane.

NIMS compliance is a community-wide effort. In addition to emergency management, fire, and medical services, incident response organizations include utilities, local public health, public works, private sector entities, non-governmental organizations, hazardous material handlers, and others. The ICS enables these organizations to develop the foundation for an effective response, requiring emergency preparedness and optimized collaboration, communication, and documentation among the response teams responsible for planning, logistics, operations, finance and administration, information management, liaison, and safety.

Software-Based ICS

Once the federal government established the blueprint for localized disaster response, it left the adoption and implementation up to each jurisdiction and emergency response organization. In response, utility companies and state and local governments have created and implemented a number of methods to manage their respective systems.

An ICS enables utility companies to develop the foundation for an effective outage response, but a typical paper-based or manual ICS is inefficient. Using an automated software-driven information system, utilities can better prepare, organize, manage, execute, and document emergency preparedness and incident management functions.



During implementation of a software-based system, emergency scenarios are identified and second roles, desired response levels, and other utility needs are specified for each scenario. The ability to customize responses to a variety of emergency situations ensures that utilities can maintain control over their processes and incorporate aspects of their current plan that have proven effective.

Using a software-based emergency management system positions utilities to better achieve compliance with ICS standards and institutionalize ICS within the company. This, in turn, automates some of the emergency preparedness and incident management functions. A software-based system provides standardized electronic forms for inputting data and utilizes intelligent business logic to orchestrate critical functions such as resource check-in / check-out, task assignment, individual performance rating, and more. All system transactions also receive a date and time stamp, building a traceable history for auditing.

Enabling an Emergency Management Process

There are many software systems on the market that can help utilities better manage their emergency response capabilities. These systems enable organizations to automate the preparation, organization, management, execution, and documentation of emergency preparedness and incident management functions. In addition to meeting the NIMS requirements, software systems conform to FEMA published guidelines, support second roles management, and contain features of ICS. Software programs also provide graphical representation of a utility's entire distribution system, enabling a highly effective outage response management and ensuring organizational compliance with ICS standards.

Software-driven solutions based on a business process management (BPM) platform are unique. A solution that helps utility companies increase business effectiveness and efficiency with technology and which also allows them to continually improve and optimize their outage response processes in recurrent natural disasters, such as hurricanes, is extremely important. Moreover, having a repeatable process in place can also help utilities take better advantage of forecasts and proactively enact specific aspects of the emergency plan.

Software-based emergency management systems consolidate in one place all of the pertinent data needed during an incident–from second roles of employees to mutual assistance contracts to post outage analysis. This enables changes to be made efficiently to an entire system, as opposed to piece-meal implementation. Software solutions provide the tools needed to help measure response and identify areas of improvement.

Perhaps the biggest benefit of a software-driven solution is that it enables companies to monitor responses and evaluate incident management to improve internal processes. When a software system is utilized, utilities can define measurement parameters for each incident and expected levels of response. During the response phase, actual performance can be measured against these pre-defined standards. Full-featured software systems contain a user interface that logs all actions with a timestamp for instant reporting of incident response activity. After an event, utility companies can access and analyze this data and produce after incident reports. As with any process, emergency management can also be altered to meet the changing needs of a utility.

Improved Processes = Easier Problem Solving

In addition to helping utilities improve their internal processes, software solutions are equipped to help companies better address key challenges in any disaster response. One of the biggest challenges facing utilities during a hurricane is managing the logistics of the event. Companies must keep track of everything from personnel details and second roles to mutual assistance. With a computer-based solution, companies can identify scenarios and include data from other systems for effective decision-making.

For example, changes in personnel as people are hired, retire, or leave the company can often be overlooked or difficult to ascertain in a paper-based emergency management system. But these

updates can be automatically reflected through data integration with the HR system, ensuring that each second role is identified and all employees are assigned proper roles on an on-going basis.

Another key challenge during outage situations is managing resources. As other regional utility companies arrive to offer their assistance, the emergency management system keeps track of the resources and supplies that are arriving. Software-based systems contain functionality that allows utilities to receive details of incoming resources. Once they arrive, the system can prompt utilities to capture the safety training for new resources, as well as outline the location of staging areas, lodging, and other logistical details.

Since a software-based system has the capability to interface with multiple legacy enterprise systems, users can access existing data systems such as the mobile dispatch system (MDS) to determine where the outages have occurred and what task is needed at each location. During an outage, the emergency management system helps utilities keep track of how many resources are on hand, where they are working, and how long they have worked. While these systems can keep track of numerous details such as equipment assigned to them, most often utilities choose to maintain only high-level information for these resources in the emergency management systems. The details of individual trouble tickets for power restoration are usually maintained in the outage management and mobile dispatch systems.

Assigning incident management and support tasks to resources also poses a challenge to a majority of utility companies. A software system contains a list of all utility employees, their roles, and training records for second roles, automatically prompting companies to conduct follow-on training if needed. During a hurricane outage situation, second roles are readily identified according to pre-determined scenarios and resources are mobilized to complete their predefined or ad hoc tasks.

For example, local companies need trained patrollers who locate the damage during an outage situation. These employees travel from location to location to gather details of the damage before a work crew is dispatched to the scene. Job details such as a tree on the line or a felled pole help the utility prepare for each incident location, saving time and resources by ensuring response crews are prepared for the work situation they are entering. Assignment and coordination of these tasks can be managed effectively in an automated manner using the software solution.

GIS Integration

Just as residents in a hurricane's path need to monitor the weather, so do utility companies. Software systems offer extensive capabilities for utility companies to utilize geospatial information system (GIS) portals and download the latest weather data and other satellite imagery. This data along with the company's power grid information enables the utility to predict which areas will be hardest hit.

The mapping functionality also helps utilities better manage their needs for static and dynamic maps. Companies can create static maps in the system showing details such as staging areas, and they can also connect to a fully functional GIS to perform spatial queries and other advanced data manipulation. This functionality also provides dynamic maps depicting the progress of restoration efforts and geographical areas that still require attention.

The benefits of a software-based emergency management system expand far beyond the height of hurricane season. By putting ICS based procedures in place and managing the process with emergency management software, utilities can better prepare for any natural disaster, other man-made events, and accidents. Enhancing the response processes during the off-season can greatly improve response times, reduce incident management costs, and improve a utility's overall communication with its resources during an outage.

Having a process-driven model in place not only ensures that a company can learn from each outage event and improve access to the resources on-hand for each successive event, but in the longer view, also results in improved customer satisfaction ratings overall. ■

About the Authors

Akhlesh Kaushiva *serves as Vice President, Commercial IT Services for Avineon, Inc. (www.avineon.com) where he leads business intelligence and business process management efforts among other IT systems for the company's growing commercial sector. He is a veteran of the utility industry and has led implementation for major utility IT projects.*

Anil Jayavarapu *serves as the Director of BPM practice for Avineon, Inc. He leads business process management solutions for commercial customers and development efforts for Avineonics®, a state-of-the-art information system that enables organizations to prepare, organize, manage, execute, and document emergency preparedness and incident management functions. He has more than 14 years of experience in the IT and GIS industry performing management, consulting, and technical roles for utility companies.*

onelivewire

DISTRIBUTECH®
CONFERENCE & EXHIBITION

A PennWell Conference
Now Including: TRANSTECH™
DISTRIBUTECH'S SOURCE FOR TRANSMISSION INFORMATION

February 3 – 5, 2009

San Diego Convention Center • San Diego, CA

www.distributech.com

www.transtech-conference.com

Owned & Produced by: PennWell

Flagship Media Sponsor: Utility T&D

Supporting Publications: Electric Light & Power, Utility Products, WaterWorld

Host Utility: SDGE, A Sempra Energy utility

PRODUCT Showcases

ADVERTISERS Index

Only One AMI System has a Dedicated Frequency That Gives You a Clear Path Above the Rest.

FlexNet from Sensus.

FlexNet from Sensus is the only AMI system with its own dedicated, primary use radio frequency. That means it is the only system that is designed to be interference-free – unlike systems that share unlicensed frequencies that anyone can use – literally!

An RF AMI system without a dedicated radio frequency is like getting a cell phone with a "party line." Anybody can use the unlicensed frequency offered by other vendors – your frequency – anytime they want – for anything they want!

FlexNet is also the only system with a full 2 watts of transmit power – enough range to actually reduce the amount of infrastructure required. So you need fewer collectors, fewer maintenance hours, and fewer things to go wrong.

FlexNet talks to anything you've got now or are planning to get in the future. Yet it's totally secure where it needs to be. We have systems available for electricity, gas, water and combination utilities. To learn more, visit **www.sensus.com/flexnet. Or call 1-800-METER-IT.**

SENSUS

SAP HELPS OVER 1100 UTILITIES KEEP THEIR MILLIONS OF CUSTOMERS SMILING.

For over 30 years, SAP has been working with utility organizations worldwide, helping them become more responsive, more efficient, and more customer friendly. How? Through an integrated solution that provides their customers with more accurate billing, timely service, and customized product options. In fact, UtiliPoint ranked SAP as the top business software provider based on its comprehensive customer information systems (CIS) offering. To learn more about SAP for Utilities and how it can help you better serve your customers, visit sap.com/ForUtilities

THE BEST-RUN BUSINESSES RUN SAP™

SAP®