



Electric Energy T&D

MAGAZINE

MAY-JUNE 2017 Issue 3 • Volume 21

The Future of Power Line Communication



SAVE THE DATE

47

CIGRE SESSION

August 26-31, 2018

Paris / France

Palais des Congrès - Porte Maillot

See our **Call for Papers**
on the website
<http://www.cigre.org>

A TECHNICAL
EXHIBITION
ON 3 FLOORS

AN ALL WEEK
TECHNICAL
PROGRAMME

A UNIQUE
OPPORTUNITY FOR
NETWORKING
WITH 6600
MANAGERS AND
EXPERTS FROM
THE WORLDWIDE
POWER INDUSTRY.

CIGRE SESSION 46



INTERNATIONAL COUNCIL ON LARGE ELECTRIC SYSTEMS
Conseil International des Grands Réseaux Électriques



POWER FORWARD

APRIL 16-19 2018

DENVER COLORADO

THE FUTURE IS A POWERFUL PLACE.

Join over 700 exhibiting companies as Denver plays host to the T&D industry's most powerful and experiential conference and exposition. This is your opportunity to gain access and expose your business to over 12,000 professionals and decision-makers. Don't miss the unparalleled chance to grow your network, connect globally and discover the latest innovations to power your business forward.

**BOOTHS ARE GOING QUICKLY.
SIGN UP TO BECOME AN EXHIBITOR
TODAY AT TANDDDENVER2018.ORG**



FOLLOW US TO LEARN MORE



Publisher:
Steven Desrochers:
steven@electricenergyonline.com

Editor in Chief:
Elisabeth Monaghan:
elisabeth@electricenergyonline.com

Account Executive:
Eva Nemeth: eva@electricenergyonline.com

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

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

Electric Energy Magazine is published
6 times a year by: Jaguar Media Inc.
834 Montée Masson
Terrebonne, QC Canada J6W 2C6
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

6 Industry News

32 Advertisers Index



Page 10

4 POWER POINTS Sparking a New Conversation

If you've just done a double take, you've probably realized I am not Terry Wildman. My name is Elisabeth Monaghan, and I am the new editor in chief for EE T&D.

9 THE GRID TRANSFORMATION FORUM: The Future of Power Line Communication

We are speaking with Lily Ho, Vice President of Product Management for Aclara.

12 GREEN OVATIONS The Killer App for Renewable Generation

Since the turn of the century, the United States has been the world leader in creating opportunities for demand response (DR) in wholesale electricity markets.

15 FROM RESEARCH TO ACTION EPRI's Telecommunications Initiative: Taxonomy Providing Wireless Opportunities and Options

The energy industry recognizes the need to improve the performance, reliability, and security of utility communication systems used for distribution automation, telemetry, and control.

17 Implementing the DHS's Lessons Learned to Secure Grid Systems

Modern advancements in grid systems enable marked improvements in efficiency, production, reliability, and safety, all through increased use of "smart" assets and digital communications.

20 What is between Grid of Things (GoT) and Internet of Things (IoT) is HoT (Holistically Orchestrated Things)

When it comes to connected things operating interactively and in close harmony with other assets, one just needs to look at the electric grid as a prime example of how efficiencies and optimization can be achieved by leveraging remote monitoring and control.

24 Electric Utility Outage Prediction Models: Assessing Their Accuracy & Implementing Improvements

Academic and industry researchers continue to press ahead to create ever new and better weather forecasting models (WFM).

26 BIGGER PICTURE Utility Analytics Survey: Maturity Levels Vary Significantly But Showing Improvement

Today's utility industry stands on the precipice of discovering new insights that will transform the future of their business in terms of both strategic growth and operational efficiencies through the power of analytics.

29 SECURITY SESSIONS Strong Passwords: Making it Difficult for the Bad Guys

A topic that comes up quite often when discussing cyber security is the use of passwords and what is the right size and complexity and how often should you change them.

SCADA INTEGRATED VIDEO MONITORING EQUIPMENT

Substation Video Automation

Thermal imaging cameras scan and measure the temperatures of critical substation assets and send the information to SCADA as analog points that can be continuously tracked and monitored. Thermal video analytics detect out of range conditions and send DNP3 alarms to the system. Live visual and thermal imaging are streamed to the SCADA HMI to provide video confirmation of conditions at the substation.



SCADA integrated video means less screens for operators to monitor and more time to focus on keeping the grid running. Automated alarms provide proactive warnings when attention is required. Monitor assets with infrared imaging to detect excessive heat generated by failing joints, insulators, bushings, arrestors and transformers.

Contact us to learn more.



Substation Hardened
Digital Video Server



Video Management Software



Substation Hardened
IP Cameras



Pan/Tilt/Zoom
Cameras



Thermal Imaging Cameras



POWERPOINTS

Sparking a New Conversation

If you've just done a double take, you've probably realized I am not Terry Wildman. My name is Elisabeth Monaghan, and I am the new editor in chief for EE T&D. During the transition, I did not get to spend a lot of time working with Terry, but he made sure to pass on how much he enjoyed working with the Electric Energy Online community and assured me I would find everyone warm and welcoming. He was right.

For the past 30 years, I have worked in some capacity as a writer, editor, publicist, and integrated marketing professional. In this time, I've also had a long and complex relationship with electricity. I knew it was dangerous, but I wanted to know more. When I was about five, curiosity got the best of me. I stuck a metal hairclip into the electrical outlet in my parents' bathroom. (I know. It was a ridiculously stupid move.) Fortunately, I did not hurt myself, but it certainly sparked (pun intended) my respect for what was going on to make that bolt run up my arm and through my body.

The five-year-old in me still is curious about electrical energy, as well as technology and innovation. I marvel at all of the ways in which we harness a wide variety of energy forms in order to keep up with – and exceed – the demands of every day modern life. Electrical energy is a critical component in maintaining our health, wellbeing and understanding of the world around us. It is a connector – literally – that threads together people from across the globe, enabling us to live under one roof.

This fascinates me. It makes me appreciate the magnitude and vastness of our human potential.

The power sector is constantly changing. Today's innovative technology is tomorrow's outmoded approach. To remain relevant and competitive we have to keep up. As editor in chief, I intend to spotlight thought leaders in the power industry, whose insights will inspire all of us to reach a bit further while remaining excited about the work we do.

For my inaugural issue, I sought the expertise of two industry veterans. What follows are some of the observations they shared with me. One of the most pressing issues is the uncertainty of how things will shake out under the Trump administration. Although Trump has been in office for nearly five months, it is still uncertain what effect his policies will have on the energy sector. If his budget slashes clean energy, how will that affect innovation both in the U.S. and internationally? Will U.S.-based companies be able to keep up with the rest of the world's advances in renewable energy? A number of communities and power plants are thrilled with Trump's promise to bring back coal production and the new jobs bringing it back could generate. There are enough articles about how a resurgence of coal could or couldn't work, but what about those plants that have shifted from coal production to producing natural gas or renewable energy?

Wayne Bishop, marketing director for Omicron Electronics, does not believe these converted plants will change course. “We have seen a huge number of coal plants close. Some of this might change with Trump, but many utilities have already announced they’re shutting down their coal plants. For example, Florida has announced they’re going to be closing 27-30 of their coal-fired plants by 2020 to comply with the Clean Power Act. I think what’s going to happen is the states are going to say, ‘We’re already on track to do this. Let’s just forge ahead and keep going.’ People realize now it is better for the environment that we have these clean energy initiatives in place and I think they’re going to push forward.”

As hackers get smarter and more resourceful, businesses are at greater risk of security breaches, so cyber security has become a top priority. Mike Guilfoyle, who is the director of research for ARC Advisory Group, says utilities are a little behind the curve in terms of tackling the issue, but by looking at how other industries are handling it, they’re coming up with their own solutions. “Utilities have started to see a greater concern for cyber security down at the distribution level, where they previously hadn’t been as concerned about it, but now, as you look at connected devices and transactive energy, security becomes much more important.”

Another issue that has begun to hit industries across the board is the aging workforce. With more Baby Boomers approaching retirement age, there is a gap of experienced workers to replace them. Guilfoyle sees digitization as one approach for capturing the aging workers’ knowledge. “You’re starting to see all these manual processes be heavily automated. That’s not going to stop until most everything manual is eliminated. What that gives you the ability to do this is to gather all the data related to that decision making process—and you can use things like analytics, and you can use things like machine learning—to take that data and create an insight out of it. This then becomes enterprise knowledge versus individual knowledge. So the fact you can put an algorithm out on a machine, run data through it and have that machine learn that data over time, takes tribal knowledge and makes it enterprise knowledge.”

While some of these issues require prompt resolution, there are other changes occurring in the industry that are more interesting than they are concerning.

For example, Wayne Bishop points out how customer behavior has changed. According to Bishop, utilities have discovered their customer base has become more knowledgeable and more assertive. About 20 years ago, utility customers were simply ratepayers, who dropped their bill in the mail or paid it in person. Today, customers want to know details on any matters concerning their personal power supply, and they expect to receive the information right away. If their power is down, they want to know what caused the outage. What other areas are affected by the outage? How long will it be until the power is back?

On the solution provider side of the industry, Mike Guilfoyle sees a trend in the way major companies like Microsoft, Honeywell, GE, SAP, and Schneider, are building their own industrial platforms with IoT services. “They very much intend to push those horizontal platforms down into their industry verticals, so I think you’ll see more emphasis on the development of after market services by these solution providers, where you can see if you can sell uptime as a service. That’s going to take a while for the utilities to come to grips with and understand, but it’s happening across multiple industries.”

This represents a small portion of my conversations with Bishop and Guilfoyle. In addition to speaking with them, I also had a brief exchange with Dave Bryant, director technology for CTC Global. When I asked for his thoughts about the industry, Bryant stated, “We are obviously living in a very interesting and uncertain time. Lots of heavy challenges, however, are offering lots of opportunity for creative problem solving.”

Bryant also pointed out why this industry and those who work in it will power through any existing or unforeseen challenges “There are a lot of bright people working on solutions for every perceivable problem.”

To me, this succinctly defines the tenacity and resourcefulness that will fuel the power industry and carry it through the next cycle of challenges and breakthroughs—and spark endless possibilities.

Elisabeth

If you have interesting technology, solutions, or story suggestions, please email them to me at Elisabeth@ElectricEnergyOnline.com. I look forward to working with you.

Appalachian Power submits 2017 Virginia Integrated Resource Plan showing continued growth in generation diversity

May, 2017

Appalachian Power has filed its 2017 Integrated Resource Plan (IRP) with the Virginia State Corporation Commission (SCC). The IRP provides a blueprint for how the company plans to meet forecast load obligations in the Commonwealth over the next 15 years through continued reliance on existing coal, natural gas and hydro generation plants and renewable energy contracts, while increasing large-scale or “universal” solar and wind energy, and energy efficiency programs.

Appalachian files its IRP with the SCC annually in Virginia. In its West Virginia territory, the company submits a plan every five years to the state’s Public Service Commission.

The IRP provides a forecast of the company’s load requirements and a plan to meet those obligations with supply- and demand-side resources over 15 years while maintaining reasonable customer prices, reliable service, energy independence, and environmental responsibility.

“This plan continues Appalachian Power’s power generation philosophy of delivering reliable power at a reasonable price to our customers through a diversified portfolio of resources,” said Chris Beam, Appalachian’s president and chief operating officer. “We will continue to be primarily a coal-fueled company, but based on lowering costs and growing customer expectations there will be an increasing contribution of renewable resources in our future energy mix.”

The 2017 IRP identifies several key components to meet its load obligations: further diversification of its mix of supply-side resources; incorporation of additional demand-side resources including energy-efficiency programs; and recognition that residential and commercial customers will add distributed generation resources, primarily rooftop solar.

The company’s proposed plan includes:

- The addition of 500 megawatts (MW) of universal solar by 2031;
- The addition of 1,350 MW of wind energy by 2031;
- The addition of 10 MW of battery storage resources in 2025;
- The implementation of customer and grid energy efficiency programs reducing 203 MW of capacity requirements by 2031;
- The assumed addition of 123 MW of customer-owned distributed generation, primarily rooftop solar, by 2031; and
- Continued operation of existing coal and gas-fueled generating plants, hydro-electric facilities, and wind resources; and the expected retirement of Clinch River Units 1 and 2 in 2026.

The SCC will schedule a public hearing for Appalachian’s 2017 IRP. The complete filing may be found on the SCC website: <http://www.scc.virginia.gov/case>.

Emera Newfoundland & Labrador set to install North America’s longest submarine electricity cables

May, 2017

The first of North America’s two longest submarine electricity cables has arrived in Atlantic Canada onboard the cable laying vessel the Skagerrak. Integral to Emera’s Maritime Link Project, these cables each measure 170 km and weigh 5,500 tonnes - combined, the two cables weigh more than the Eiffel Tower. The first cable was manufactured in Halden, Norway, while the second cable, which is expected to arrive in mid-May, was manufactured in Futtsu, Japan.

The arrival of the Skagerrak, operated by the cable supplier Nexans, marks the start of the submarine cable installation process. Over the next few weeks members of Nexans’ highly specialized crew will prepare for the installation of the first electrical connection across the Cabot Strait between Nova Scotia and the island of Newfoundland.

Throughout the various stages of the manufacturing process and transport of each cable, members of Emera Newfoundland & Labrador’s Marine Team have been monitoring and inspecting the progression to maintain quality assurance.

“The arrival of the submarine cables is the result of more than three years of dedication to safety and quality by our team,” says Rick Janega, President and CEO, Emera NL. “Throughout the manufacturing process, the successful testing phase and the transportation of cables, the team’s commitment continues to be the driving force of our success to date. This brings us another step closer to the completion of the Maritime Link Project later this year.”

Nexans used two facilities for cable manufacturing, allowing both cables to be produced at the same time. The cable manufactured in Futtsu, Japan, was spooled onto a giant barge in early April, and then loaded onto a heavy lift vessel (HLV) for the long journey to the Cabot Strait to await installation.

The HLV carrying the second submarine cable from Japan will take approximately six weeks to travel to the port in Sydney, NS. It will travel across the Pacific Ocean, through the Panama Canal and then up the Eastern Seaboard. Expected to arrive in mid-May, it will be loaded onboard the Skagerrak once the first cable is installed. Installation of both submarine cables is expected to be completed by late summer.

Forward Looking Information

This news release contains forward-looking information within the meaning of applicable securities laws. By its nature, forward-looking information requires Emera to make assumptions and is subject to inherent risks and uncertainties.

About The Maritime Link Project

The Maritime Link Project is part of a larger strategy to address the growing demand for more renewable energy in the region. It will enable the transmission of clean, renewable and reliable electricity from Newfoundland and Labrador to Nova Scotia.

The Maritime Link is a 500 MW high voltage direct current (HVdc) transmission project bringing clean renewable energy from the Lower Churchill project at Muskrat Falls to Nova Scotia. The Project will include two 170 km subsea cables across the Cabot Strait, with almost 50 km of overland transmission in Nova Scotia and more than 300 km of overland transmission on the island of Newfoundland.

Students from Massachusetts and California win DOE's 27th National Science Bowl®

May, 2017

Students from Lexington High School in Lexington, Massachusetts, won the 2017 U.S. Department of Energy (DOE) National Science Bowl® (NSB) in Washington, D.C. This year's championship team in the middle school competition is from Joaquin Miller Middle School in San Jose, California.

"Congratulations to this year's National Science Bowl Champions from Lexington High School and Joaquin Miller Middle School, as well as all of the other finalists, for their outstanding accomplishments in this challenging academic tournament," said Secretary of Energy Rick Perry. "These students represent the future leadership and innovation that will allow American science and engineering to excel in the 21st century. I encourage all of them to continue their hard work and dedication. One day I hope to see you working at one of our flagship national laboratories and being role models for the next generation of STEM students."

The top two high school teams emerged victorious from a field of 63 high school regional champions who came to D.C. to compete in the National Science Bowl® Finals. Altogether, about 9,000 high school students and 5,100 middle school students from across all 50 U.S. states, the District of Columbia, and Puerto Rico participated in this year's regional competitions.

Lexington High School defeated Thomas Jefferson High School for Science and Technology from Alexandria, Virginia by correctly answering the physics question, "To the closest integer, what is the ratio of the energy radiated by a 7.8 earthquake to that radiated by a 6.8 earthquake?" with the correct answer, "32." The members of the winning high school team are Catherine Wang, Derik Kauffman, Joshua Park, Benjamin Choi, and Anka Hu, and they are coached by Nicholas Gould and Robert Pohlman.

For winning the national championship, Lexington High School will receive a nine-day, all-expense paid science trip to Alaska. While on the trip, the students will take day trips that provide learning opportunities about glaciology, marine and avian biology, geology, and plate tectonics. They will explore the Copper River Delta, known for its highly prized stocks and prolific runs of wild salmon; experience the mystical appeal of old-growth hemlock and spruce while hiking through the Chugach National Forest; and white-water raft on the Sheridan River and travel across the scenic Prince William Sound and Orca Inlet, home to the world's largest population of sea otters. The trip also includes visits to Childs Glacier and the Alaska Wildlife Center, which is a rehabilitation facility for injured and orphaned wildlife.

For finishing second, Thomas Jefferson High School for Science and Technology will receive a seven-day, fully guided adventure tour of Cordova, Alaska. They will travel by boat up the Copper River to Childs Glacier to learn about glaciology and hike through the Heney Ridge Trail to experience three complete ecosystems. They also will learn about the diverse marine life in tidal pools and see the historic Million Dollar Bridge.

The top three high school teams received trophies and individual medals, and the top 16 high school teams won \$1,000 for their schools' science departments.

In the middle school competition, Joaquin Miller Middle School defeated Odle Middle School from Bellevue, Washington. The members of the winning middle school team are Jonathan Huang, David Hu, Wilson Ho, Michael Zhao, and Alexander Zhang, and they are coached by Raymond Huang and Vibha Walia.

The top two middle school teams emerged victorious from a field of 48 middle school regional champions who came to D.C. to compete in the National Science Bowl® Finals. The top 16 middle school teams in the academic competition won \$1,000 for their schools' science departments, and the top three teams received trophies and individual medals.

DOE created the National Science Bowl® in 1991 to encourage students to excel in mathematics and science and to pursue careers in these fields. More than 275,000 students have participated in the National Science Bowl® since its creation. Students may sign up to compete in next year's National Science Bowl® competition beginning in October.

DOE's Office of Science manages the National Science Bowl® and sponsors the finals competition.

Additional information about the teams and the National Science Bowl® is available at: <http://science.energy.gov/wdts/nsb/>.

Entergy Arkansas and Comverge to Deploy Bring Your Own Device Demand Response Program

April, 2017

Comverge, Inc., the leading provider of cloud-based demand response and energy efficiency solutions for electric utilities, today announced a new contract with Entergy Arkansas to deploy a bring your own device (BYOD) demand response pilot. Comverge will aggregate consumer-purchased Wi-Fi-enabled smart thermostats to evaluate a potential new demand response resource for Entergy Arkansas, Inc.

The BYOD pilot will complement the Comverge and Entergy Arkansas Summer Advantage residential demand response program.

"As the leader in mass market demand response, Comverge is excited to work with Entergy Arkansas to add consumer-purchased smart and Wi-Fi-enabled thermostats to its portfolio of demand response resources," said Dave Neal, Chief Operating Officer, Comverge. "The new BYOD demand response pilot enables Entergy Arkansas to better engage customers with Wi-Fi thermostats, while also creating a potential new source of capacity."

Entergy Arkansas will utilize the Comverge IntelliSOURCE-Connect software to coordinate and communicate with the consumer-purchased devices. IntelliSOURCE-Connect is completely integrated with the Comverge IntelliSOURCE Enterprise demand response management system to give Entergy Arkansas a single platform for managing both the existing direct load control program and the BYOD pilot.

Entergy Arkansas provides electricity to more than 705,000 customers in 63 counties across the state of Arkansas. It is a subsidiary of Entergy Corporation, which is an integrated energy company engaged primarily in electric power production and retail distribution operations.

Nova Scotia Power Sets Another Record in Renewable Energy

May, 2017

Nova Scotia Power continues to make progress in reducing carbon and increasing renewable energy, with 28% of the electricity used by Nova Scotians in 2016 coming from renewable resources. The amount topped the previous high mark of 26.6%, set in 2015.

"We're working to build a future focused on clean energy, smart technology and enhanced customer service," said Mark Sidebottom, Chief Operating Officer for Nova Scotia Power. "Our customers expect more of their energy to come from more sustainable sources - together, we're building a cleaner province for future generations."

The results exceeded the legislated requirement that 25% of NS Power's electricity comes from renewable sources, and continue NSP's pace to meet the 40% renewable requirement that takes effect in 2020. As recently as 2007, only 9% of Nova Scotia's electricity was renewable. Additionally, Nova Scotia Power has already achieved and exceeded Canada's 2030 target of reducing carbon dioxide by 30% from 2005 levels. By 2030, NSP expects to have achieved a 58% reduction from 2005 levels, which is almost double the national target.

"Our employees take pride in making these changes for a cleaner, lower carbon future in Nova Scotia," Sidebottom said. "In meeting and exceeding these requirements, we strive to be Canadian leaders in clean energy improvements."

Nova Scotia's growth in renewable electricity has been largely through the development of wind power. There are now more than 300 commercial wind turbines generating electricity in Nova Scotia, making the province a national leader in wind energy as a percentage of total generation capacity.

RENEWABLE ENERGY PROGRESS: ELECTRICITY BY SOURCE

	2007	2016
Coal & Petcoke	76%	55%
Natural Gas & Oil	13%	13%
Wind	1%	17%
Hydro & Tidal	7%	8%
Biomass	1%	3%
Imports	3%	4%
RENEWABLE TOTAL	9%	28%

The new generation of simulation hardware for the RTDS® Simulator is
a revolution in real time.

A powerful multicore processor
 makes the
 world standard in real time
 power system simulation

**faster, more capable,
 and more accessible
 than ever before.**




RTDS Technologies proudly presents **NOVACOR**

www.rtds.com/novacor



THE GRID TRANSFORMATION FORUM

Envisioning the 21st Century Grid

The Future of Power Line Communication

We are speaking with Lily Ho, Vice President of Product Management for Aclara.

EET&D: We hear a lot about RF networks for advanced metering infrastructure (AMI). Is Power Line Communication a viable option for utilities?

Ho: Yes, Power Line Communication (PLC) is actually the best solution for many AMI requirements and is often preferred to RF, depending on certain conditions. PLC meets all the essential AMI system requirements and with advancements made in concurrent feeder/phase communication it now delivers exceptional improvements in network throughput.

For example, PLC systems are ideal for utilities operating high geographically disbursed networks (e.g. a low density of end points per square mile) because the required investment in communication infrastructure is very low. PLC only requires communication equipment in the substation to collect and convey information from end points. There is no additional network infrastructure needed as all communications goes over the existing power lines. Anywhere that an electric signal goes, we can get out to the meter or device even if it's more than 100 miles away. Plus, investment in R&D on technologies and add-on solutions that use PLC data to deliver an ever-broadening array of new capabilities continues.

EET&D: What are the benefits and advantages of PLC?

Ho: The benefits and advantages of PLC really relate to the fact that the infrastructure it needs to operate exists by virtue of the electric distribution network. This differs from an RF

network, which is dependent on data collectors placed within range of the meters at all points. The only infrastructure equipment that's required with PLC is substation communications equipment. Different from Power Line Carrier solutions, no intermediary equipment such as repeaters, line conditioners, or any kind of signal booster are needed.

This is an important consideration for utilities with meters that are dispersed over a large geographic region. With RF-based AMI, a network infrastructure must be built to read meters and devices, and while this type of system works well in densely populated areas, it can be inefficient for those utilities that are more rural. For example, if a utility has a meter density of 20 meters per square mile, a DCU and access-point infrastructure is still required to be able to read those meters, which may be cost inefficient.

EET&D: What are the differences between power-line communications and power-line carrier?

Ho: The real difference between the two is that PLC does not generate a carrier signal over the distribution line as Power Line Carrier solutions do. Instead, PLC modulates at the zero cross of the sine wave. On the outbound signal, PLC modulates at the zero cross on voltage, and on the inbound signal it modulates on current.

This enables an exceptionally robust communication network even in the face of line harmonics and other distortions that degrade Power Line Carrier network performance. These issues do not affect PLC network performance.

EET&D: How are PLC solutions poised to meet the throughput and performance demands of AMI?

THE GRID TRANSFORMATION FORUM

Envisioning the 21st Century Grid



Ho: In addition to supporting all current AMI system requirements, PLC is also uniquely positioned to meet future demands not only from the standpoint of performance, but also in relation to reinforcing other technologies that Aclara brings to the market.

There are instances where power line may be the primary infrastructure technology chosen, but where RF or cellular network technology could be used to meet specific requirements for throughput, data rate, or number of channels over the air. For example, a utility may have its residential meters on a PLC system, but may have some commercial meters transmitting data at five-minute intervals to support time of use rates. In this type of case a cellular or RF solution might supplement the PLC system. Combining technologies and offering a hybrid solution benefits utilities by allowing them to leverage data collected from all sources.

For example, Aclara has developed unique fault detection and localization solution that employs one-byte fast ping signals to collect data in areas where there might be a power outage. Then enhanced data analytics are applied to identify areas of probability for an outage, to verify where power failures have occurred, and to monitor restoration.

PLC also has ability to deploy analytics in the head end, which allows us to leverage the information that would normally be collected.

In terms of throughput, PLC can collect data in up to 15-minute intervals and perform on-demand reads. Moreover, in addition to being able to perform concurrent communications on feeder and phase, sophisticated grouping methodology in the head end system allows grouping reads together on an outbound basis, allowing the system to handle groups containing up to 256 devices. That enables PLC to deliver the throughput and performance that customers require.

Plus, when you look at the installed base, no customers have exceeded a 50% free time network usage. What this means is that for many customers, a daily read or the customer's daily requirements are finished within three to four hours. Since no

one has saturated a network more than 50%, there's still a lot of capacity and capability to take advantage of in the PLC systems out there.

There also continue to be developments to improve the ability of PLC to read meters and perform other functions, allowing it to work even faster. As customers have articulated requirements, there are certainly situations where a five-minute interval would be beneficial. These requirements can be met with other solutions in a hybrid situation. The key is to sit down and talk with customers to understand what they need and how to align PLC to meet their performance requirements.

EET&D: What other functional areas beyond AMI can PLC support?

Ho: From a functional perspective, PLC systems support load control and demand response solutions, as well as capacitor switch bank controllers and transponders. In fact, demand response systems were some of the earliest solutions available over power lines, even for customers not using AMI.

EET&D: Is PLC always a suitable technology solution?

Ho: There are some power distribution architectures—such as those that are typically found in higher density urban environments—that don't really lend themselves to using PLC. For instance, where a high number of feeders are emerging downstream from a distribution substation. If those feeders are interconnected, then issues could result related to feedback of the power line signal, causing distortion.



A power line communication system operates on existing power line infrastructure, with communications equipment required in the substation.

THE GRID TRANSFORMATION FORUM

Envisioning the 21st Century Grid



EET&D: What about the use of power-line communications in urban environments? Is there a way to mix power-line communications with RF?

Ho: When we talk with some customers that have a mix of urban and geographically disbursed environments, that's where we start to discuss hybrid systems that combine RF and PLC.

For dealing with urban-rural cases, the key is to understand meter densities. The meter-dense area could be a city, but it could also be a growing subdivision with a much higher density than the bulk of a service territory. Obviously, the challenge in a hybrid system is not to double up on the infrastructure. The utility must separate the substations that have the more geographically disbursed assets from those that have a higher meter density, and apply the most appropriate solution to each group of substations.

By blending PLC and RF, hybrid solutions could offer significantly lower cost of ownership for the customer. This requires an examination of the structure in terms of substations, including what areas are more urban. By closely working with the customer, the data about substation configurations necessary for applying the best combination of solutions can be developed.

EET&D: What is the advantage of investing in the technology and what do you see as the future for power-line communications solutions?

Ho: We're investing not only in the actual communication technology, but also in the analytics – what we do with the data. Combined with the knowledge we've gained through our acquisition of a meters company, our data scientists have been very creative in how we leverage the data from our smart meters to create new value. For instance, the prospect of developing a cost-effective PMU (phasor measurement unit), is something that would have proved challenging in the past, but is now something that we are considering.

And it's not necessarily just infrastructure that we're investing in—it's the entire solution for the customer. Certainly, we have next generation R&D in the works where we are looking at ways to reduce the cost of substation communication equipment. We also will also be integrating some of our grid monitoring solutions with PLC so that we can provide enhanced fault detection with smart grid sensors on the medium-voltage side of the distribution grid. In addition, much of our development is happening at the head end and system as we try to take advantage of the data we're collecting to provide a broader range of solutions.

Because of its unique capabilities, PLC is specifically suited to a segment of the North American power distribution market where it is the ideal, best-in-class solution.

About the author



Lily Ho leads Electric AMI product management and new product introduction initiatives at Aclara. As Vice President of Product Management and Product Marketing/Electric, she is responsible for driving growth in Aclara's smart infrastructure solutions portfolio. Ho has over 15 years of experience in the energy and utility space managing large engineering projects closely aligned with risk management and sales functions. Before joining Aclara, Ho worked at TransCanada and, most recently, GE Energy, where she was responsible for over \$400 million of sales in the Power Generation Services business.

Ho holds a Bachelor of Aerospace Engineering degree from Carleton University.

i. Aclara acquired the electric meters business from General Electric Grid Solutions in December 2015. <http://bit.ly/AclaraMeters>

GREEN OVATIONS

Innovations in Green Technologies

The Killer App for Renewable Generation

By Ross Malme



Since the turn of the century, the United States has been the world leader in creating opportunities for demand response (DR) in wholesale electricity markets. Beginning in the early 2000s and starting on the East Coast, DR provides necessary energy and capacity resources when increased wholesale prices are high, driven by generation capacity and transmission congestion constraints. Today, the markets have evolved to allow DR to provide ancillary services such as non-spinning reserves, spinning reserves and even frequency and voltage support to its consumers. Even with all of its success over the last two decades, DR has been viewed as a “siloe,” or standalone, application with little communication and connection to other grid resources like storage or renewable energy resources.

At the Peak Load Management Alliance (PLMA) Spring Meeting in Nashville in April 2017, several industry experts pointed out the days of DR as a standalone application are over. DR is now viewed as an integral part of “edge of the grid” distributed energy resources (DER) such as rooftop solar panels, behind the meter energy storage, electric vehicle charging stations and microgrids. In fact, DR will now complement and compete against other DERs in various wholesale markets.

One of the more intriguing transformations in the industry is the way in which residential electric water heaters are being used by electric utilities (mainly electric cooperatives) as DERs. Use of resistance heating water heaters in utility one-way direct load control programs has been around for several decades. These programs have reliably provided valuable capacity to utilities and are one of the most cost-effective programs that these utilities deploy.

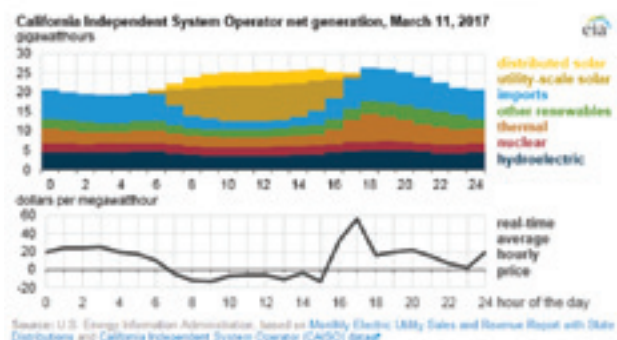
The convergence of two separate but related phenomena is about to change the paradigm of how we think and utilize the residential water heater as a DER for the

grid. The first is the evolution of the Internet of Things (IoT), which has now made cost effective two-way communication available to devices in the home such as smart thermostats, electric water heaters, load control devices such as pool pumps, and other smart appliances. This enables two-way communication with the water heater to provide not only near real time measurement and verification (M&V), but also to monitor the water heater during load management and charging cycles to assure the customer will never experience a program driven cold-water event, allowing more dynamic control of the water heater while still maintaining customer comfort.

The second phenomenon is the dramatic growth of renewable energy resources, most notably wind and solar, in several states that have high Renewable Portfolio Standards (RPS). Indeed, some states on the East Coast, Midwest and West Coast have renewable energy goals that exceed their RPS and over time will approach 50 percent. This has already resulted in frequent periods of overproduction, meaning that non-dispatchable base load generation (usually coal plus nuclear) and renewable energy generation exceeds demand during certain periods, resulting in curtailing renewable energy generation, negative energy prices or both. These negative energy prices have occurred frequently in the Midwest and in Texas. Both areas have significant wind generation resources which receive a \$23-\$24 Federal Production Tax Credit (PTC) for each megawatt (MW)-hour generated, incentivizing the generators to produce even when wholesale prices are negative.

This occurred last March in California, which is soon to have as much as 5,000 MW of excess solar generation in the afternoon. This same phenomenon is predicted to occur throughout the PJM ISO territory in the near future. How are these two-phenomena related? Let me cite a real-world example for you.

Rising solar generation in California coincides with negative wholesale electricity prices



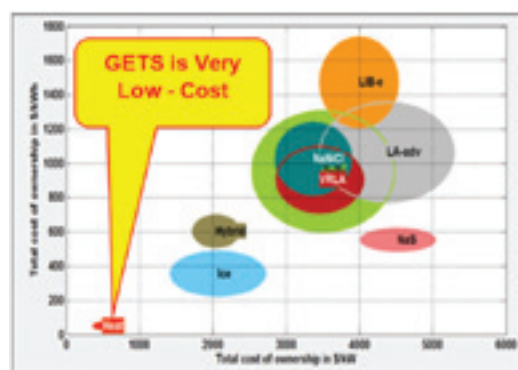
Great River Energy (GRE) is a generation and transmission electric cooperative in the Midwest that has more than 1,000 MWs of wind energy resources under contract in its resource portfolio. GRE is required to take delivery of the wind energy from its wind energy resources even when the demand for energy from its member cooperatives is at its lowest – typically in the middle of the night. Because GRE is part of the MISO system—they buy all of their energy needs from the market and sell all of their energy resources to that same market. In many hours – particularly in the off-peak hours, the price that MISO is willing to pay to GRE for its wind resources is far below GRE’s production cost – that’s a loss you don’t make up in volume! There are some hours that GRE may have to pay MISO to take the energy (negative prices).

In order to manage this potential challenge, GRE uses its residential grid-interactive electric water heater program. GRE has 70,000 large (85-105 gallon) electric water heaters, which they “charge” each night. It costs GRE a little more than two cents per kilowatt-hour to purchase energy in the wholesale market during off-peak hours – generally 11 p.m. to 7 a.m. (In essence, they are storing the excess wind generation by pre-charging hot water heaters). The water heaters are then shut off (not charged again) for 16 hours during the day when the demand for electricity and price to charge the water heaters is significantly higher. This is not only a win for GRE and its members, but also for the renewable wind generators.

Take a minute and think about the implications. Environmentalists need to realize there are roughly 50 million electric water heaters in this country. The market for new and replacement residential water heaters is estimated at 8 million units per year, depending upon new construction

rates. Roughly half of the water heaters are electric and half are natural gas or propane. In the past, the environmental community strongly preferred gas over electricity to heat water as electricity came from coal-fired generation and gas was thought to be a much cleaner resource. Fast forward to today’s environmental footprint, we have a much different picture as much, if not most, of the generation is supplied by renewables of its environmental footprint.

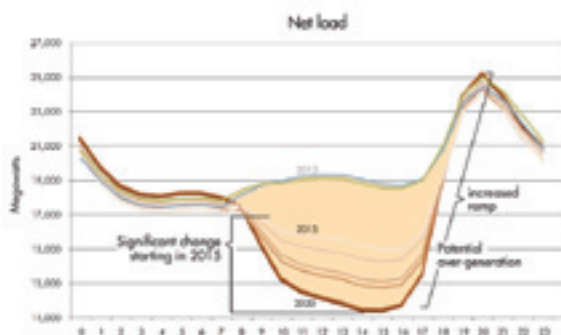
From a DER perspective, we have just turned a one-way direct load control device into a grid-interactive thermal battery that can be charged and discharged one or more times a day without any degradation in performance. That device holds twice the energy of a Tesla Powerwall at roughly 10% of the price. A recent study, performed by The Brattle Group in January of 2016, entitled “The Hidden Battery – Opportunities in Electric Water Heating,” found the cost of a new grid-interactive water heater installation would have a payback in the range of five years in certain markets, and for controls only retrofits the payback would fall to three years or less. From an alternative perspective, one could say the grid-interactive electric water heaters are **the most environmentally friendly and by far the least cost-method** of energy storage by a factor of five-to-one. The environmental community should be beating a path to electric utilities to promote grid-scale electric water heaters. This may also include systematic replacement of gas water heaters with grid-interactive water heaters. It’s a no brainer.



As shown in the illustration, developed by Keith Dennis with NRECA using Sandia National Labs energy storage analysis tool ES-Select™, Grid Enabled Thermal Storage (GETS) is very attractive compared to other energy storage options for load shifting applications.

California is an interesting case, where the majority of the state's residential water heaters served by the investor owned utilities are using natural gas. Each of these natural gas water heaters is putting greenhouse gases into the atmosphere every day. Recall that California also has a growing problem with excess solar generation in the late morning and early afternoon causing problems, which require the ramping up of thousands of MWs of gas fueled generation each hour in the evening. This problem is shown in CAISO's "infamous" Duck Curve¹.

Growing need for flexibility starting 2015



Converting the millions of gas water heaters in California to grid interactive electric water heaters would be a "twofer". First, a significant source of greenhouse gas emissions would be eliminated and secondly, the California solar industry would benefit from a thermal battery fleet which can "soak up" a significant amount of renewable generation reducing grid "over/under supply" operating issues and the potential for curtailments in the future of renewable generation. Grid interactive hot water heaters could time shift excess renewable supply as well as address the ramping problems in the morning and afternoon.

This is but one example of how an "old" demand response resource is being repurposed to integrate other DER resources in a new paradigm. I believe that in order to take this resource from pilot-project stage to market transformation, the environmental community needs to get on board with the utility industry, and the grid-interactive water heater community needs to educate the policymakers as to why this is a low risk/high return opportunity for the energy industry. What do you think? Whether you agree or disagree, let me know so we can spark a great discussion in influencing transformation.



Your electric storage water heater is a thermal battery that can help integrate renewable energy into the grid.

About the Author



Ross Malme is a partner and member of the Skipping Stone board of directors. Malme joined Skipping Stone in May of 2011 and leads Skipping Stone's Smart Grid, Demand Response, and International Business Practices. These practices have included leading Skipping Stone's engagement as technical advisor to the US Trade and Development Agency (USTDA), which is focused on export of US Smart Grid Technologies to the developing world as well as similar engagements with the United Nations and international development banks. In addition, Malme is a former member of both the National Energy Standards Board (NAESB) Executive Committee Retail Gas Quadrant and the Advisory Board to the US Secretary of Commerce on Renewable Energy and Energy Efficiency. He also currently serves on the Advisory Committee for Pennwell Publishing's DistribuTECH Conference.

1. The Duck Curve depicts the CAISO hourly load required to be supplied by conventional generation after all available renewable generation is utilized (Net Load). As renewable energy quantities are steadily increasing in early afternoon (see Rising Solar Generation in

California chart above) the conventional generation required to serve Net Load is reduced towards zero. This causes significant grid problems in the afternoon as solar energy rapidly decreases requiring conventional generation to quickly ramp up to supply load.



From Research to Action

EPRI's Telecommunications Initiative: Taxonomy Providing Wireless Opportunities and Options

This is the second in a series of five articles focusing on each of the five pillars of EPRI's Telecommunications Initiative, which is studying the impacts of a changing telecoms environment in the utility space.

By Tim Godfrey and Chris Kotting

The energy industry recognizes the need to improve the performance, reliability, and security of utility communication systems used for distribution automation, telemetry, and control. Currently there is no one architecture or technology solution that meets the needs of the industry, or even the entire operating area of a single utility. The diversity of proprietary and standard technologies—and the complex and fast-moving pace of new technologies, particularly in wireless communications—compound the difficulty in identifying an optimal architecture.

In response to these challenges, the Electric Power Research Institute (EPRI) is developing a utility telecom wireless taxonomy as part of its Telecommunication Initiative. This taxonomy will guide utilities in framing telecommunication needs, help them understand the technology options, and inform the process of identifying architectures and systems that meet both current and future needs.

Taxonomy is the practice and science of classification of things or concepts. Taxonomy helps people make sense of the things around them.

EPRI will work collaboratively with electric utilities and the telecommunications industry to focus on defining and characterizing the needs and requirements of an evolving electric grid and develop an approach to specify architectures and technologies. EPRI's researchers have identified logical tiers of classification based on the requirements of different utility applications and the natural, functional boundaries of current and emerging technologies. The process may also identify where there is a "gap" or mismatch between the capabilities of available technologies and the requirements of applications. EPRI is exploring these boundaries in the areas of utility networks and centralized generation, substations and distribution systems, distributed generation, and technologies at the edge of the grid, such as advanced metering infrastructure (AMI) and metering technology. Achieving interoperability with different classes of systems and technologies and properly defining and classifying them is the primary part of this research mission.

The Quest for the Telecommunications Holy Grail

The Holy Grail for buyers of communication systems is interoperability: the ability to pair equipment from vendor A with equipment from vendors B, R, Q, and Z and know that they will

work the first time, every time. Unfortunately, many vendors seek to "lock in" customers with equal fervor. For the utility, being locked-in to a vendor's platform limits flexibility and system expansion and eventually leads to costly wholesale replacement of systems to implement new technologies. Because of this issue, the taxonomy is being built primarily around standards-based technologies. The use of standards-based technology has many benefits including multi-vendor sourcing, multi-vendor interoperability, backwards compatibility, extensibility, and easy migration to future technologies. Where standards-based technologies are not yet available, EPRI's researchers will develop ways to support interoperability through industry alliance-based testing and certification.

Defining the Universe

In general, available wireless communications technologies break down into a few broad categories, with differentiation between those categories being a matter of the wireless spectrum used, whether the spectrum is licensed or unlicensed, and whether any licensed spectrum is owned or shared with other uses. Each of these factors leads to tradeoffs in range, bandwidth (how much data can be communicated), latency (the time lag between transmission and reception between two points on the network), or other factors affecting their use in a utility environment.

- Mesh systems, in which each communicating device on the network also serves as a repeater and range extender, are easy to deploy, low-cost, and flexible, but they can have higher latency than point-to-multipoint technologies depending on the number of "hops" between points. Mesh networks for AMI have relatively low data rates, but some types of mesh networks based on Wi-Fi can provide rates high enough for video.
- Point to Multi Point (PMPT) systems have better throughput for enabled links, but they are complex to manage and difficult to scale.
- Systems using higher frequency bands have more limited range per hop, but they can provide very good bandwidth and often have less interference.
- Commercial LTE-based systems have the advantage of mature technology and broad availability, but they have the disadvantage of requiring subscriber or sharing arrangements or operating as an overlay on other networks, each of which makes managing the quality of the utility's network connections difficult. Private LTE systems are desirable, but the options for accessing suitable spectrum are limited and can be costly.



From Research to Action

Because of these tradeoffs, there is no clear winner for all utility systems, or even for any one utility. Often, the ideal architecture incorporates multiple technologies, taking advantage of the strengths of each, and applying each technology where it is most advantageous.

Coming Attractions

EPRI's taxonomy report will be distributed to participating utilities in the summer of 2017, although preliminary results are being shared now with utilities participating in the research collaboration. In the next phase of the research, the team will develop a planning framework, which will be released in early 2018. However, the need for research in the evolving world of wireless communications never truly ends. EPRI's ongoing research into communications technologies will build upon the reports currently being developed and provide a continuing source of updated, relevant information for the utility industry. Taxonomy is the first step. To learn more contact the authors.

About the authors



Tim Godfrey is a Technical Executive with the Electric Power Research Institute, specializing in Telecommunications. He manages the Telecom Initiative, a research project addressing the key challenges utilities face related to the telecommunications infrastructure supporting the smart grid. He holds a BSEE from the University of Kansas and has worked in the area of wireless networking and communications for 20 years. He has 23 granted patents. Mr. Godfrey has participated in IEEE standards development since 1994. He is the Chair of the IEEE 802.24 Smart Grid Technical Advisory Group, and the IEEE 802.16 GRIDMAN Task Group.



Chris Kotting is a technical advisor for ICT and Cyber Security at the Electric Power Research Institute. He was previously engaged as a consultant and author on the development of communication standards for the electric industry, working with SGIP, NAESB, and other industry alliances. Earlier in his career he was on staff at the Public Utilities Commission of Ohio, working in numerous policy and regulatory roles, in both the energy and telecommunications industries. He has a BA in Communications from The Ohio State University.

HIGH VOLTAGE, INC.
HVI - The World's Source for High Voltage Test Equipment

Cable Fault Locating & VLF Testing

HVI Makes it Easy and Efficient

VLF/Thumper Combination
 VLF hipot: 0 - 33 kVac @ 1 μ F @ 0.1 Hz
 Fault locate: 0 - 13 kV @ 760 J
 VLF Fault Burner
 Radar/TDR ready
 Other Thumper models:
 5/10/20 kV @ 1000 J
 9/18/36 kV @ 3200 J

All That You Need

- Very Low Frequency AC Technology
- Cable Diagnostic TD & PD Testing
- Cable Fault Locating with Controlled Energy
- AC & DC Hipots, Aerial Lift Testers, Oil Testers
- Ω -CHECK® Concentric Neutral Testing
- Custom Engineered & Fabricated Van Pkgs.

50 kVac @ 3 kVA Hipot
1 piece & w/cable output

VLF 0.1 Hz @ 34 kVac
Comp. control - wireless

80 kVdc Hipot/Megohmmeter
1 instrument - 2 tests

ISO 9001 2008
HIGH VOLTAGE, INC.

USA All HVI Products are Made in the USA

31 County Rt. 7A • Copake, NY 12516 • p. 518.329.3275 • f. 518.329.3271 • sales@hvinc.com • www.hvinc.com

Implementing the DHS's Lessons Learned to Secure Grid Systems

By Scott Coleman

Modern advancements in grid systems enable marked improvements in efficiency, production, reliability, and safety, all through increased use of “smart” assets and digital communications. However, this has led to a dependency on communication technology that is seemingly at odds with the ever increasing pressure to enhance cybersecurity in critical infrastructure. Even though much of T&D infrastructure is not explicitly subject to NERC CIP, these systems are vulnerable, and a target, as evidenced by the recent cyberattack on the power grid in Ukraine¹.

To better balance the need for communication and security in OT networks, such as power substations, and to determine how best to secure them, it's important to recognize the reasons behind each of their connections. The two primary reasons that organizations provide data paths into or out of their grid networks are:

- *To provide information to remote users outside the OT network (production data, SIEM, files, historians, monitoring/maintenance information, etc.)*
- or
- *To allow for remote command and control by users outside the OT network (error remediation, system adjustments, etc.)*

To this end, the US Department of Homeland Security, in conjunction with the FBI and NSA, studied the attack in Ukraine and released recommended best practices² that any organization can use to help secure their ICS communications. Considering much of the same architecture, converters and systems in use in the Ukrainian power grid are currently in use in the US, American operators would be wise to take the lessons learned by the DHS in that attack.

1. Map and identify all external connections within the OT network architecture

Until you have accurately mapped the network, there is no way of assuring that all points of entry into the OT network are secured, including connections to other networks within your organization. Therefore it is vital to take the time to thoroughly assess, map, and understand the literal ins and outs of your OT network, whether it is performed internally or by a respected

third party. This mapping often proves incredibly useful not just for securing ICS communications, but also for any number of cybersecurity or operational projects you may consider.

2. Reduce the attack surface of your OT network

No matter what the purpose or number of authorized users, it's very important to recognize that each external connection is a potential attack vector for cyberthreats both into and out of your OT network. In order to reduce the attack surface of the OT network, you must first reduce the number of connections to an as-needed or as-authorized basis only.

The DHS recommends that organizations, “Isolate ICS networks from any untrusted networks, especially the Internet. Lock down all unused ports. Turn off all unused services. Only allow real-time connectivity to external networks if there is a defined business requirement or control function.”

As evidenced by the Ukraine attack, where grid systems had to be reset manually, it also may not be advisable to remove all manual controls in place of a completely automated system. If they had not had the manual controls, some systems may have been rendered completely inoperable, with no way to recover them.

Further, the DHS suggests the logical use of network segmentation to restrict and further control communication paths. “This can stop adversaries from expanding their access, while letting the normal system communications continue to operate. Enclaving limits possible damage, as compromised systems cannot be used to reach and contaminate systems in other enclaves. Containment provided by enclaving also makes incident cleanup significantly less costly.”

Consolidating, limiting, or eliminating any unnecessary external connections and services makes it easier to monitor and defend those fewer remaining points of entry into (and exit from) your OT network. Segmenting your networks can also cut off malware proliferation before it finds its way throughout your organization.

3. If any of the remaining external connections are for monitoring purposes only, convert them to one-way connections

Many times it is thought that the only way to perform remote monitoring is to allow remote access into the substation network to gather data for monitoring. In a disconnected architecture, service personnel may have to make a trip out to each substation to gather the data. However pushing or replicating data (historians, databases, or other monitoring data) out of the remote substation to the IT network has proven to be a secure way of getting data into the hands of end-users, without the need for a trip to the remote location to retrieve the data.

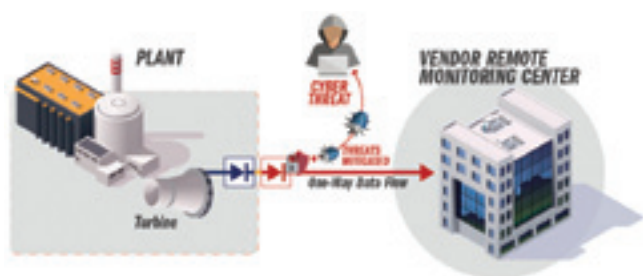


Figure 1. One-way connections for remote monitoring without remote access

Again the DHS recommends “If one-way communication can accomplish a task, use optical separation (“data diode”). ... Where possible, implement ‘monitoring only’ access enforced by data diodes.” Data diodes are one-way transfer devices that allow operational data to exit the organization for monitoring or use by a remote user, without opening a potential entry point or attack vector into the OT network.

4. If data transfers into the OT network are required (software updates, patches, etc.), convert as many as possible to one-way connections

Despite the desire to lock down the network and keep all threats out, data files, usually in the form of a software patch or update from a vendor, often need to be transferred into OT systems. With a locked down network, this is typically achieved with some kind of portable media (thumb drive, laptop, etc.). However, this runs the significant risk of infecting the network when something other than the software update exists on the media. As the DHS notes, “ICS-CERT responded to a Stuxnet infection at a power generation facility. The root cause of the infection was a vendor laptop.”

The DHS recommends that organizations, “Get updates from authenticated vendor sites. Validate the authenticity of downloads. Insist that vendors digitally sign updates, and/or publish hashes via an out-of-bound communications path, and use these to authenticate. Don’t load updates from unverified sources.”



Figure 2. Using one-way connections for data transfers into the OT network

Data diodes can simplify this process for secure inbound transfers by utilizing a manifest and hash code verification to ensure the correct and unmodified file is transferred, including matching the file provided by the vendor on their website or portal. Any file or software that doesn’t appear on the manifest or have a matching hash code is placed in quarantine and is never transferred to the OT network.

5. Lock down any remaining two-way connections with defense in depth

Most likely, some business or support operations are going to require a two-way external connection. Whether it’s for remote command and control, error remediation, or some other critical purpose, it’s not always possible to eliminate two-way external connections completely, but it’s vital that these remaining connections be heavily controlled.

“Limit any accesses that remain,” says the DHS. “Some adversaries are effective at gaining remote access into control systems, finding obscure access vectors, even ‘hidden back doors’ intentionally created by system operators. Remove such accesses wherever possible, especially modems as these are fundamentally insecure. ... If bidirectional communication is necessary, then use a single open port over a restricted network path.” This can be accomplished through a highly secured firewall, or a specialized bilateral data diode implementation, using one data diode for each direction in and out of the network.

Implementing the DHS's Lessons Learned to Secure Grid Systems

In addition, like NERC, the DHS advises against any kind of persistent connections to grid systems, especially from third parties (or the Internet) – “Do not allow remote persistent vendor connections into the control network.”

Bottom line, make sure all external connections are limited in capability, restricted in their paths, and if possible, only exist for a limited amount of time.

Defense in Depth

As part of a layered, “defense in depth” cybersecurity strategy for grid systems, a variety of tools are employed, from role-based access controls, multi-factor authentication, whitelisting, and more. Beyond these baseline tools, the two major transfer technologies used to control access points within OT networks, firewalls (software-based) and data diodes (hardware-based) provide the strongest means to secure ICS communications. Yet it's important to point out that the fundamental differences, and reasons for using both of these tools, either together or separately, in different situations, to increase the security of your ICS systems.

Software solutions, such as firewalls, are highly versatile cybersecurity tools that can be augmented with a number of security information and event management (SIEM) capabilities, from intrusion detection to deep packet inspection. However, they are also inherently vulnerable to configuration changes, bugs, and they will always require regular updates (or replacement) to stop new and emerging threats.

Hardware-enforced solutions utilize physical components to prevent access to secured networks. For instance, data diodes contain specialized circuitry that only allows data to flow in one direction. The sending circuit is incapable of receiving data, and the receiving circuit is incapable of sending data. For this reason, hardware-based transfer solutions cannot be hacked, and when used to transfer data out of an OT network, cannot be used as a threat vector back into the OT network.

These fundamental differences don't necessarily have much of an impact in environments where cybersecurity is less important, but they have a big impact when it comes to critical or sensitive networks. For example, data diodes are used in US military and intelligence cross domain deployments, to transfer data between networks of different security levels, while software solutions cannot be used in these cases, as they are simply not secure enough. On the other hand, well configured firewalls can be useful to secure a vital two-way connection, or used in conjunction with a data diode solution.

Keep in Mind

So in summary, the DHS advises that organizations reduce the number of connections to grid systems, use hardware-enforced one-way transfers where possible to limit exposure, anticipate one-way transfers may have to be made **into** and **out of** grid systems based on business needs, and for those two-way connections that cannot be eliminated, limit their capability, their communication paths, and the amount of time they are connected.

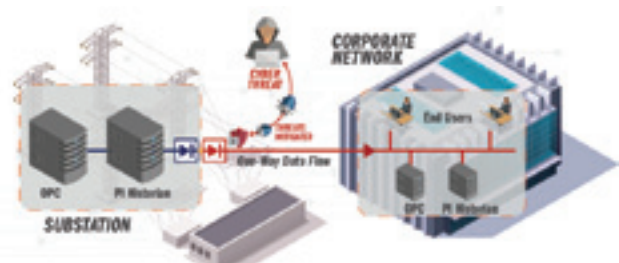


Figure 3. A secured substation network architecture

While defending the perimeter may have fallen out of vogue recently in favor of intrusion detection, advanced biometric authentication, and other measures, keeping intruders out is still one of the best methods to prevent damage to or hijacking of critical systems. Following these five concrete steps from the DHS can help to dramatically improve the cybersecurity of grid systems with minimal disruption to normal business operations. Those that may have considered data diodes years ago may have found them “out of their league” or prohibitively expensive. However, with recent advances in technology and the corresponding dramatic decreases in cost, data diodes are now actually more accessible and widely distributed than ever and are being used every day in a variety of industries and applications. For more information on data diodes, visit www.owlcti.com.

About the author



Scott Coleman has a strong technical background with 25+ years of experience working in high tech as a programmer, product manager and now as marketing manager for Owl Computing Technologies. His experience in real-time network solutions covers a number of industries including healthcare, telecommunications, call centers, wiretapping and cybersecurity for both the private and public sectors. He has authored many articles, hosted numerous webinars on a variety of topics and is an invited speaker at conferences.

1. <https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/>

2. https://ics-cert.us-cert.gov/sites/default/files/documents/Seven%20Steps%20to%20Effectively%20Defend%20Industrial%20Control%20Systems_S508C.pdf

What is between Grid of Things (GoT) and Internet of Things (IoT) is HoT (Holistically Orchestrated Things)

By Ron Chebra

The Grid of Things

When it comes to connected things operating interactively and in close harmony with other assets, one just needs to look at the electric grid as a prime example of how efficiencies and optimization can be achieved by leveraging remote monitoring and control. Intelligent grid and network-connected assets can be readily found throughout the transmission, substation and distribution networks. Some of these are shown in Figure 1.



Figure 1: Grid of Things

With assistance from the American Recovery and Reinvestment Act (ARRA) of 2009, increasing numbers of phasor measurement units (PMUs) are now being deployed, monitored and analyzed to provide greater visibility into our transmission network. These intelligent sensors are able to capture millisecond samples of power quality and transient information with extreme accuracy of both the physical measurements and precision time stamping; thus building a repository of data that can help prevent challenges in transmission.

Information that is gathered from PMUs and other line sensors will enable greater use of renewable energy resources to be grid tied at the supply level. When coupled with intelligent inverters that can be controlled by energy management systems (EMS), these assets now become viable assets to support the needs of bulk generation.

The interplay of PMUs and inverters is just one example of how the Grid of Things (GoT) leverages smart assets, communications networks and analytics to drive value to the enterprise.

Connected substations and interaction among connected elements has been a cornerstone of supervisory control and data acquisition (SCADA) operations. Intelligent end devices (IEDs), protective relays, power quality metering, compensation systems, and load tap changers have been orchestrated in concert, to deliver high availability, critical operational optimization and reliable and safe functionality. Standards such as DNP3 and IEC 61850 have helped drive wide acceptance of diverse elements from a variety of suppliers to achieve key operational requirements. Here again, the energy industry has achieved many of the objectives that the generalized IoT target is seeking.

On the distribution network side, there is a large number of assets that are operated either under centralized control or by local autonomous action. Fault location and service restoration (FLISR) is just one example where the operational objective for fast problem isolation, accurate network protection and improved service availability is met with a combination of line sensors that are either integrated into the recloser or provided by remote sensors.

However, with the proliferation of even more sensors and grid re-enforcement tools, such as advanced smart metering and grid connected distributed energy resource assets with smart inverters, the GoT interaction becomes even more critical requiring greater situation awareness and complex power flow models with near real time sensor data to drive algorithms that can be used to achieve the most effective result.

Conservation voltage reduction (CVR) and Volt/VAr optimization (VVO) are also some of the applications that are leveraging the capabilities of Advanced Metering Infrastructure (AMI) that provide near-real time remote voltage monitoring along the feeder to provide closed loop control of line regulators, capacitor banks and load tap changers (LTCs) at the substation. While one may consider that these capabilities can be enabled by simple machine to machine (M2M) communications, the real value of the GoT is achieved when all elements of the solution are fully managed.

What is between Grid of Things (GoT) and Internet of Things (IoT) is HoT (Holistically Orchestrated Things)

Management of all elements in the chain including end devices, communications networks, security and applications, are key characteristics of a GoT that must be in place to ensure the sustainability and viability of a given solution. Configuration data, operational characteristics, device rules, security keys, and core functional foundations, such as operating system (OS) updates are essential characteristics of device management. Providing this over a secure over-the-air process eliminates the need to visit each device. As networks become more integral to the solution, traditional means of network management must be augmented with tools and methods that must now include fail-over configurations, quality of service (QoS) and air-link management. Application management also becomes a critical component of the solution set particularly if this is provided as a cloud-based platform.

Building on the GoT movement is becoming essential to achieve key utility business objectives, such as improving customer average interruption duration index (CAIDI), and system average interruption frequency index (SAIFI) and managing distributed energy resource (DER) hosting capability. GoT is a foundational requirement for effective grid modernization.

Leveraging asset information that is delivered over reliable, robust and readily available communications infrastructures that enable actionable activities driven by analytics is the core foundation for sustainability required by the IoT.

The Internet of Things

Industrial, commercial, consumer and community use of the Internet of Things (IoT) represent another interesting aspect where the ability to leverage asset information command and control is leading to operational transformation.

Some of areas of interest include Commercial and Industrial IoT, Residential IoT and “Smart Cities” IoT.

- **Commercial and Industrial IoT**

Many industrial users have made significant investments and have a high reliance on process control systems to optimize their operations. Raw sensor data from instruments, such as voltage, current, phase angle, temperature, pressure, flow and humidity, are combined to drive programmable logic controllers (PLC) to manage manufacturing elements. Environmental information, such as occupancy sensors, outdoor temperature, wind, weather forecast, building envelope data, chillers, etc., are orchestrated under Building Management Systems (BMS) to efficiently control facilities.

A high level view of Industrial IoT is shown in Figure 2.

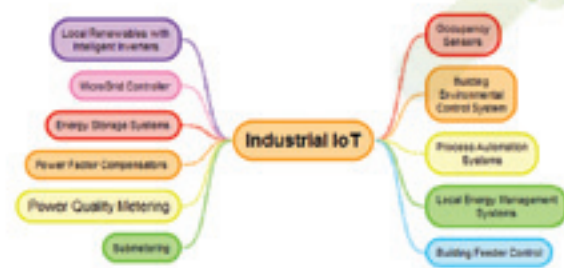


Figure 2: Industrial IoT

Many of these larger operations are now looking at a microgrid as an alternative to their traditional energy supply. These microgrids are generally equipped with combined heat/power (CHP), renewable resources, battery storage and load management, and load switching capabilities. Frequently these installations are balancing energy supply requirements against options that include supply from their traditional supplier and/or self-generation capacity. This optimization decision system focuses on achieving economic supply parity or to avoid peak or ratchet demand charges from their supplier. This mode of continuous optimized operation frequently includes local demand response or energy efficiency measures. Optimization of all of these resources is important when the facility is grid connected or operating in parallel; the measures that must be taken to ensure operations in an island mode are critical particularly when the self-generated resource mix falls short of the load it is required to support. Effective islanding mode must include levels of load shed and balancing. Intelligence is mandatory to ensure safe operation during island mode. This is most acute when system re-synchronization is required during re-establishment of a grid connection.

- **Residential IoT**

In the Residential IoT space, there has been a growing interest in Home automation (HA). Many providers are offering customers the ability to manage their lighting systems, media centers and even white-good appliances using device connectivity. There is an explosion of connected devices communicating over Wi-Fi directly or over Z-Wave, or ZigBee bridges that are connected to the internet to access simple interactive and intuitive applications that can be found on smartphones. While for some time this was considered to be a home hobbyist domain, connected home applications are among the fastest growing consumer market. With the advent of Amazon Echo (Alexa) and Google Connect (hey google), the technical knowledge needed to automate a residence has dropped drastically. The Consumer Electronics Show this year had thousands of devices that had some energy management capability pre-integrated with Alexa.

Some of the Residential IoT areas are highlighted in Figure 3.

What is between Grid of Things (GoT) and Internet of Things (IoT) is HoT (Holistically Orchestrated Things)



Figure 3: Residential IoT

• Smart Cities and IoT

Smart Cities is a very topical discussion among municipalities seeking to leverage available assets such as streetlights and emerging community interests. Many utilities are evaluating how to provide community services such as intelligent parking space monitoring, traffic signal flow management, intelligent LED-based street lighting, camera surveillance, bus arrival times, emergency call buttons and so forth. Municipal entities are seeking ways to monetize these applications through smart advertising and other commercial methods, while approaching communications carriers to take advantage of the existing streetlight real estate to enable small cell networks.

Smart Cities applications frequently leverage sensors, such as motion or occupancy, to adjust street light illumination, resulting in economic savings from lower energy usage when full illumination is not necessary. Centralized knowledge about streetlight outages also reduces labor costs associated with traditional activities. In a similar fashion to payphones of the past, intelligent lighting assets are a natural location for electric vehicle charging stations. Common “Smart Cities” IoT applications are shown in Figure 4 below.



Figure 4: Smart Cities IoT

Holistically Orchestrated Things (HoT)

Although each particular area of IoT is of unique interest, there is a need to exploit the intersection of GoT and IoT, in an area identified as Holistically Orchestrated Things (HoT). See Figure 5.



Figure 5: Holistically Orchestrated Things

GoT and Industrial IoT

The opportunity for coordination among these domains focuses on transforming the relationship between grid providers and load entities from a “service delivery point” to an “energy partner.” This will become increasingly more prevalent as customer or jointly owned and operated supply assets transactively participate with the grid.

With lower-cost renewable assets finding their way on to facility rooftops or parking lots, many passive energy user customers are forging into deeper understanding of the potential energy value they can provide. Possible intersecting areas for Industrial IoT and the grid include:

- **Short-term grid support during anomalies (e.g. Voltage/Frequency Ride through)** – With the direction of IEEE 1547a, grid support functionality will need to be supported. The control of this may be an augmentation of a Distributed Energy Resource Management System (DERMS).
- **Improving grid stability by using customer-owned compensation elements** – Since some facilities have capacitor compensation to overcome local VAR conditions, these assets may be called upon by the utility to augment utility-owned assets.
- **Intelligent building control response to demand response requirements** – Leveraging the intelligence within a building management system may offer new tiers of potential demand reduction based on occupancy sensors, build envelop characteristics, etc.
- **Coincident Demand Peak Avoidance** – With grid-wide knowledge of demand characteristics, intelligent load control and sequencing may be used to minimize co-incident peak situations.
- **Customer based thermal/energy storage to as a Non-Wires Alternative (NWA)** – As utilities seek short-term options to new construction or re-enforcement, customer owned assets or potentially co-owned assets may be leveraged to overcome seasonal peak demands.
- **Microgrid optimization** – Utilities are in a position to help customers better understand their options for supply, load management and load profile characteristics.

What is between Grid of Things (GoT) and Internet of Things (IoT) is HoT (Holistically Orchestrated Things)

- **Outsourced MicroGrid operations and maintenance** – With increasing intelligence provisioned within the facility microgrid controller, utilities may be in unique position to provide services to support internal staff for operations and maintenance (O&M) as a service (when permitted).

Grid and Residential IoT

Although the individual contribution of any single residential energy provider may not be significant, aggregation of functionality and services provide an interesting potential area for greater exploration. Some of the intersecting areas of interest include:

- **Intelligent Demand Response** – Leveraging occupancy sensors and next generation thermostats that profile temperature recovery can provide new options for demand management.
- **Advanced Time of Use (TOU) applications** – With intelligent appliances and smart apps, the goal of autonomous, predictable and user-friendly, time-of-use device interaction may be realized.
- **Vehicle to Grid (V2G)** – With intelligent charging stations combined with knowledge-rich electric vehicles, the use of this customer asset may now effectively leverage grid conditions to react accordingly while still ensuring customer needs for convenience and cost.

Grid and Smart Cities IoT

Smart Cities provide additional potential for intersection of HoT. Some of the potential areas for collaborative value between “Smart Cities” and utilities include:

- **Common use for Communications Infrastructure** – Many AMI providers have already incorporated smart street light applications as part of their offering suite. Including streetlights as nodes on an AMI network has shown to improve performance, lower latency and deliver.
- **Gateway for fixed radio AMR** – The potential exists to leverage these assets as a home for collection gateways for older automated meter reading (AMR) that use a drive-by methodology.

- **Intelligent EV Charging Stations** – Since many of these assets would be located near vehicle parking, intelligence using Near Field Communication (NFC) or other tagging could be used to provide smart charging programs.
- **Smart Lighting Control** – LED replacement for traditional overhead lights can result in substantial savings (30-50%) and when coupled with motion sensing can further reduce many of these unmetered services by another 10%.
- **Streetlight Outage Response** – Leveraging luminary intelligence, servicing of dark lights can be optimized.

Conclusion

The collaboration between the GoT and the IoT provide opportunities for synergy, growth and innovative ways to bring value to the utility, customers and the community.

About the author



Ron Chebra, EnerNex Vice President of Grid Modernization, is a recognized thought leader and industry expert in utility modernization.

He has a deep operating knowledge in technology solutions in areas such as MicroGrids, Renewable Energy Integration, Smart Grid, Distribution Automation (DA), Advanced Metering Infrastructure (AMI) and Demand Response. He provides strategic consulting services to leading energy industry suppliers of products and services, in the following areas: microgrids, demand response, battery energy storage solutions and “Behind the Meter” technologies. Ron has over 35 years of experience, including previous positions with Schneider Electric and DNV GL.

REAL SECURITY
for Ringless Meter Sockets just got
FASTER!!!



U.S. PATENT PENDING

MADE IN THE USA **INNER-TITE** **MADE IN THE USA**
introduces the
BOTTOM-MOUNT JIFFY LOCK
Fast and Safe Installation • Preload Convenience
Extremely Rugged and Durable
INNER-TITE CORP. • HOLDEN, MASS • 508-829-6361 • www.inner-tite.com

Electric Utility Outage Prediction Models: Assessing Their Accuracy & Implementing Improvements

By Dr. Ronald O. Mueller
and Jason Singer

Introduction

Academic and industry researchers continue to press ahead to create ever new and better weather forecasting models (WFM). At the same time, electric utilities are continuing intensive work to improve the accuracy of their outage prediction model(s). And, of course, these two forecast modeling areas are highly inter-related – since weather forecasts are the single most important input to a utility's outage prediction model (OPM).

But, how do the major users of weather forecasts and of outage prediction models - namely electric utility storm centers - *really know* that the models and predictions are getting better and therefore can be relied on more during a storm event?

And, if the forecasts are getting better, it is important for the storm center personnel to know by how much, and for what types of storm events are things getting better, and which of the modeling areas is getting better – the weather forecasts or the outage predictions? Lots of really important questions need to be addressed in a quantitative scientific fashion.

To find this out, we need to quantitatively and accurately measure the accuracy of weather forecasts and outage predictions over a wide range of storm conditions. We believe the only realistic way to do that is to assemble, and then maintain going forward, a complete historical database containing all of a utility's:

- Weather forecast data
- Actual observational data
- Outage prediction data
- Actual outage data

Having this database in place, and maintaining it going forward, are the keys to examining critical questions on the accuracy of weather forecast and outage prediction models. Moreover, with this database platform, utilities can begin to examine – **for their specific utility service area** - the quantitative benefits

of bringing in various new weather forecasts, engaging in ensemble forecasting techniques, or possibly scaling the weather forecasts they have to account for special geographical conditions in the utility's service area that may not be well modeled by the general weather forecasting services.

Moreover, having this database platform in place, will also allow a utility to engage in quantitative evaluations of their current outage prediction models under different storm conditions, and to evaluate, again in a quantitative way, the benefits of various improvements that might be made to the models.

Database

To do this type of quantitative analysis we therefore need to assemble weather data and outage data, both forecast and actual. We need to assemble the forecast data and actual data over a utility's entire service area for an extended historical period, and incorporate processes for continuing this data assembly process going forward. This is quite a bit of work, and there are a number of tricky issues that will need to be dealt with to normalize, standardize, and summarize all the source data from the various data sources, as well as to put in place a series of statistical calculations for assessing the accuracy of the forecast data.

But once the database is in place, you now have a flexible analysis platform for assessing weather forecast accuracy and outage prediction model accuracy under a variety of different circumstances and conditions, for example: a particular storm event; a particular type of weather condition (e.g. for periods when sustained winds are over 40mph); a specific date period or specific section of the utility's service area. And as the issues or challenges change, the database platform can easily be engaged to analyze new issues and ideas since all the historical weather and outage forecast and actual data is already pre-loaded in the system.

Assessing Accuracy of OPM Forecasts

Our specific focus in this paper is on assessing accuracy of the OPM forecasts, and falls into three areas:

- Validating a utility's existing OPM model(s)
The goal here is to create a series of accuracy measures for assessing the utility's current Outage Prediction Model for each of the qualifying storms over the historical period in the database. With this in hand, the utility will have a quantitative view of the accuracy of their current model. As new qualifying storm events occur, the new OPM forecast and actual data can be added into the system to provide a continuing benchmark of how well the OPM does over time.
- Simulating the performance of the OPM under different weather forecasts
With both weather and OPM data loaded into the database, a new window of analysis opens up. We all know that the accuracy of weather forecasts translates directly into the accuracy of the outage prediction model, since weather is the predominant input to the outage model. The worse the accuracy of the weather forecast, the worse will be the outage prediction.

In this second type of analysis we are thinking of, the database platform can be used to devolve the compound inaccuracies of the weather forecast from the outage prediction model. That is, we can run **simulations** in which we increase the accuracy of the weather forecasts for all or some historical events (or eliminate inaccuracies all-together by changing the forecast weather data to be the same as the actual data). Then we can see how much that improves the outage prediction forecasts. In this way, the database platform can be used to see how accurate the OPM forecasts are intrinsically, aside from the inaccuracies introduced by the weather forecasts.

- Using the database framework to assess new OPM Features
A key new way this database platform can be used is as a validation framework for testing out the benefits of various possible new enhancements to a utility's OPM. As new improvements are made to the OPM, we can then use the database framework directly and easily to assess how much improvement each new feature makes to the accuracy of the OPM, as judged over the full historical storm dataset.

So the database will provide a quantitative benchmark for judging improvements one by one. This gives a utility a facts-based, *data-driven* way to assess their OPM currently and then to assess the benefits of various improvements made to the model.

Summary

Hopefully we have made the case – namely, that the validation capabilities inherent in building this weather and outage database platform are really an essential and appropriate tool for a utility to quantitatively assess their current weather and outage prediction models and for assessing improvements as well.

While not easy, building this database platform provides a utility with a data-driven and statistics-based framework to really see what the current OPM model delivers, and what different possible enhancements to the OPM system can achieve.

About the Authors



Dr. Ron Mueller is CEO and founder of Macrosoft. He is also Macrosoft's chief scientist, defining and structuring Macrosoft's path forward on new technologies and products, such as Cloud; Big Data; and AI. Ron has a Ph.D. in Theoretical

Physics from New York University, and worked in physics for over a decade at Yale University, The Fusion Energy Institute in Princeton, NJ, and at Argonne National Laboratory. Ron also worked at Bell Laboratories in Murray Hill, NJ, where he managed a group on Big Data, including very early work on neural networks.



Jason Singer has been the director of Macrosoft's Utilities Practice since 2005. Jason manages all aspects of Macrosoft's utility portfolio including Resources on-Demand, RAMP-UP, Outage Central, and Mine-Weather. Jason works closely with dozens of major utility clients to delivery

technology solutions that solve emergency restoration challenges. Jason earned a bachelor's degree from Rutgers University.



Utility Analytics Survey: Maturity Levels Vary Significantly But Showing Improvement

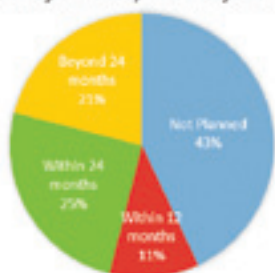
Today's utility industry stands on the precipice of discovering new insights that will transform the future of their business in terms of both strategic growth and operational efficiencies through the power of analytics. Specifically, the use of predictive analytics harbors enormous potential to help shape and transform the organization.

BRIDGE Energy Group's recent BRIDGE Index® Survey on Grid Analytics confirms predictive analytics is going mainstream; nearly half the utilities surveyed indicated they have deployed or are developing predictive analytics. In fact, the survey shows that:



- 22% have predictive analytics in operation
- 24% are developing predictive capabilities
- Asset health (33%) and outage management (37%) comprise top use cases

Plan Major Analytics Project in 2017



However, there is still a gap. Only 36 percent of the survey participants indicated that they were planning a major analytics project within the next 24 months, leaving a significant majority of utilities without a plan. Also, striking, utilities that do have major projects planned have demonstrated a lack of maturity in their analytics program. 54 percent of survey participants indicated that their efforts to date have been done without business case justification. Survey participants also overwhelmingly responded to the current state of their organization as "spreadsheet and information anarchy." Furthermore, a very small number of respondents reported that business process changes have resulted from their analytic efforts.

So why the gap between the potential of analytics and the progress with analytics? In part, it may be attributed to what is often viewed in utility organizations as the overwhelming prospect of collecting and extracting data across internal and external sources needed for analytics projects. Big Data is, in particular, a foundational requirement for advanced analytics programs looking to move towards predictive analytics.

However, a lack of in-house expertise can further exasperate the ability to evaluate gaps and determine use cases needed to solve specific business problems. Utility organizations can take the following measures to formalize an organization-wide direction to collect and analyze and use data for analytics.

Defining Your Vision & Strategy

Before launching an analytics project, utilities should ask and provide answers to these additional questions:

- What are we going to do?
- What type of a business challenge are we going to solve to gain high ROI?
- Can we justify the expense of the analytics project?



- Can we get the support of Business and IT departments to evaluate and access the integrity of the data to determine gaps that would impact execution?
- How would it meet the needs of future grid modernization efforts?

The answers to these questions will insure that your analytics initiative, large or small, has the right foundation from which to build. This focus on the core will also enable the organization to select and implement toolsets and frameworks that are reusable across the business.

Creating a vision for how your analytics program could improve your organization's performance gives the sense of a greater purpose for what is to follow, beyond a single independent initiative. This phase should lead you to answers to "why are we doing this" and "where do we want to go." The vision should also incorporate leadership's view, both at the business level and at the executive level, of where the organization should be with analytics in three-to-five years. Such a vision must also take into account key process changes that would need to align with meeting that vision, including adoption strategies and change management.

The strategy phase requires a disciplined view of the vision as it relates to identifying where analytics could solve a pressing business challenge and validating the impact; a high return on investment (ROI) or a cost savings, will help further justify the expense of the project; Each use case should be evaluated by business and IT to determine required criteria including access to data, integrity of data, and organizational changes to business processes. This step will also allow leaders to discover gaps that would impact execution.



For utilities focused on maturing their analytics programs, part of the strategy will be to look beyond spreadsheets or vendor tools that only report 'what happened.' BRIDGE defines

Predictive Analytics as using analytical tools to predict future operational conditions to prioritize where effort and capital would best be focused to deliver upon goals. In general, a core aspect of Predictive Analytics is using algorithms, for example in machine learning techniques, to analyze past situations to predict future situations. It is common to augment historical data with forecasted data from other sources for use in Predictive Analytics algorithms. For example, granular weather forecasts from external sources can be fed into algorithms to tweak dynamic line ratings.

Setting Priorities

With a holistic vision of your analytics program outlined and a strategy in place, the next step is to formulate the path you'll take to get to that vision. Creating a road map will ensure that initiatives are prioritized across the organization with a clear focus on delivering value. The process will require:

- Continued planned activities
- Prioritization of use cases, based on existing organizational, technical and data competences
- Value and complexity associated with the business case

For operational analytics, the value will be determined by the possibilities of improving efficiency, reliability, or operational safety for the grid. For those utilities selecting use cases entrenched in new technologies, they should be aware of the higher risk -- and should evaluate how these use cases can -- or cannot -- fit into the finalized roadmap. If faced with this challenge, utilities can leverage a 2x2 matrix to select high impact use cases, which will require low efforts.

Delivering ROI

With budget constraints facing today's utilities, long-term projects may not be easily accepted or financed. To avoid scrutiny and gain greater support, offer near-term wins that show the value of predictive analytics to solve business challenges and improve efficiencies. To succeed in this approach, it's imperative that the project team works closely with the business clients to define and refine needs and requirements. Creating a collaborative development team that provides feedback at regular checkpoints, including weighing in on concepts, designs and finished products will also allow for a seamless transfer of knowledge across the organization.

To offer reliable results, utilities should also focus on a minimal viable product (MVP) concept, which will also help establish support for future projects, since the basic foundations have already been built.



Conclusion.

In the BRIDGE Index survey, the single highest concern was the availability of resources with the necessary skills. Almost as many respondents reported challenges with integration and existing tools. BRIDGE recommends that utilities expect to need multiple resources to provide the necessary skills and experience to get value from their analytics investments. For example, utility SMEs could work alongside analytic and tool experts to explore data, to define rules for automatically assessing potential issues, and to specify key metrics for summarizing the results. Other resources could be needed for specialty skills in visualization (including human factors) and change management.

As stated before, analytics projects will bring great success to utility organizations and offer tangible business strategies that can help define a clear direction for the organization. Furthermore, analytics initiatives in the modern utility can be used to define operational changes, efficiency improvements, retain human capital knowledge, and determine where capital will be spent.

ABOUT THE AUTHOR



Glen Sartain,
VP of Grid
Analytics
at BRIDGE
Energy
Group, is
responsible

for strategy and design of analytic roadmaps and the implementation of these strategies. With more than 35 years experience in analytics and technology innovation for the energy sector, Sartain is recognized in the analytics community for his expertise in advancing analytic capabilities to help utilities improve operations.



OmniMax™ How a Street Says Welcome

All the benefits of LED without sacrificing the light you love.

It's the right light—not just the brightest light—that creates inviting environments. OmniMax was designed to mimic the HID bulbs it replaces in both size and performance. It screws directly into any existing fixture, and takes advantage of the lamp's optics, as they were designed.

Experience smart technology, guaranteed reliability, and the best overall value in LED retrofits. Special introductory pricing available to select customers.

evluma.com/beautifullight

evluma
the evolution of illumination

010101010101010101010100

By Dr. Tim Shaw

SECURITY SESSIONS

Strong Passwords: Making it Difficult for the Bad Guys

A topic that comes up quite often when discussing cyber security is the use of passwords and what is the right size and complexity and how often should you change them. The confusion around password usage often derives from a lack of understanding about what they are used for and the risks associated with improper use.

Knock three times and tell them “Charlie sent me”

Something such as a password would seem to be a pretty simple and obvious thing right? You pick a simple word you can remember, such as your wife’s name, you make a note of it on a “sticky,” which you attach to your PC just in case you forget, and you are good to go. I’m trying to be funny but the sad fact is that I see things like that all the time. Usually because the person has no idea about how passwords are compromised and what makes that process far less difficult for the bad guys.

To begin with, a password serves two purposes: First, it acts as a proof of identity to the computer onto which you are trying to login; second it acts as a barrier to prevent others from being able to login on that same computer pretending to be you. With most computers that support multi-user operations, each user is given a unique ID that is going to be associated with the access rights granted to that user and the files and software created and used by that user. But in most such cases user IDs are created using a simplistic scheme such as your first name, last

name and, (if there are more than one of you), a number. So I might have an ID such as “tim.shaw2”. It isn’t very difficult to guess that another user named Jim Phelps probably has a user ID in the form: jim.phelps# where the trailing number is something between 1 and 9. It won’t take many attempts to figure that out. So user IDs are not a very effective way of uniquely identifying a user. This is why unique passwords were added. For some applications, there is a desire to have even better proof that a person is actually the valid user they are claiming to be, and in those application technologies such as biometrics are used to give even stronger proof that a person is the actual user they claim to be. But for most of us a password is the way we prove our identity to the computer-based systems and devices we use.

We mentioned the purposes of having passwords above, but we have not actually defined what a password really is: a shared secret – only you and the computer know what your password is ... as long as you don’t write it down and stick it to your PC or office wall. Of course for your computer to be able to compare what you type-in to the password you both agreed to use when you initially specified the password it has to maintain a copy. But unlike writing it on a sticky note in most computers the password is scrambled using something called a hashing algorithm and only the scrambled version remains in the computer.

This is because in older operating systems the passwords themselves were maintained in a file and in memory and this made them too easy to steal. If you could get a copy of a memory dump or a system backup you could search it for passwords. Today more secure systems store only a “hashed” copy of the password. A hashing algorithm is a ‘one-way’ encryption scheme meaning you can’t unscramble it to get the original password back. When you enter your password the computer hashes it and compares that to the stored hash value. If they match your password was correct.

So how do the bad guys steal or “break” your password if the password doesn’t actually exist in the computer? That question, and its answer, set the stage for why most passwords need to be long and complicated and changed on a regular basis. I am not going to address insecure protocols wherein your ID and password are sent across the network, making them potentially available to snag. That issue is separate from why passwords need to be complicated and change occasionally. It has to do with the need to encrypt sensitive message traffic.

Breaking/cracking a password is the process of figuring out what your password must be by taking possible passwords you may have used and hashing them and comparing the hash value to the one stored on the computer. In some cases that process can be performed on the computer itself if the necessary data and software can be loaded and executed. But realistically most of the time passwords are broken (or ‘cracked’) by getting a copy of the hash file containing all user password hashes and taking that file to another computer where the cracking tools can be used. Readily available tools such as “Jack the Ripper,” which can be downloaded from the Internet, can take a long list of possible passwords and run through them one at a time generating a hash and comparing that value to the ones in the stolen password file. The longer your password the longer this process can take. If the attacker knows anything about your password policy the process can be speeded up by not trying possible passwords that don’t meet your policy. So if passwords, for example, must be 8 characters or more, the attacker will skip any possible passwords that are shorter. (A good reason not to let everyone know your password policy.)

Most such attacks work off of word lists of commonly used passwords or words in the dictionary and so avoiding use of actual words (and your name) is a good password practice. A brute force version of this method just runs through every combination of ASCII characters, including numbers and punctuation characters, to find your password. Using a distributed network of computers even a really long and complex password can be broken in a few weeks to a few months. (Using just a single PC the process could take many, many years.) And that is why you need to change your password every so often – so the bad guys don’t get enough time to crack it before you change it and force them to start over again. There are also something called ‘rainbow tables’ available on the Internet and these tables contain pre-computed hashes for millions of possible passwords. Such tables get quite huge and unwieldy for longer-length passwords (12+ characters) but when used they provide an almost instant ability to crack passwords of a short to moderate length.

So that brings us back to the two questions about passwords: how long and complex should they be and how often should you change them? The answer to those questions depends on the possibility of your hashed password file (the so called SAM file in a Windows computer) being extracted from your computer and taken away to be cracked. There are bootable CD and USB toolsets that let you boot-up your PC into the tool set without starting Windows. Using those tools one can extract the SAM file from the hard drive. There are remote exploits that enable access to the SAM file on a running system. If your system has the vulnerabilities this requires, then a remote attacker could get your SAM file and ‘crack’ your passwords. This is why most IT departments require 10+ character, complex passwords (e.g. special characters, numbers, upper/lower case letters) and ask you to change them monthly. Of course that often leads to people writing down their passwords in non-secure places because it becomes challenging to remember them.

Now all of this is well and good if we are talking about a PC or server running Windows (or Linux or OS-X) but does it apply to all digital devices and systems? Clearly, it can't, as you have devices such as PID controllers, protective relays, PLCs, trend recorders, annunciator panels, Ethernet switches and other digital/smart devices, which don't support this more advanced password functionality. Many of these types of devices either support one universal (and not terribly complex) password that all your instrument techs know or possibly two such passwords: one for read-only (look-see) access and the other for making changes, which all your techs know. In these cases, the purpose for the password is only to act as a barrier to prevent unauthorized use/access. Since many people may need to know those passwords their use provides no unique user authentication. On some of these devices, the password may be limited to a numeric sequence because the thing only has a numeric keypad for user input. You may have hundreds of these sorts of devices in your plant and changing all their passwords every month would be a Herculean task. They probably came from the manufacturer with a default ("factory") password – why not just use those? After all, if you forget one you can look them up with a Google search (as can everybody else!)

For the vast majority of these types of devices (but not all of them) there is no way to extract the stored password, either locally or via a network communications means, unlike with a PC. This means you have to 'brute-force' the password to find the correct one. If I can attempt a remote login to the device, and it places no limits on the number of tries I can have, then I can write a program to send all possible passwords until I find the right one (so hopefully that communication pathway is monitored for attacks or only enabled when needed). But if the device is isolated your only option is to stand in front of the device and enter password after password on its local HMI till you find the correct one.

As that activity might look suspicious it is unlikely to go unquestioned and thus an attacker would have

limited tries before being forced to move along. In such a situation it is potentially unnecessary to change the device's password unless someone who knows it is terminated.

Rather than changing passwords in such isolated devices on a periodic basis, some plants have elected to change them only when they are used. I know of a plant where device passwords are treated like keys. If a tech needs the password for a device they are given it from a master list and after they perform the needed work, the password is changed and recorded in that same master list, which is held by someone in authority and trusted. This scheme means that if someone leaves, you have very few devices that would need a new password.

So something as seemingly simple as a best practice for passwords is actually not simple at all. And there are lots of other cyber security factors that also seem simple at first look but have a lot of intricacies that are not immediately apparent and that can make them ineffective if not addressed properly. But that will have to be the subject matter for a future column.

ABOUT THE AUTHOR

(William) Tim Shaw (PhD, CISSP, CIEH, CPT) has been active in industrial automation for more than 35 years and is the author of Computer Control of BATCH Processes and CYBERSECURITY for SCADA Systems and co-author of Industrial Data Communications. Tim has contributed to several other books, and is a prolific writer of papers and articles on a range of technical topics. Tim has been directly involved in the development of several DCS and SCADA system products and regularly teaches courses for the ISA and the University of Kansas on a range of topics from cyber security to process automation and basic process instrumentation and measurement. Inquiries or comments about this column may be directed to Tim at timshaw4@verizon.net.

PRODUCT SHOWCASE

MITSUBISHI ELECTRIC
Changes for the Better

120 Series LED Display Wall



Guaranteed to give you up to 11.4 years of 24/7 continuous operation!

- Over 99.5% reliability rating
- No Burn-in
- No Image Retention
- Modular, Scalable and Upgradeable

www.mitsubishi-displaywall.com

THE EASIEST WAY TO BUILD



Precast Concrete Buildings
VERSATILE • DURABLE • FAST
ECONOMICAL • SECURE
Standard or Custom Designs • 8'x8' to 50'x250'
EASI-SPAN clear span roofs up to 50' wide

EASI-SET BUILDINGS

ONLINE QUOTE FORM
EasiSetBuildings.com
866.252.8210

ADVERTISERS INDEX

COMPANY	WEB SITE	PAGE
Cigre	www.cigre.org	Inside Front Cover
Doble Engineering Co.	www.doble.com	Back Cover
Easi-Set Worldwide.....	www.easisetbuildings.com	32
Edison Electric Institute.....	www.eei.org	Inside Back Cover
Evluma	www.evluma.com	28
High Voltage.....	www.hvinc.com	16
IEEE Power & Energy Society	www.ieeet-d.org	1
Inner-Tite Corp	www.inner-tite.com	23
Mitsubishi Electric Visual Imaging Systems	www.me-vis.com	32
RTDS Technologies Inc.	www.rtds.com	8
Systems With Intelligence Inc.	www.SystemsWithIntelligence.com	3

June 11-14, 2017 | Boston Marriott Copley Place | Boston, MA

Plan Now to Attend EEI's 2017 Annual Convention

Our popular closing general session dialogue, The EEI Leadership: A CEO Perspective, moderated by **Tom Fanning**, Chairman, President and CEO of Southern Company, will bring together EEI's leadership group for a candid discussion of the industry's top issues. Speakers include incoming EEI Chairman **Pat Vincent-Collawn**, Chairman, President and CEO, PNM Resources; **Chris Crane**, President and CEO, Exelon Corporation; and **Greg Abel**, Chairman, President and CEO, Berkshire Hathaway Energy.

The convention's **Energy Matters** breakout sessions will explore major opportunities and challenges that lie ahead for the industry.

Key topics for Boston 2017 include:

- Energy Policy at a Crossroads
- Building an Energy Workforce for Tomorrow
- Crafting Wholesale Markets to Last
- Powering Mobility in the 21st Century
- Driving Customer Value in a Changing World
- Taking Smart Cities to the Next Level
- Securing the Nation's Energy Grid
- Distributed Energy Resources: The Road Ahead
- The Dramatic Reality of Energy Storage

Don't miss The Connection

A networking hub where you can unwind and interact directly with industry executives, vendors, and colleagues. Enjoy coffee, breakfast, lunch, and our networking happy hour. Plus, take advantage of additional amenities such as virtual golf, shoe shine, and refresh and recharge lounge.

KEYNOTE SPEAKERS



Tom Brokaw

Award-Winning Journalist



Andy McAfee

Co-Director, MIT Initiative on the Digital Economy
Principal Research Scientist,
MIT Sloan School of Management



Edison Electric
INSTITUTE

CYBER SECURITY REGULATIONS ARE CHANGING.

IS YOUR TESTING PROGRAM READY?



New regulations are going to change the way you work – from the field to the office.

Laptops and equipment you use to test and maintain your substation assets have been identified as potential cyber security risks. There are new NERC CIP requirements to protect these assets from being compromised.

What does this mean for your testing program?

Doble can help you develop a compliant Field Force Automation program that will not only meet new regulations—it will fit into your work practices and improve efficiency.

We will work with you to make sure the program makes sense for your teams, your needs, and your systems.

**GET READY FOR THE APRIL 2017
DEADLINE**

Download our white paper: What does
NERC CIP mean for my testing program?
www.doble.com/NERCCIPpaper

