

**20** YEARS **EET&D**  
MAGAZINE

November/December 2018 Issue 6 – Volume 22



**EXPLORING  
JAPAN'S ENERGY  
AND OTHER  
GLOBAL INDUSTRY  
TRENDS**

02

INDUSTRY NEWS

08

POWER POINTS

**WRAPPING UP 2018** | Elisabeth Monaghan, Editor in Chief

If we are going to fulfill our mission to be the “go-to resource for the latest on the transmission and distribution side of the global electric energy industry,” we must remain a conduit for open communication. That means we also must pay attention when someone provides negative feedback or points out gaps in our content.

10

THE GRID TRANSFORMATION FORUM

**EXPLORING JAPAN’S ENERGY AND OTHER GLOBAL INDUSTRY TRENDS** | Interview with Ben Cohen

For this last Grid Transformation Forum of 2018, we spoke with Ben Cohen, director of global strategy with Autogrid. Cohen shares his insights on the energy market in Japan and other markets around the world where smart grid initiatives are transforming how electricity is produced and managed.

16

GREEN OVATIONS

**WINDS OF CHANGE: HOW ARTIFICIAL INTELLIGENCE AND OTHER EMERGING TECHNOLOGIES ARE REVOLUTIONIZING THE WIND POWER INDUSTRY** | Dr. Yan Ke

In the U.S. alone, the wind industry invested more than \$11 billion in new plants in 2017 and added more than 7,000 megawatts of new capacity, representing a full 25 percent of all electric capacity additions across the energy industry last year.

22

**THE ROLE OF CABLE REJUVENATION IN ADDRESSING THE MAINTENANCE OF AGING UNDERGROUND CABLES** | Glen J. Bertini

Consumers are generally unaware of the jumble of cables that each box comprises, and they rarely need to consider whether the URD itself is in an adequate state of repair. Most utility providers, on the other hand, are in a constant state of responding to aging cable and the threats it represents.

30

**SMART GRID WIRELESS COMMUNICATION: WHAT UTILITIES NEED TO KNOW** | Randolph Wheatley

Conducting a thorough examination of architectural impacts, signal attributes, business and regional challenges, as well as other factors impacting wireless utility communications, will help utilities make smart choices when investing in AMI. In this article, we examine the distinction between point-to-multipoint and mesh networks.

36

GUEST EDITORIAL

**HOW TO APPLY THE FOUR TYPES OF THREAT DETECTION** | Selena Larson

Modern threat detection falls into one of four categories: Configuration, Modeling, Indicator and Threat Behavior. Each is different, and it’s up to the organization to determine what they need and whether a new method can complement existing security tools.

40

GUEST EDITORIAL

**INDUSTRY-SPECIFIC CYBER PROTECTION REQUIREMENTS: POWER INDUSTRY IN NORTH AMERICA** | Jens Puhlmann

The last few decades have seen major advances in technology, resulting in significantly smaller devices, increased functionality and a new range of connectivity options. In general, the effect has been positive for everyone: Added convenience for consumers and industries alike; from online shopping and online banking, to increased productivity in all industries.

46

SECURITY SESSIONS

**CYBER IMMUNITY: A HOLISTIC VIEW FOR INDUSTRIAL CONTROL SYSTEMS** | Jonathan Azarcon

This article addresses the greater issue at hand – the potential future of cyber attacks, and whether this has become the new warfare. Attacks such as these have led to an intensified concern in various industries surrounding the protection of operational technology (OT) environments.

# COMING IN 2019...



...ELECTRIC ENERGY MAGAZINE WILL NOW  
BE PUBLISHED 4 TIMES A YEAR.



#### PUBLISHER

**Steven Desrochers**  
steven@electricenergyonline.com

#### EDITOR IN CHIEF

**Elisabeth Monaghan**  
elisabeth@electricenergyonline.com

#### ACCOUNT EXECUTIVE

**Todd Shipway**  
todd@electricenergyonline.com

#### ART DESIGNER

**Z communications**  
r.poitras@zcommunications.ca

ELECTRIC ENERGY MAGAZINE IS PUBLISHED 6 TIMES A YEAR BY:

#### JAGUAR EXPO INC

PO Box 50514, Carrefour-Pelletier, Brossard, QC Canada J4X 2V7  
Tel.: 888 332.3749 | info@electricenergyonline.com  
electricenergyonline.com

## ADVERTISERS INDEX

03

**SYSTEMS WITH  
INTELLIGENCE**

05

**RTDS TECHNOLOGIES**

07

**NETA**

09

**TECH PRODUCTS  
EASI-SET BUILDINGS**

28

**MITSUBISHI ELECTRIC**

52

**ELECTRONSYSTEM MD**

C3

**TALLMAN EQUIPMENT**

C4

**DOBLE**

## PJM COMPLETES FUEL SECURITY STUDY AS PART OF RESILIENCE INITIATIVE

*Results Confirm Grid Reliability, Identify Stress Points to Address Through Competitive Markets*

**November 2018**

As part of PJM Interconnection's ongoing initiative to assess the resilience of the electrical grid, today (11/1) the nation's largest grid operator released a summary of its study examining one critical element of grid resilience - fuel supply.

PJM's fuel security analysis results found that the system serving 65 million people in 13 states and the District of Columbia is reliable and can withstand extended periods of highly stressed conditions.

"The findings underscore that PJM is reliable today. But in this study we are also looking into the future, to stress-test our system to reveal future vulnerabilities and make sure we are resilient under many different conditions," said Andrew L. Ott, president and CEO of PJM.

The study was designed to test the grid's limits to endure high-impact, long-term disruptions to generators' fuel supply. The study also identified scenarios in which the system would face power outages, applying extreme, but reasonably plausible assumptions for weather, customer demand, generator retirements and fuel availability.

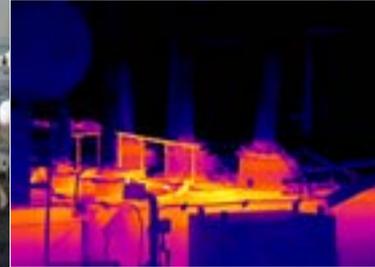
*"These results indicate that assessing generator fuel security should be a priority for PJM and its members," Ott said. "We will continue to look for opportunities to address resilience through the competitive wholesale electricity markets, in this case, by valuing resources that have secure fuel supplies."*

PJM's analysis stressed the system using more than 300 different scenarios that could occur from 2023 into the future. Testing conditions ranged from typical winter operations to extreme, but reasonably plausible scenarios. The analysis found that in a sustained period of cold weather with typical customer demand, PJM's system can operate reliably over an extended period of stress.

As with any stress test, the analysis was intended to identify tipping points at which stressed conditions begin to impact the PJM system. By subjecting the system to a series of extreme, but plausible scenarios, PJM found stress points, starting in 2023, which could result in material levels of generation unavailability and load shedding.

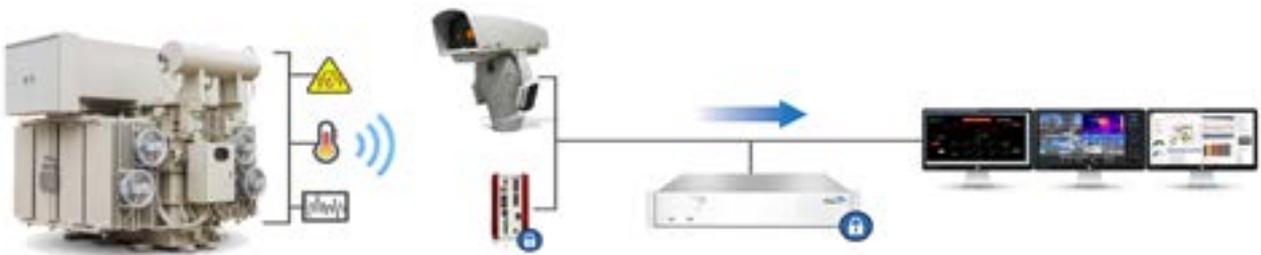
*"We found that in extreme scenarios, the more the grid was stressed, the more important fuel supply characteristics, location of the fuel supply disruption and demand response became," said Michael Bryson, vice president of operations. "We believe that some changes to the system in the future - both market-based and operational - are warranted. As with any stress test, there are extreme cases, and building to mitigate or eliminate risk must be balanced with costs."*

# REMOTE ASSET MONITORING



## Automated Data Collection

Knowing the health of your assets is the key to preparing an efficient, condition based maintenance plan. Gather the health indicators remotely, 24/7, with an intelligent automated system. Reduce truck rolls for inspections and maintenance with visual and thermal cameras and sensors. Track and trend data for condition based maintenance. For remote monitoring of substations, underground vaults or overhead line equipment, the SWI system provides real time visualization, data concentration and storage.



Aggregate, analyze and store data from remote sensors and cameras. Designed for electric power applications, the SWI system is substation grade and connects to SCADA, GIS and asset management applications.

Contact Us to Find Out More



Substation Hardened Servers and Gateways



Video Management Software



Substation Hardened IP Cameras



Mobile Monitoring

# PUC APPROVES TRANSFER OF JOINTLY OWNED UTILITY POLES FROM HAWAIIAN TELCOM TO HAWAIIAN ELECTRIC COMPANIES

*Plan aims to eliminate double poles and expand wireless networks*

## November 2018

The Hawaiian Electric Companies have acquired Hawaiian Telcom's ownership interest in approximately 120,000 jointly-owned utility electric distribution poles on Oahu, Maui, Moloka'i, Lāna'i and Hawaii island under agreements approved by the Public Utilities Commission.

In approving the plan, the PUC noted it "reflect(s) the efforts of both the Hawaiian Electric Companies and Hawaiian Telcom to provide a more efficient and effective administration of the pole infrastructure which includes the removal of double poles and implementation of current and future technologies such as 4G, LTE, and 5G networks, all of which will benefit the State of Hawaii."

The transfer is intended to reduce operating and maintenance expenses over time while creating efficient and safe practices for companies seeking to place new devices on poles.

### Other benefits include:

- Eliminating approximately 14,000 "double poles" in less than 10 years
- Improving customer service at a reduced cost by providing a single point of contact and a standardized management system across the Hawaiian Electric Companies for communication and data attachments by third parties onto utility distribution poles and Maui streetlight poles
- Reducing and shortening outages through faster pole repair and replacement with increased safety for utility workers and the public
- Enabling Hawaiian Telcom to focus on its core communications business while creating opportunities for Hawaiian Electric, Maui Electric and Hawaii Electric Light to control costs for all customers.

*"In the nearly 100 years since the first joint pole agreement, our businesses and maintenance practices have changed dramatically," said Alan Oshima, Hawaiian Electric president and CEO. "This new arrangement will help both companies as well as other stakeholders move safely and quickly in using the poles to deploy new equipment to provide services that will improve the lives of our customers."*

*"This modern agreement is a win for our companies and our state by streamlining the pole repair and management process and maximizing efficiency," said John Komeiji, Hawaiian Telcom president and general manager. "With this change, Hawaiian Telcom joins many other communications providers that lease space on poles, enabling us to channel more of our resources toward investment in fiber and expansion of next generation services statewide."*

Under the approved arrangement, Hawaiian Telcom transfers ownership interest in the jointly owned poles to the Hawaiian Electric Companies in exchange for \$48 million in credit against past and future charges for attaching to the poles.

On Oahu, the joint ownership arrangement dates back to 1922 when Hawaiian Electric, Mutual Telephone Co. and the Honolulu Rapid Transit Co., which operated electric streetcars, decided to share maintenance expenses and reduce the number of poles lining city streets.

Today, in addition to electric wires, phone lines and street lights, space on poles is rented by cable television and wireless carriers through sub-attachment agreements. The various individual agreements, combined with joint ownership, causes confusion and delays.

Now, the Hawaiian Electric Companies will be solely responsible for maintaining the poles and managing attachments. Along with other communications providers, Hawaiian Telcom will rent space on the poles through agreements with the Hawaiian Electric Companies and maintain its lines on the poles.

Hawaiian Telcom will retain its solely owned poles, as well as joint poles on Kauai that are not part of the agreement. The state and counties continue to retain joint ownership interest in utility poles with attached streetlights on Oahu and Hawaii islands. Hawaiian Electric is working with the respective governments to transfer this ownership as well to further this initiative.

**Approximate number of joint poles affected by this agreement:**

- Oahu -- 51,000
- Maui County -- 24,000
- Hawaii Island -- 46,000

In addition to the joint poles, the Hawaiian Electric Companies own 100 percent interest in 50,000 additional poles not affected by this agreement.

# This is the Simulator for grid modernization.

For over 20 years, the RTDS<sup>®</sup> Simulator has been the industry's de facto tool for the closed loop testing of protection and control systems. Today, RTDS Technologies continues to lead the way with innovative developments, ensuring real time simulation's applicability for the grid modernization practices that are critical for utilities, protection and control manufacturers, and research institutions around the world.

Our new generation of simulation hardware, NovaCell<sup>™</sup>, is bringing digital grid, distribution automation, and grid-edge connectivity to life in real time — from single units on the desks of utility change-makers to huge installations in the world's most prominent innovation centres.



the world standard for real time digital power system simulation

[www.rtds.com](http://www.rtds.com)



# EDF LAUNCHES THE FIRST FRENCH MICROGRID DEMONSTRATOR OPERATIONAL IN SINGAPORE

November 2018

EDF, Enedis and the Nanyang Technological University, Singapore (NTU Singapore) have launched the MASERA microgrid project (Microgrid for **A**ffordable and **S**ustainable **E**lectricity in **R**emote **A**reas), as part of the Singapore International Energy Week (SIEW) and the 2018 France-Singapore Year of Innovation. This demonstrator will allow EDF to deploy a commercial offer of affordable and high-performance microgrids for isolated territories in South-East Asia.

EDF's MASERA is part of NTU's offshore microgrid testbed known as REIDS (Renewable Energy Integration Demonstrator - Singapore). Located at Semakau landfill, NTU's REIDS is the region's first offshore microgrid testbed which integrates multiple renewable energy sources to develop solutions to tackle regional electricity issues.

On this platform, EDF, at the head of a consortium of French smart grids/smart cities companies, has designed, built and commissioned the MASERA demonstrator within one year, a record time for such a prototype, integrating various innovative solutions:

- 50kW of bifacial photovoltaic panels;
- A Lithium-Ion storage system provided by Socomec;
- An affordable and eco-friendly Zinc-Air battery from Zinium (EDF spin-off);
- A Nissan Leaf electric vehicle
- A V2G (Vehicle to Grid) software platform and bidirectional charging hardware from Nuvve Corporation;
- A load bank to reproduce typical customers' consumption;
- A 100 percent EDF local and remote microgrid control system allowing standardised communications and generation optimisation,
- A reliable and secure smart meter infrastructure with the expertise of Enedis.

In Singapore, EDF relied on the experience of local companies such as Aurecon, for the detailed technical design and Caxton, for the construction of the MASERA demonstrator.

The MASERA project is the demonstration of an industrial, innovative and easily deployable solution. It will allow EDF

to support economic development in South-East Asia and therefore improve the quality of life of communities.

This project illustrates EDF's drive and unique expertise in designing, developing and executing smart grid and microgrid projects on islands and territories with no access to the grid or facing reliability issues. In recent years, EDF has developed multiple innovative microgrid solutions including a 100 percent renewable energy system on La Réunion island, the Nice Grid demonstrator in Carros near Nice and hybrid microgrids in Toucan and Kaw in French Guiana. In the frame of these developments, EDF benefits from Concept Grid, the EDF R&D leading smart grid laboratory near Paris.

Microgrid solutions leveraging the potential of renewable energies offer development perspectives in South-East Asia, taking into account the geographies, the current lack of infrastructures and the economic growth of the major countries in the region.

Bernard Salha, Senior Executive Vice President (VP) of EDF Group, President of EDF Research and Development, declared, "I am happy to be celebrating the launch of the MASERA demonstrator. This project allows us to combine the expertise and knowledge of Enedis, of the Nanyang Technological University of Singapore, of companies from the French Think Smartgrids association, which federates the whole players of the Smart Grid ecosystem like Enedis, Socomec, Sagemcom and start-ups, and of the EDF Group in the domain of microgrids. Thanks to MASERA, EDF whose ambition is to become one of the world leaders in microgrids will improve its knowledge of local markets, reinforce its R&D and demonstrate the reliability of off-grid and microgrid solutions which can be developed in South-East Asia, which is at the heart of the Group's international strategy: renewable generation, energy efficiency, smart city".

Marianne Laigneau, EDF Group Senior Executive Vice President (VP) in charge of international division, declared, "the inauguration of MASERA illustrates both the technological know-how of EDF, its ability to match the specific demands of its customers and its willingness to develop its footprint in Asia which is at the heart of its international strategy".

THE PREMIER ELECTRICAL MAINTENANCE AND SAFETY CONFERENCE



# 2019 POWERTEST<sup>®</sup> CONFERENCE

## EARLY BIRD REGISTRATION

September 1 – December 31, 2018 **Register Early and Save**

Gaylord Texan Resort and Convention Center - Grapevine, Texas

Hosted by **NETA**<sup>®</sup>  
PowerTest.org | 888.300.6382

# WRAPPING UP 2018



**ELISABETH MONAGHAN**  
Editor in Chief

Welcome to the final issue of 2018. Throughout this past year, the team at *EET&D* had several meaningful discussions with industry influencers, which made our 20<sup>th</sup> Anniversary celebration that much better! To those readers who sent emails, texts and cards to congratulate us on this significant milestone, thank you.

Between events and meetings, we have benefitted from the insights and expertise of our industry partners, letting us know about any new topics they would like us to cover, along with those on which the magazine should continue to focus. This feedback is essential. If we are going to fulfill our mission to be the “go-to resource” for the latest on the transmission and distribution side of the global electric energy industry,” we must remain a conduit for open communication. That means we also must pay attention when someone provides negative feedback or points out gaps in our content. Such was the case with one of our articles in our September/October 2018 issue.

In response to the article titled “The Importance of 5G for Utilities,” Robert Landman with H&L Instruments emailed us to explain that while 5G may be heralded as a huge advancement in global connectivity, the vision is flawed. According to Landman, “It is flawed because users will not value the higher data rates that are promised and will not need the higher capacity forecast. It is flawed because technological advances are insufficient to realize the vision and because mobile operators are insufficiently profitable to afford it.” We appreciate it when readers like Mr. Landman take the time to weigh in. Going forward, we will continue to explore the topic of 5G and what the future holds for its emergence, along with the advancement of additional technology in the utility space.

Contributed content is one of the most valuable channels for the *EET&D* staff to share what is happening in the world of energy. Participating in user conferences and other events also allows us to meet those who are moving the power sector forward. In September, I attended a press tour hosted by Albuquerque, New Mexico-based Array Technologies. A solar tracking solutions and services provider for utility-scale projects, Array has been testing its bifacial technology with solar trackers. In addition to the manufacturing plant and one of their test sites, Array also took us to visit a local utility site that uses the company’s solar trackers.

One of the most rewarding learning experiences for me this year was sitting on the jury for the Bentley 2018 Year in Infrastructure Awards. In total, 57 finalists were selected from 420 nominations in 18 categories. My category was Advancements in Utilities Transmission and Distribution, where my fellow jurors and I narrowed down the top three finalists to the following:

- Northeast Electric Power Design Institute Co., Ltd. of China Power Engineering Consulting Group: New project of a 750 kV substation in the Bortala Mongol Autonomous Prefecture – Bortala Mongol, Xinjiang Uyghur, China
- Pestech International Berhad: Substation Design & Automation for Olak Lempit Substation Project – Banting, Selangor, Malaysia



# EXPLORING JAPAN'S ENERGY AND OTHER GLOBAL INDUSTRY TRENDS

*For this last Grid Transformation Forum of 2018, we spoke with Ben Cohen, director of global strategy with Autogrid. Cohen shares his insights on the energy market in Japan and other markets around the world where smart grid initiatives are transforming how electricity is produced and managed.*

**EET&D:** Ben, thanks so much for joining us for this discussion. There's a lot of ground to cover. Let's start with Japan where the energy market is going through a major transformation. What are you seeing there and what lessons does that have for the rest of the world?

**BC:** Thanks so much for having me. Yes, Japan is a fascinating place to start with because, in many ways, its energy market is very different from the rest of the world. And yet, there are important takeaways for everyone working on smart grid initiatives; regardless of whether you are in Philadelphia or Finland.

Japan is unique because it's one of the few places where changes in its energy market are not being driven entirely by deregulation. The typical scenario that has played out around the world is that deregulation occurs after a legislative or other governmental action to foster more competition. Then, the newly deregulated market is hit by a number of economic forces as companies compete fiercely and innovate fiercely, causing a re-shaping of how energy is produced and delivered.

But Japan is different and more nuanced. The catalyst for change in Japan isn't just regulatory in nature. It's incorporating a desire to really be at the cutting edge of technology and the development of a business case for energy generation and management at the household level. PV panels and residential battery storage for solar-

generated electricity collectively have such a significant return on investment that they have proliferated in Japan. Yes, they have a deregulated market, and yes, they have had government incentives for residential solar, but those ingredients exist elsewhere. The true driver for the hundreds of thousands of households in Japan that have residential solar is that it makes financial sense.

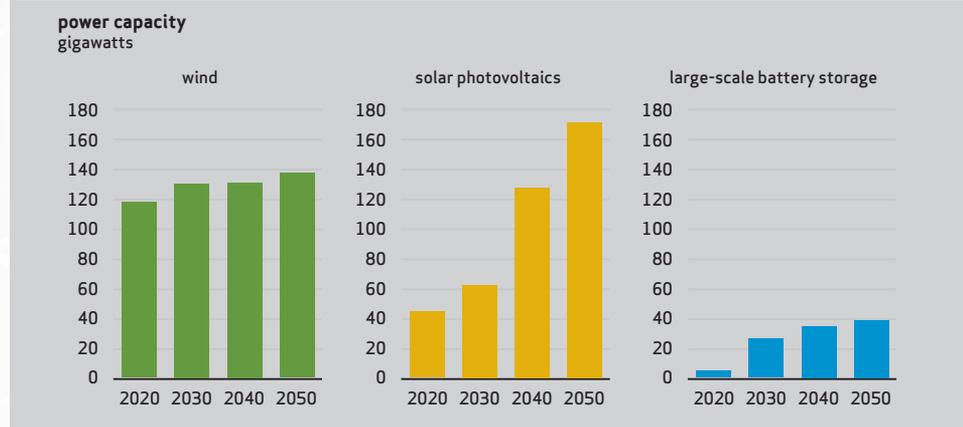
**EET&D:** That would be news to people who still have the mindset that PV solar systems aren't cost-effective.

**BC:** Exactly. There wasn't a giant parade and 90-point-font headlines in newspapers when the solar industry turned that corner, but we are there, and Japan is Exhibit A in many ways. The cost of residential solar and in-home battery systems have dropped to a point where the economics are no longer a question. Now, it's a matter of how you implement it at scale, hooking into the right value streams, and nailing down the customer value proposition as to packaging for the end consumer: who owns the assets, energy as a service, and all sorts of other flavors.

The latest research I saw from Bloomberg's New Energy team predicts 128 GW of small-scale PV generation in Japan over the next three decades. That is a staggering volume, and that's just one country. The financials don't lie. Solar systems linked to a residential battery can do very heavy lifting for a country's energy needs. →



## U.S. Large-Scale Wind, Solar, and Battery Storage Capacity Projections (2010–2050)



Source: U.S. Energy Information Administration, *Annual Energy Outlook 2018*

**EET&D:** We read that you will be working with an IT services firm on smart grid implementations to tie together these residential solar systems in Japan. What are the main challenges there and what can other utilities learn from your work there?

**BC:** Yes. The IT services firm at the forefront of this new energy market in Japan. They work with all of the major utilities in Japan, and we are providing the software and integration services that will enable these households to be linked together effectively.

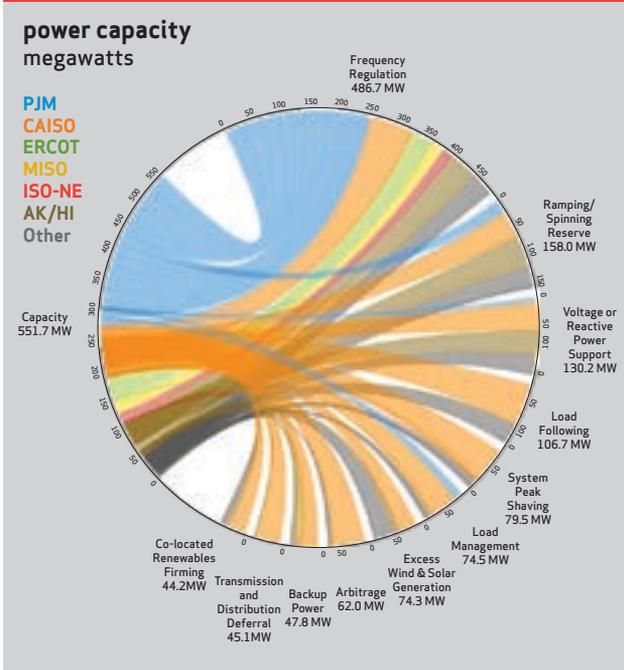
The critical part is not simply linking these households together with behind-the-meter technology that allows them to be both consumers and producers of energy. The key is to create a functioning marketplace, where energy is produced, bought, sold, traded in a way that is fluid and responsive to the market's needs over the course of an hour, a day, a month and a year. Our team is working on how to do that so that these networks work in the moment...and work during high-demand scenarios... and work in ways that show that distributed energy generation can begin replacing base loads. Coordinating all of that is what we specialize in, and our projects in Japan are exciting because we are making all of that happen at such a large scale. To me, the key lesson from what's happening in Japan is that the energy companies that are thinking about how to do all of that at scale and create a true distributed energy marketplace are the ones that will be best positioned to succeed.

**EET&D:** Let's hop across the Pacific Ocean to California. That state generated a lot of headlines recently with their goal of sourcing 100 percent of their energy from clean sources. Do you think that will be a "critical mass" moment for renewable energy that will spur growth of a distributed solar energy generation similar to what you just talked about in Japan?

**BC:** That's a great question. Actually, I might be a bit contrarian on this topic. Don't get me wrong. I think the state's decision to do this is a milestone... but I don't think it's going to be a catalyst because I think the catalysts were already in place for states like California to move to a 100 percent clean energy model.

That doesn't lessen the significance of California's announcement. I just take a different view of the causality. That announcement by California is a recognition of the direction that we are already heading because the combination of low-cost PC, affordable residential battery storage and a deregulated market make this model a realistic goal at scale. We were already there. But California's announcement puts a spotlight on that reality in a way that is important because it marks a key moment in the evolution of the energy industry.

## U.S. Large-Scale Battery Storage Capacity and Applications Served (2016)



**Note:** The figure does not include a 10 MW/7.5 MWh battery storage unit located in Maui, Hawaii, which did not report any applications in 2016.

**Source:** U.S. Energy Information Administration, Form EIA-860, *Annual Electric Generator Report*

**EET&D:** California already has a diversified power generation model that relies on a significant volume of renewable sources. Do you think there's a significant role for distributed residential solar to play as it has in Japan?

**BC:** Definitely, and the exciting thing is that it's already happening. We are working with a leading energy storage

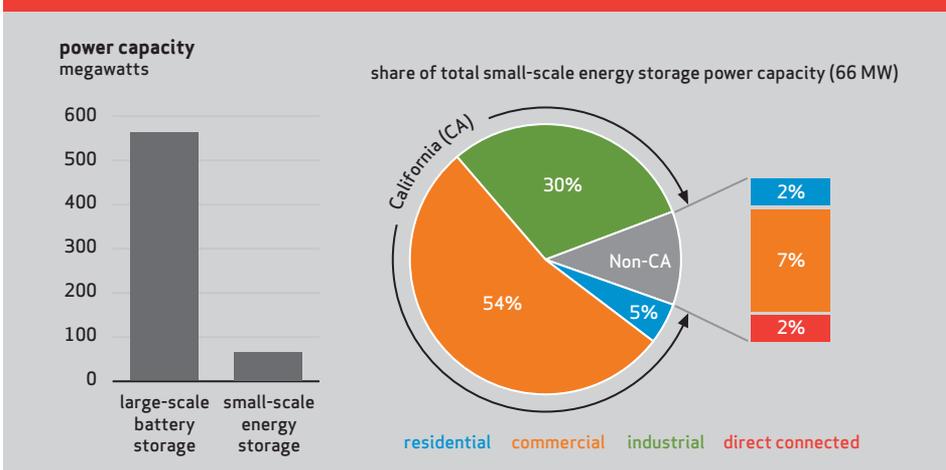
provider on a distributed solar initiative that assembles thousands of households in Southern California into a virtual power plant, which allows the state to respond to high-demand situations. It's just in its infancy, and it's already capable of harnessing nearly 40 MW of power. That will be much larger in the very near future. The model works, and it's simply a matter of having the right combination of consumer education, utility rollout strategy and supporting incentives to go bigger.

I love that you started with Japan and California, because on the surface these are two dramatically different energy markets in terms of the structure and underlying dynamics, and yet both tell the same story: that distributed energy is already working at scale in both places, and both markets will make a major leap forward in the scale of that with the right technology to tie all of it together.

**EET&D:** Those are both examples of forward progress, but let's talk about what's standing in the way of a faster evolution of other energy markets. Not every market is as progressive on these issues as Japan and California. What are some obstacles that still need to be addressed?

**BC:** So many of the past obstacles have been cleared out of the way. PV is at a price point where the economics of residential solar are undeniable. And residential batteries are being produced on a scale that solves the previous bottleneck, plus there are proven financial models for how to make them affordable to consumers so that it's built into the model for how they are paid for the energy they produce. And you're seeing governments and regulatory agencies embracing this trend as a way to achieve sustainability goals and energy independence directives. Those hurdles are already cleared or in the process of being cleared, which is remarkable compared to where we were a decade ago. →

## U.S. Small-Scale Energy Storage Capacity by Sector (2016)



**Note:** Data collected on small-scale storage may include forms of energy storage other than batteries. Direct-connected storage is not located at an ultimate customer's site but are in front of the meter and/or connected directly to a distribution system.

**Source:** U.S. Energy Information Administration, Form EIA-861, *Annual Electric Power Industry Report*

But there are some remaining obstacles, and I don't want to minimize them. These have to do with the mindset of utilities and consumers, for whom this is a major change in the model for how energy is produced and consumed.

Let's start with consumers because in many ways this is the easier of the two obstacles to overcome. Households see themselves as consumers of energy. They use a certain number of kilowatt hours of electricity and a certain volume of natural gas, and they pay those bills, and then they repeat that process the following month. It's a major shift for them to get their heads around being an energy producer, but to be honest, I'm not worried about that obstacle. Consumers are practical, and when their utility makes it clear they can make money every month with a PV-plus-battery implementation rather than writing a check to the utility every month, they won't be confused for long. Yes, it's a major shift in how they think about energy, but money talks.

The harder mindset transition will be with some utilities, I think.

**EET&D: How so?**

**BC:** I don't want to paint with too broad a brush, because there are so many utilities that are forward-thinking and doing really innovative work that is a win-win for consumers and for their organization. But some utilities are playing catch-up, and you can hear it in the language they use. When you still refer to customers as "ratepayers," that's a clear sign that you are thinking about the energy marketplace in the old way rather than with a mindset that sees households as partners in an integrated network of power generation and power consumption.

I know that's a semantic issue, but it reflects a larger mindset. And my experience is that the companies that speak with that language are the ones who are moving slowest to understand the new energy model and position themselves to be competitive against other energy providers who are several steps ahead.

**EET&D: That's a major shift for organizations that have been in an industry that changed very little for decades before the wave of deregulation.**

**BC:** I agree, but the bottom line is that companies that keep thinking that way are going to have a hard time catching up as the market continues to evolve. When I talk to utilities, I avoid making this an all-or-nothing proposition. They don't need to design these as massive projects to begin reaping major benefits. One thing I always make a point of saying is that you don't need a million customers right out of the chute in order to move forward. For reasons I completely understand, utilities are conditioned to think of their user base either in total or as large segments. But projects like

the one we are doing with the energy storage provider in California is a great example of how you can solve specific problems as a utility with a highly-defined new energy project.

One of the thorniest problems for utilities to solve is demand-response events where there are spikes that cannot be met by the core power generation infrastructure in place. Very smart people have wrestled with that challenge for decades using the toolkit they had in place, but distributed energy like residential solar gives them a new tool. And it's a powerful one. For even the most conservatively-inclined utilities who still use the "ratepayer" language, this is often the best way to get started with the distributed energy model. You don't need a million customers involved. A few thousand can give you more than enough energy to take the edge off of demand-response events. And there are proven models for how to roll this out, how to make it work financially for consumers, and how to manage all of that with software that creates this bi-directional marketplace.

**EET&D: You're talking about demand-response situations, but what about replacing base power generation with this kind of distributed model. How far off are we from that?**

**BC:** It will happen. When the marginal cost of a kilowatt hour of power from a PV system is zero, there's no reason why residential solar can't begin replacing base power generation needs at some point soon. It's not a technology issue. It's not an integration issue. And it's not a financial model issue. It's just a matter of time.

The key for many utilities is not to replace 100 percent of their base power generation, though. In the same way that bridges are designed to handle 200 percent or 300 percent of capacity, utilities would want to have well more than 100 percent of base power generation before they would feel comfortable shifting their base power load away from coal-powered plants and natural-gas-powered plants to distributed energy. That's on the horizon, but in the meantime, these smart grid implementations provide an effective solution for one of the pain points that utilities have struggled with forever. To me, that's where these initiatives prove their initial worth for a lot of organizations, and then it can grow in scope from there.

**EET&D: Before we wrap up, what are you and your team seeing in other parts of the world? And do you see a willingness to embrace these models there?**

**BC:** One of the best parts of my job is working with people in parts of the globe that you don't traditionally associate with the cutting edge of technology, but that's exactly what I'm seeing in places like Africa and South America and underdeveloped areas of Asia.

It's a bit ironic, I guess, but the countries with the most advanced traditional power grids have often been the most risk-averse when it comes to these models. They have systems that work, and they are conservative about trying new things that may represent a risk in their mind. But there are lots of places on the globe where power delivery infrastructure has traditionally been unreliable, and to them, these distributed energy models managed by smart grids aren't a risk. It's a chance to make a major leap forward in reliable, flexible energy infrastructure.

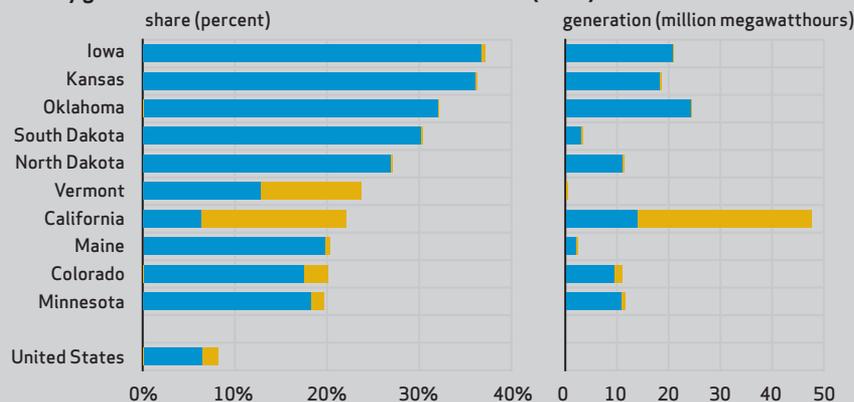
India is a great example of this. The country has traditionally had a weak grid system, so the energy industry there (in collaboration with governmental agencies) have taken much more of a "blank page" approach that re-thinks energy production and distribution. These distributed models – where households are not just consumers of energy but collaborative producers of energy – are more cost-effective to implement than traditional infrastructure. And faster. And easier to manage, with the right systems and software in place. The same is true in areas of South America, Central America, Africa and Asia where power infrastructure has been less-than-reliable for decades.

This isn't just exciting stuff from a technical point of view. It's life-changing for the people who live there and who run businesses there. For us, in the most developed nations, all of this energy stuff is primarily a business story about which companies are winning and how many rooftops have PV panels. But for so many parts of the world, this is so much more than that. This is a chance for companies to create more jobs in impoverished areas, for parents to make enough money to send their kids to school, and for kids to do their homework under working lights at night. I'm so proud to be a part of helping that happen. Everyone in our industry should feel the same way because what we are doing is proliferating around the world in a way that is making the world a better, more equitable place.

**EET&D: That's an important perspective, Ben. Our industry is a truly global one, and it's about much more than just electricity. Thanks for sharing your insights with us, and safe travels as you criss-cross the globe working on these exciting projects.**

### Combined wind and solar made up at least 20% of electric generation in 10 states in 2017

Electricity generated from wind and solar in selected states (2017)



Source: U.S. Energy Information Administration, Electric Power Monthly

#### ABOUT BEN COHEN:

**Ben Cohen** is the director of global strategy at AutoGrid, which provides flexibility management software used globally by utilities, electricity retailers, renewable energy project developers and energy service providers to deliver clean, affordable and reliable energy by managing networked distributed energy resources (DERs) in real time and at scale. Cohen earned his undergraduate degree at Stanford and his MBA at Harvard.



# WINDS OF CHANGE: HOW ARTIFICIAL INTELLIGENCE AND OTHER EMERGING TECHNOLOGIES ARE REVOLUTIONIZING THE WIND POWER INDUSTRY





### **DR. YAN KE**

The wind energy industry is growing rapidly. In the U.S. alone, the wind industry invested more than \$11 billion in new plants in 2017 and added more than 7,000 megawatts of new capacity, representing a full 25 percent of all electric capacity additions across the energy industry last year. Today, wind energy contributes more than six percent of the nation's electricity supply, more than 10 percent of total electricity generation in fourteen states, and more than 30 percent in four of those states. However, as with other renewable energies, the wind power industry still faces many obstacles. One of the biggest challenges to growth remains the high costs of constructing wind farms, as well as the ongoing operations and maintenance costs. The industry also still relies heavily on government subsidies and federal tax incentives, which can be unreliable and phased out, depending on whichever way the "winds" of the current political climate are blowing.

To further its growth, reduce costs and increase profitability, the wind power industry is increasingly turning to emerging technologies such as artificial intelligence (AI), machine learning (ML), edge computing and Internet of Things (IoT) sensors and devices, such as autonomous drones. These technologies are being combined in new and innovative ways to help wind farms automate costly and time-intensive operational tasks such as turbine inspections and are delivering real-time data insights to help wind farms lower operational costs and improve efficiency for greater profitability. →

## Challenges Facing the Wind Power Industry

The need to lower operations and maintenance (O&M) costs remains a persistent challenge in the wind power industry, especially as turbines age. According to analysts, O&M costs average between \$42,000 and \$48,000 per megawatt during the first 10 years of a turbine's operations, and wind farm owners are expected to spend more than \$40 billion on O&M over the next 10 years.



**The tip of an average wind turbine blade rotates at a speed of 300 km per hour (more than 180 miles per hour). That's the speed of a bullet train, running 24 hours a day while exposed to the harsh conditions of driving wind, rain, hail, dirt and ther particles.**



One reason O&M costs remain high is due to the conditions in which wind turbines operate. The tip of an average wind turbine blade rotates at a speed of 300 km per hour (more than 180 miles per hour). That's the speed of a bullet train, running 24 hours a day while exposed to the harsh conditions of driving wind, rain, hail, dirt and other particles. Faced with this environment, turbine blades degrade rapidly, which can reduce a wind farm's output by 12 percent over a 20-year lifetime and increase the cost of electricity by nine percent. It's no wonder that lowering O&M costs is top of mind for every wind farm owner and operator. Fortunately, new digital technologies can help wind farms lower these costs while boosting performance, increasing operational efficiency and extending the life of turbines. Here are just a few examples:

### "Talking" Turbines Powered by IoT

Today's wind turbines are increasingly equipped with hundreds of IoT-connected sensors, enabling them to "talk" to wind farm operators and provide greater visibility into operations. These sensors can continually measure every aspect of wind turbine operations such as acceleration, temperature, vibration, environmental conditions, sounds that could indicate a problem with the turbine and more. AI and data analysis are applied to sensor data to identify problems and suggest actions that can improve performance and increase productivity. For example, to produce the most electricity, turbines need to be turned

toward the wind, but it takes a significant amount of time and energy to turn the direction of the blades. By using AI and advanced algorithms, operators can better predict wind intensity, direction and angle, in order to turn blades in advance of changes in weather conditions. One turbine manufacturer in China has been able to help its customers boost energy production by 15 percent by using turbine sensor data to optimize the angle and speed of their blades based on environmental conditions.

With the growing prevalence of IoT sensors and data, wind farms are beginning to build networks where they can monitor nearly every aspect of operations in order to increase energy production and better manage the condition of equipment over its lifetime. However, one area where many still struggle to gain significant improvements has been in the time- and labor-intensive task of visual turbine inspections – but that is beginning to change.

### Automating Visual Inspections with Drones and AI

Though many turbines today are equipped with a variety of IoT sensors measuring vibrations, sounds and more, wind farm operators still need greater – and earlier – visibility into the condition of blades. For instance, by the time a turbine has degraded to the point where it is vibrating or creating an unusual noise, the damage is already severe. Regular visual inspections of blades are needed to identify cracks or other blade damage that can be fixed with a simple patch while still small. However, if an operator is not alerted to a problem until the blade is vibrating or whistling, they will likely need to shut down the turbine and replace the entire blade. This can cost the operation hundreds of thousands of dollars, as they will need to purchase new blades, bring in heavy equipment to hoist them up, and spend many labor hours installing them – not to mention the cost of downtime as the turbine may be turned off and not producing electricity for weeks or months as they wait for the new blades arrive and be installed. Clearly, having greater visibility into blade conditions in order to minimize the need for repairs and downtime is a highly-sought after advantage that can save wind farms a tremendous amount of time and money.

This is where emerging technologies such as autonomous drones equipped with AI, ML and advanced computer vision are making a dramatic impact. Traditionally, visual inspections required shutting down a turbine and, sending one or more highly trained technicians up the tower, on ropes, to inspect the blades. A typical inspection could take six to eight hours per turbine. However, by using autonomous drones for visual inspections, wind farm operators can complete turbine inspections in as little as 15 minutes.



A typical inspection could take six to eight hours per turbine. However, by using autonomous drones for visual inspections, wind farm operators can complete turbine inspections in as little as 15 minutes.



With essentially the click of a button, the autonomous drone can fly itself up the turbine, conduct a detailed, visual inspection and then land itself without the need for a human pilot. Wind farms first began experimenting with using drones for inspections several years ago, but those had to be manually piloted and required two highly trained operators: one to fly the drone without colliding into the turbine and the other to take photos of the blades. With today's autonomous drones, only one operator is required, and that person needs only minimal training. The drone launches itself and, using built-in sensors and AI, closely tracks a precise path along each blade. Precision photography and advanced computer vision are used to identify automatically and flag defects such as hairline cracks or chips as small as one millimeter by three millimeters – better than the human eye can. In fact, autonomous drones are so precise, they have even been known to photograph and identify a common fly resting on a blade during an inspection! Built-in machine learning automatically stitches together thousands of photographs to give operators a holistic view of the entire blade.

By reducing the inspection process from days to minutes, wind farms no longer need to have their turbines powered-down and not generating electricity for prolonged periods of time. They're also able to dramatically reduce the amount of labor involved, both of which help the farms reap tremendous cost savings. Those are just the beginning of the benefits. By leveraging AI and ML, such autonomous drone solutions can analyze huge volumes of data in the cloud, almost instantaneously, and deliver real-time insights that can help wind farms identify trends and make decisions to improve operational performance. Recent advances in edge computing are enabling this type of real-time data analysis. Because wind farms are often located in extremely remote locations, transferring data from turbine sensors to a centralized location not only takes time but is also limited by lack of bandwidth to these areas. With real-time data analysis at the edge, wind farm operators can make critical decisions faster, such as shutting down a turbine to avoid cascading damage. Moreover, with cloud-based reporting, they can easily



track the entire lifecycle of turbines, see the progression of damage and view trend reports on individual turbines or their entire fleet.

Using autonomous drones for visual inspections have demonstrated promise such that analysts estimate the market to grow at a compound annual growth rate (CAGR) of 12.93 percent during the period 2017 – 2021 as more and more farms start adopting this technology.

### Predictive Maintenance

In addition to using AI, IoT and data analytics to identify necessary repairs and existing blade damage on turbines, some wind farms are beginning to go a step further and use these technologies to predict when faults will occur and schedule maintenance before it's needed. As mentioned earlier, the longer a wind farm waits to fix a problem, the costlier it becomes as turbines need to be powered-down and are not producing electricity. With the real-time data from visual inspections and turbine sensors, wind farm operators can understand the growth rate of defects and determine if component failure is imminent, or if repairs can wait for a more opportune time. Predictive and preventative maintenance allows operators to save time and money by scheduling maintenance in advance, avoiding long downtimes and scheduling repairs for times of year when the weather conditions are best. →

## What to Consider When Exploring Emerging Technologies

The wind power industry is only just beginning to explore the possibilities provided by AI, ML, IoT, autonomous drones, edge computing and other emerging technologies. As with any new technology, there are considerations to keep in mind before diving in. For example, if considering adopting new technologies to automate inspections or enable predictive maintenance, I recommend wind farms use a service model rather than investing in the drones or other hardware themselves. When evaluating service providers, consider the speed at which they are able to perform inspections, as this will affect turbine downtime and, therefore, loss of revenue. You should also consider the accuracy and completeness of inspections and defect reports, which can vary widely depending upon the technological capabilities of the provider and their solution.

Perhaps most important, however, is the need to consider how these technologies can impact the culture of an organization and be perceived by workers. Assure your workforce that AI is not to be feared, and that it's not going to replace your valuable employees. Rather, AI assists people, helping make their jobs easier and safer to perform. Instead of requiring technicians to climb up dangerously high turbines, which can result in accidents and injuries, wind farms can now use drones to take blade photos and utilize their human employees to perform the higher-level thinking – determining the best course of action based on the data provided. Ultimately, AI and other emerging technologies result in higher-skilled jobs for employees, wage increases and safety improvements.

As new digital technologies continue to proliferate, we are beginning to see the many ways they can be used to transform the global wind power industry and drive further growth. From reducing downtime and extending the life of turbines, to improving energy production and increasing productivity, artificial intelligence and other emerging technologies are helping create a smarter and more sustainable energy sector.

### ABOUT THE AUTHOR:

**Dr. Yan Ke** is the co-founder and CTO of Clobotics, a global leader in intelligent computer vision solutions for the wind power and retail industries. Prior to co-founding Clobotics, Ke was the chief software development officer of EHang, Inc., a technological innovation company specializing in R&D, manufacturing and sales of intelligent aerial vehicles. He hired, led and developed a group of more than 50 developers, testers, and product managers on the R&D of its drone flight control, mobile and PC apps, and server and cloud services. Dr. Ke is an expert in data mining, machine learning, computer vision, and distributed systems. He previously spent eight years at Microsoft leading the Bing Entity Understanding Group.

Ke has a Bachelor's in computer science, a Master's in electrical and computer engineering, and a Ph.D. in computer science, all from Carnegie Mellon University. His Ph.D. thesis topic was on using computer vision to recognize automatically human actions in videos. He is a recipient of the Intel Research Scholar Award, NSF IGERT Fellowship, Microsoft Technical Leadership Award, multiple Microsoft Gold Star Awards, published over 18 top tier conference and journal papers, and holds seven U.S. patents.



# THE ROLE OF CABLE REJUVENATION

## IN ADDRESSING THE MAINTENANCE OF AGING UNDERGROUND CABLES

GLEN J. BERTINI

Medium voltage underground cable is designed to be used and not seen. Pad mount electrical transformer boxes containing and connected by underground residential distribution (URD) cables are a ubiquitous sight throughout residential neighborhoods, spaced, on average, 330 feet apart. Consumers who live in the community are generally unaware of the jumble of cables that each box comprises, and they rarely need to consider whether the URD itself is in an adequate state of repair. Most utility providers, on the other hand, are in a constant state of responding to aging cable and the threats it represents.

Over time, utility companies face significant challenges for addressing deteriorating URD conditions. URD cables are most commonly degraded when moisture diffuses into the cable's dielectric layer, gradually diminishing the cable's insulative properties. This condition, called "water treeing" because of the tree-shaped structure observed when the degraded cable is viewed microscopically, is the most common contributor to URD reliability issues. When the insulation on the cable connecting two transformers degrades to the point of failure, the lights go out in the entire neighborhood.

Aging URD cables are a growing problem in communities around the world, disrupting customers and causing business challenges for utility providers. But in most cases, the traditional remedy for URD cable failure – taking the impacted cable out of service and putting new cable in its place – has proven to be unfeasible. When cables fail, the resulting outages and the replacement work required to restore power create logistical problems that are usually unpredictable and expensive – costs that must be absorbed by the provider, the customer or both.

Meanwhile, customers often experience multiple outages as the providers install new cable, often disrupting the customers' property and landscaping in the process.

### **Cable Rejuvenation: The Modern Go-to Option for Upgrading URD Cable**

When rehabilitating aging URD infrastructure, many utility providers forgo cable replacement and opt for rejuvenation as the proven superior method for fixing damaged cable. With cable rejuvenation, the affected cables are left undisturbed and injected with compounds that restore each cable's dielectric strength, effectively adding the same value as a new cable but without the burden of time, cost, environmental disruption and consumer downtime associated with cable replacement. This method was first developed in 1986, and its use has steadily gained adoption and popularity in the 30 years since.

Rejuvenation technology focuses on the injection of silane-based fluid into the strands of aging medium-voltage power cables. The fluid is injected by accessing cables through transformers or other cable termination points. Technicians typically open two adjacent transformers and de-energize cables in a way that generally does not impact power to customers. Then, specialty fittings are attached to each end of the cable to allow for fluid injection. As the fluid moves through the cable, it migrates into the conductor shield and insulation. The chemistry and the physics of the insulation are modified, and the result is a cable that is returned to full dielectric strength in as little as seven days. →





The use of cable injection is approved for capitalization by the Federal Energy Regulatory Commission, and hence, does not impact tight operation and management budgets.

#### Sustained vs. Unsustained Pressure

Engineers have developed a variety of injection fluids and techniques over the years, enabling technicians to deploy specific processes depending on a given cable type, circumstance or environment. The technology is also easily adaptable to different cable configurations, including splices in the cable. In these cases, technicians

create splice excavation pits measuring roughly six feet square and four feet deep. These pits have far less impact on landscaping than the trenching or tunneling typically required for cable replacement.



In these cases, technicians create splice excavation pits measuring roughly six feet square and four feet deep. These pits have far less impact on landscaping than the trenching or tunneling typically required for cable replacement.



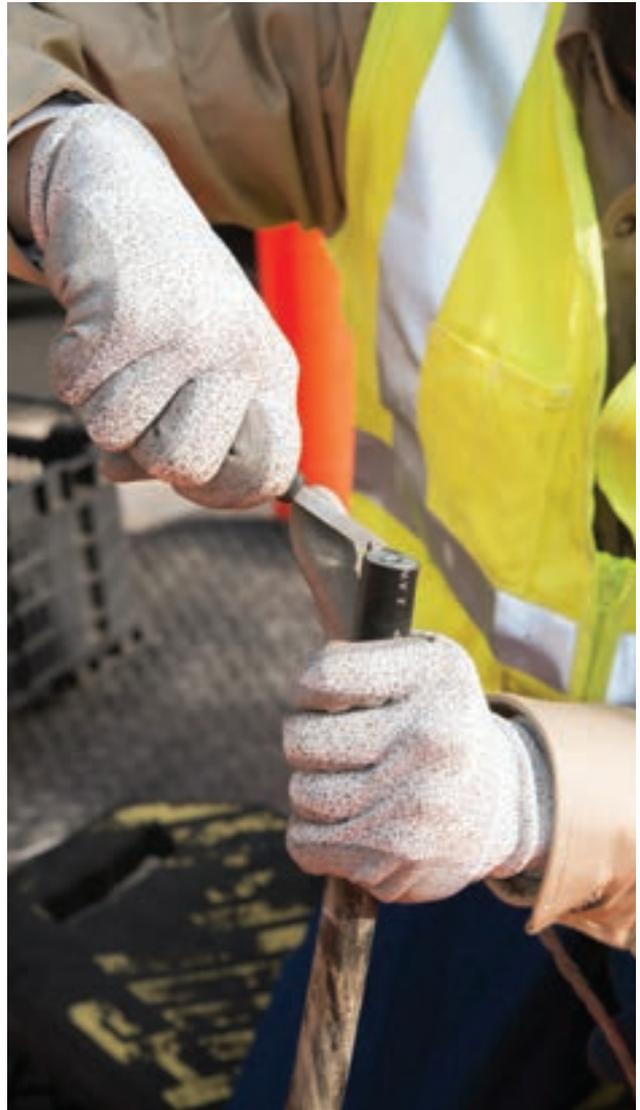
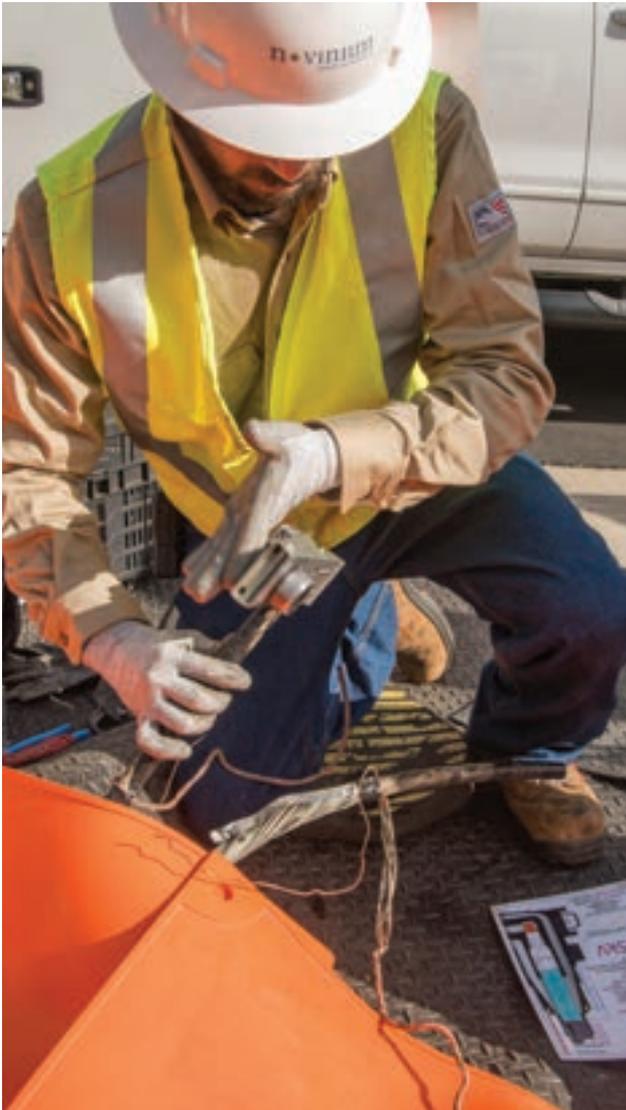
With sustained pressure rejuvenation (SPR), cables are restored to full dielectric strength in seven days, and injection can be completed in a single day. The steps are as follows:

1. Isolate, test and ground the damaged cable.
2. Using a time-domain reflectometer (TDR) device, check each segment for splices, neutral corrosion and overall length. If splices are present, technicians pinpoint their locations using a radio frequency locator and measuring wheel, then dig a pit to expose the splices and replace them with new splice connectors and injection adapters, using templates to ensure proper injection adapter placement.

3. Inject each segment at a moderate pressure. A 300-foot segment (100 meters) typically takes 30 minutes or less to inject. Following injection, technicians remove all equipment and install standard elbows at each end of the cable.
4. Re-energize the rejuvenated segment of cable, and then move on to the next segment.

Technicians typically apply the *improved* unsustained pressure rejuvenation (iUPR) process in areas that are difficult to access or cost prohibitive to replace. This process uses low pressure, so fluid can flow through splices while the circuit is energized. The steps are as follows:

1. Isolate, test and ground the damaged cable.
2. Using a TDR device, check each segment for splices, neutral corrosion and overall length.
3. Perform air flow testing to confirm the rejuvenation fluid will flow properly.
4. Install new connectors and injection elbows.
5. Connect a feed tank to the injection elbow at one end of the cable and a vacuum tank at the other.
6. Re-energize the cable segment, and with the transformer closed, begin the injection process. →



With iUPR, injection typically takes 24 hours or less to complete. The following day, technicians remove all equipment. Except for the initial installation of the injection components at the terminations, the cable remains energized throughout the process.

### Benefits of Rejuvenation

- **Cost Savings.** On average, a rejuvenation program yields a 40 percent savings over abandon-and-replace programs. For utilities facing ever-increasing cable maintenance and management demand, rejuvenation helps address and repair more miles of cable for the same budget, compared to replacement.
- **Ecological Impact** Cable rejuvenation reduces new pollution; no resources are consumed to produce new cable; no diesel fuel is spent on installation, and the environment benefits when cables are not abandoned in the ground. For a 10-mile run of a typical 15kV 1/0' cable, cable rejuvenation mitigates approximately

184 metric tons of CO<sub>2</sub> equivalent. This equates to CO<sub>2</sub> emissions of 201,313 lbs of coal burned, or 27.6 homes' electricity use for 1 year.<sup>1</sup>

- **Fewer Outages** Because utilities can perform rejuvenation proactively rather than waiting for an emergency, there are fewer occasions when customers will be without power. Even during injection, customers experience a relative continuity of service, as opposed to tolerating planned outages as required for replacement.
- **Low Failure Rate** In the past 30 years, more than 150 million feet of cable have been rejuvenated, and more than 300 utilities on five continents across the globe have used cable rejuvenation. In that time, the overall post-injection failure rate is less than 3.5 percent.

With these benefits all in mind, utilities are best served to consider rejuvenation first when developing reliability programs for the URD cable they manage.



---

Cable rejuvenation reduces new pollution; no resources are consumed to produce new cable; no diesel fuel is spent on installation, and the environment benefits when cables are not abandoned in the ground.





#### ABOUT THE AUTHOR:

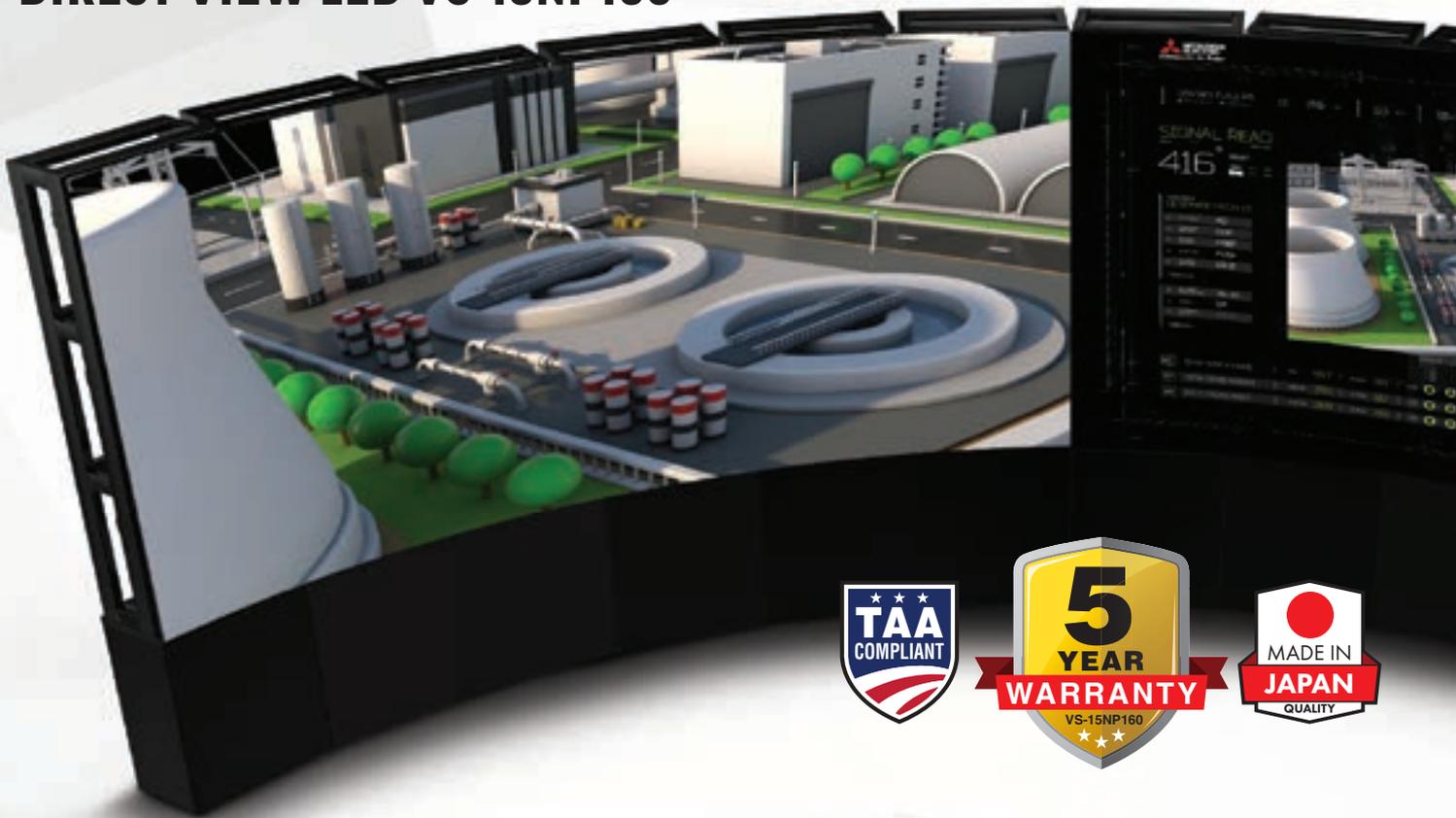
**Novinium CEO Glen J. Bertini** has more than two decades of working with cable-rejuvenation technology beginning with its development at Dow Corning in 1986. He has published more than 45 articles and 31 patents on cable rejuvenation and related technologies. Bertini was the 1992 co-recipient of the prestigious R&D 100 award for cable rejuvenation and the 2006 winner of the \$100,000 Zino Zillionaire Investment Forum award for the best investment opportunity in the Pacific Northwest. In 2010, he won the Puget Sound Engineering Council's Industry Engineer of the Year award as well as Seattle Business Magazine's Top Innovators award. Bertini is a senior member of the American Institute of Chemical Engineering (AIChE), an Institute of Electrical and Electronics Engineers (IEEE) fellow, a voting member of the Insulated Conductors Committee (ICC) and a licensed professional engineer. He received a Bachelor of Science in chemical engineering from Michigan Technological University.



<sup>1</sup> <https://www.epa.gov/energy/greenhouse-gas-equivalencies-calculator>

# THE FUTURE OF

## DIRECT VIEW LED VS-15NP160



**THE MITSUBISHI ELECTRIC DIRECT VIEW LED IS A HD INDOOR EXCLUSIVE LED DISPLAY CREATING A SEAMLESS DISPLAY WALL WITH A WIDE VIEWING ANGLE IN CRYSTAL-CLEAR**

Outstanding performance, intelligent patented features and low power consumption make the VS-15NP160 the ideal solution in the professional control room market.

The stunning performance of Mitsubishi's direct view LED makes it the perfect choice for large scale control rooms or areas where high ambient light is a challenge. Specially designed 3-in-1 SMD (RGB) LED packages

deliver up to 800 cd/m<sup>2</sup> brightness and a 100,000 hour lifespan which makes for a long lifespan and total return on investment.

**Designed and made in Japan**  
**24/7 command and control room projects.**

\*Images shown are for illustration purposes only.

[www.mitsubishi-displaywall.com](http://www.mitsubishi-displaywall.com)

TOLL FREE 888.307.0309

[www.mitsubishielectric.ca](http://www.mitsubishielectric.ca)

PHONE 905.475.7728

## UPGRADE YOUR VIDEO

# TECHNOLOGY.



**WITH A 1.5MM NARROW PIXEL PITCH,  
CLARITY AND SHARP DETAIL.**

High brightness with excellent contrast and 100,000 hours of life make it perfectly suited to control room roles where reliability are critical requirements.

Designed to meet the highest standards demanded by mission-critical applications. Perfect for all your government and industrial control room applications.

## MITSUBISHI ELECTRIC ORIGINAL TECHNOLOGY FEATURES:

### NATURAL COLOR MATRIX

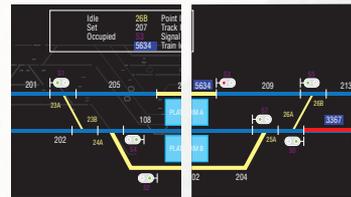


Before

After

Natural Color Matrix system enhances picture quality to achieve an exceptionally wide color reproduction range by controlling red-green-blue and also cyan-yellow-magenta.

### ANTI-BURN-IN



Burn-In Effect

w/ Anti-Burn-In Compensation

The Anti-Burn-In feature prevents variations in luminance and chromacity where static graphics are displayed for long periods of time, extending the LEDs operational lifetime.

### INTELLIGENT POWER CONTROL



Active power peak saving function detects image brightness and adjusts the power output accordingly to optimize power consumption and reduce operator eye-fatigue.

### DYNAMIC GAMMA W/ 2-DIMENSIONAL NOISE REDUCTION



Before

After

Dynamic Gamma Management improves the contrast ratio in darker images with a patented 2-Dimensional Noise Reduction system to help lower visible noise in compressed videos.

**DISPLAY WALLS TODAY!**

**MITSUBISHI  
ELECTRIC**  
*Changes for the Better*

# SMART GRID WIRELESS COMMUNICATION:

## WHAT UTILITIES NEED TO KNOW

RANDOLPH WHEATLEY

In a rapidly evolving utility landscape, advanced metering infrastructure (AMI) has emerged as an attractive solution for organizations seeking to enhance connectivity and transform their infrastructure into smart infrastructure.

As AMI adoption has accelerated, electric service providers have a choice of networks to power their smart grid communications:

1. Privately licensed spectrum signals carried over a point-to-multipoint network architecture
2. Publicly available spectrum signals carried over a mesh network architecture

The two approaches differ in architecture and signal type and offer distinct benefits and features for utilities. When selecting and designing a wireless communication network, utilities must compare, contrast and evaluate the two approaches as they relate to their unique challenges and needs. Conducting a thorough examination of architectural impacts, signal attributes, business and regional challenges, as well as other factors impacting wireless utility communications, will help utilities make smart choices when investing in AMI.

In this article, we examine the distinction between point-to-multipoint and mesh networks.

### Point-to-multipoint vs. Mesh: Key Differences

While mesh and point-to-multipoint networks both offer advantages for utilities, key differences exist that point to distinct advantages.

### Architectural approaches

Mesh and point-to-multipoint are two distinct architectural approaches to two-way radio communication networks. In a mesh network, many radios (also referred to as endpoints) can talk to each other, peer-to-peer. Each point on the network can receive, store and transmit signals to other points in many directions. In a point-to-multipoint network, there is a “master/hand” relationship in which a single point can talk to all the other points individually, and they can talk back to it—but not to each other.

### Privacy

All mesh networks use unlicensed spectrum for their communications channel. They operate on public, not private channels. Often referred to as the industrial, scientific and medical (ISM) frequency band, this spectrum is shared with a wide range of devices including cordless telephones, baby monitors and wireless Internet access modems.

Licensed spectrum networks are private. Government regulators lease or sell use of an assigned bandwidth range which may only be used by a specific licensed user in a particular region. Interference is not tolerated within that region and is protected by government agency enforcement. →



## Interference

Unlicensed mesh networks often have a high noise floor. A noise floor is like people talking during a movie; due to the number of voices being heard, understanding what's being said during the movie becomes more difficult. When industrial, institutional and medical devices are all sharing spectrum, the noise floor is high. With more devices "talking" above, below and even on the same operating frequency, utilities that deploy a mesh system architecture face challenges in the signal-to-noise ratio, which leads to inferior throughput and reliability.

Licensed spectrum systems have a naturally low noise floor, maintaining excellent signal-to-noise ratios even across longer distances and in the presence of signals on nearby bands. And, like an open highway, signal traffic can move swiftly and travel further than when plagued by congestion. Licensed spectrum allows data to be transferred to and from the meter quickly and reliably.

## Range

Unlicensed mesh networks, being public, are prohibited from generating more than one watt of output; which makes the signal range limited. Even if they could transmit further, they would suffer poor signal-to-noise ratios across longer distances. For these reasons, mesh networks require many points close together and move signals across a larger area through a series of short-range transmissions to intermediate nodes.

Licensed spectrum systems enable utilities to use higher power levels to optimize performance. Because of this flexibility, licensed spectrum networks are virtually interference-free and untroubled by crowded channels, as opposed to mesh networks whose power allotment largely relegates architecture to line-of-sight coverage only. Licensed spectrum signals routinely reach many times the distance of mesh signals.

## Bandwidth requirements

Unlicensed mesh networks use a lot of bandwidth for each transmission because the data "hops" from node to node and requires a new slice of spectrum for each step. As such, the cumulative sum of bandwidth for sending a signal from its source to a final endpoint can really add up.

Licensed spectrum systems can work with a narrower band; however private spectrum is not as abundant as public spectrum. It's not free, either. It must be purchased or leased, sometimes in auctions where bidders must compete for licensed bandwidth. →



**This lag or latency increases not only with distance but when there is traffic from voice communications or a high volume of other data.**





## Latency

Low latency, or reduced delay time, is increasingly important in the data-heavy smart grid era. Unlicensed mesh networks involve a processing step with each node they reach, and this slows the signal's process to its destination. This lag or latency increases not only with distance but when there is traffic from voice communications or a high volume of other data.

Licensed spectrum systems allow signals to move through fewer or no mid-point nodes, so processing time is minimal, and the signal moves swiftly to its destination. For utilities, reducing delay time in communication to and from the meter allows technicians to identify outage information faster, which improves response time and provides the data needed to proactively address issues before a customer calls in to report an outage.

## Top Criteria for Utility Communications Applications: What Matters and Why

Taking note of the features and architectural considerations that differentiate each approach, utilities must consider the below factors to determine which wireless network will perform best for their needs:

1. Cost
2. Privacy and security
3. Reliability
4. Redundancy
5. Range
6. Signal to Noise Ratio/interference
7. Latency
8. Interoperability
9. Scalability
10. Resistance to obsolescence
11. Ruggedness in weather
12. Geographic challenges

Which matters most? It depends on the utilities' project requirements. The type of communication network was a big factor in the AMI solution deployed at Benton PUD.



### ABOUT THE AUTHOR:

**Randolph Wheatley** is vice president of Communications Solutions at Sensus. Wheatley has 30 years of experience within the technology space with leadership roles in product management, operations, and product development at Sensus. He obtained his MBA at the University of Texas at Dallas.

# PUBLIC UTILITY PERSPECTIVE ON WIRELESS COMMUNICATION OPTIONS

## STEVE HUNTER

Benton PUD is located in the heart of Washington State's Tri-Cities—also known as “Washington Wine Country.” We serve more than 50,000 customers across Kennewick, Finley, Benton City, Prosser and outlying areas. While residents of this “year-round paradise” are known for a sense of fun and adventure, they're serious when it comes to their demand for reliable and efficient service.

To proactively address our customers' needs for higher quality service, we realized that we needed to think bigger about our electricity infrastructure, and that meant upgrading to advanced metering infrastructure (AMI) technology.

We wanted to deploy a network that would allow us to improve overall operations and communication with customers, so AMI made sense. While we knew AMI was the right path, there was a lot of research that went into identifying the right AMI provider and that included understanding the difference between a point-to-multipoint network architecture and mesh network architecture.

### Laying the foundation

Our team understood that the communication network would be the foundation for a successful AMI deployment, so we prioritized the criteria list. Most importantly, we wanted a network that would allow for fast communication with our electric meters while also serving as the foundation for future applications.

We knew that an AMI deployment was an investment, so the team needed to identify what additional services were needed to meet customer expectations now and provide an opportunity for growth in the future.

### A solution that checked all the boxes

After evaluating AMI solutions, we ultimately chose a point-to-multipoint network architecture based on the need to optimize network performance and quickly process data on a secure and reliable network.

The solution, provided by a North Carolina-based utility technology provider, met all of our criteria and would lay a foundation for future success. One of the biggest factors in the decision was the vendor's two-way communication

network that offered the right capabilities to meet both current and future needs.

### Providing value for our customers

Now fully deployed, our AMI solution on the point-to-multipoint network has exceeded expectations. For starters, the solution has delivered the flexibility and security we desired while allowing our utility to add more enhancements for customers.

Our team knows we made the right choice because the value of the network has only increased over time. Since the initial deployment, we've been able to add a new customer portal so residents can monitor their usage and we have plans to launch a prepaid program by the end of the year.

Because the meters communicate to our utility staff in near-real time when there is an outage, we've improved response time to outages and are able to pinpoint issues that previously would have never been detected.

All of this helps us work more proactively on behalf of our customers. When utility staff receives an outage notification, we can communicate with customers and swiftly initiate repairs.

It's a win-win for our utility and customers.

### Charting a path to the future

The AMI solution on the point-to-multipoint network is our foundation for the future. As the industry progresses and new smart grid applications hit the market, we will continue to evaluate new capabilities.

The factors that affect a utility's choice of a wireless network are highly influenced by the individual organization's resources, goals and challenges. In practice, a combination of mesh and private/point-to-multipoint approaches may exist across a utility's different applications or even within them as projects scale and grow.

By weighing the factors, utilities can select a wireless communications network that will fit their current budget and future needs, deliver equal or improved reliability and support long-term customer satisfaction with rates and services.

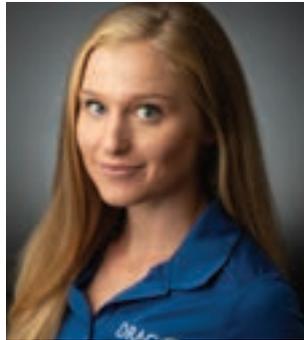
### ABOUT THE AUTHOR:

**Steve Hunter** is director of operations and assistant general manager at Benton PUD, overseeing the safety and reliability of the utility's electric system. He has more than 30 years working in the engineering and operations departments. Hunter is a Washington State-licensed professional engineer and obtained his bachelor's degree in electrical engineering from Washington State University.



# HOW TO APPLY THE FOUR TYPES OF THREAT DETECTION





## **SELENA LARSON**

There are three critical pieces to cybersecurity functionality: Prevention, Detection and Response. Prevention puts up roadblocks for adversaries aiming to conduct malicious activities, while response triages incidents after they occur. The middle piece is most crucial – detection identifies active threats, thereby reducing financial impact, helping to inform prevention measures and minimizing the time hackers have to cause harm within an environment.

Modern threat detection falls into one of four categories: Configuration, Modeling, Indicator and Threat Behavior. Each is different, and it's up to the organization to determine what they need and whether a new method can complement existing security tools.

Threat detection rose to prominence as the internet transitioned from a small group of friendly parties to an open collective now including people who would do harm to others. It began in earnest in the mid-1980s following the publication of Dorothy Denning's intrusion detection model. The first commercial intrusion detection system (IDS) launched in the early 1990s, and anti-virus products – early elements of threat detection – became fully established in that decade as well. Commercial products began to standardize host- and network-based anomaly detection, but as the space evolved and threats changed, the industry began shifting from exclusively using indicators of compromise (IOCs) and signatures, to methods like machine learning and behavior analysis.

For the last few decades, collecting and storing data has been expensive, which has limited our capabilities. Now, as the price of computing has dropped, what was once impossible due to limited storage (behavior analysis) and computing (machine-learning) is now possible. Both of these approaches can now be worked into defensive strategies and existing security models; however, buzzwords can overpromise undeliverable results. →

Though there is no one-size-fits-all detection strategy, grouping the four types of threat detection provides a collection of approaches that defenders can use and identify which one, or group, best work in their environment.

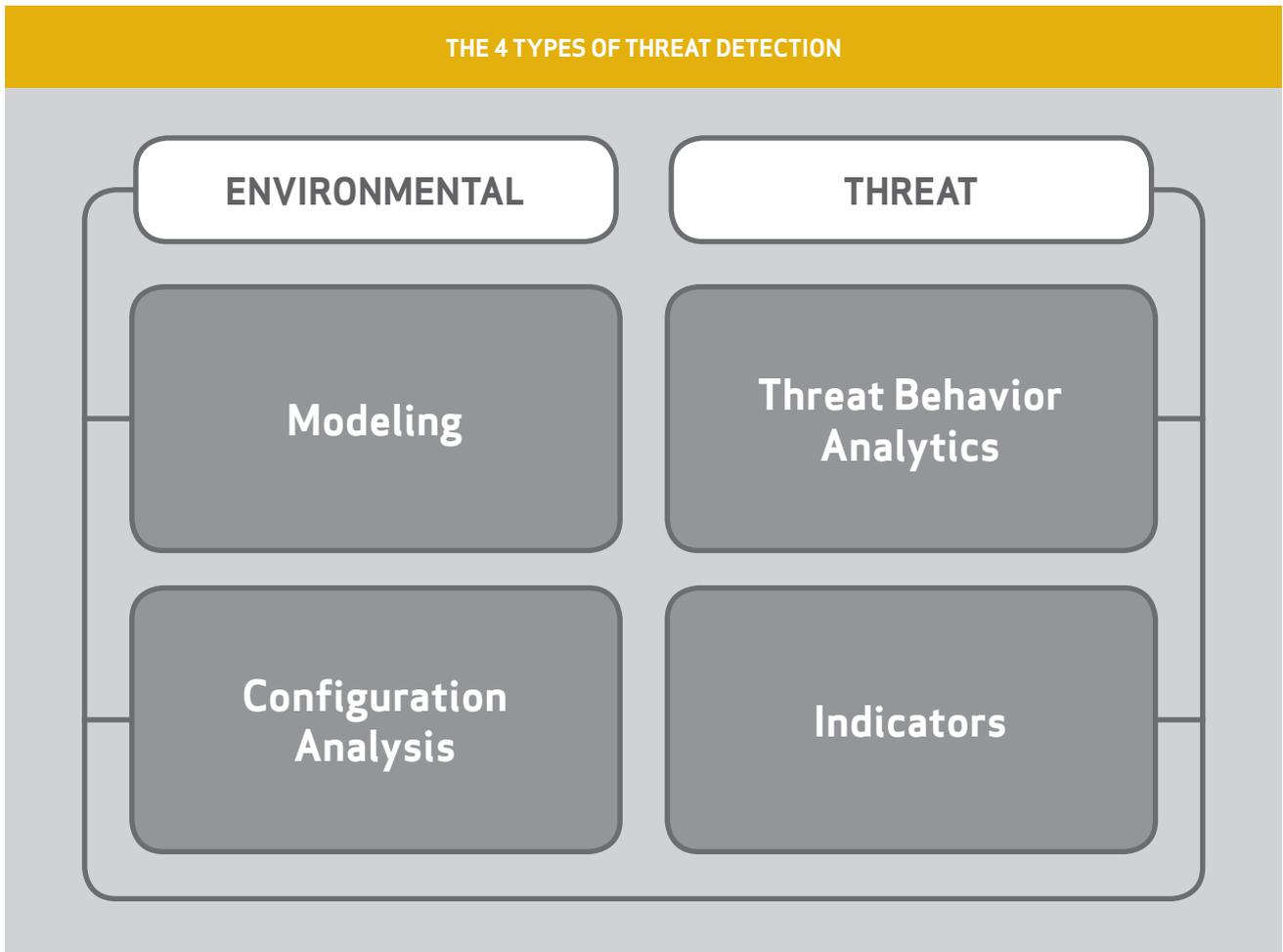
The first step to any security strategy is threat modeling. Creating an inventory of the system, the most vulnerable assets and relevant threats will help drive organizations' threat detection decision-making and prevent overburdening security operations. In order for your detection strategy to be successful, so too must your threat model.

The first threat detection category, **Configuration-based detection**, identifies changes from a known architecture, like two devices communicating with each other over the same ports on regular intervals. Let's say one device, a Programmable Logic Controller (PLC) in a field environment, regularly and exclusively communicates to an Engineering Workstation (EWS) at the company's headquarters over TCP 102. Configuration-based

detection could detect a potentially malicious deviation if the EWS began communicating to a device outside those ports and protocols.

This detection type could theoretically identify all malicious activity, and it's easy to maintain if the environment does not change. However, it does not work well for identifying bad actors on systems requiring frequent modifications. This method also requires defenders to have an in-depth and hands-on knowledge of the system architecture and configurations.

**Modeling-based detection** is similar to configuration-based methods; however, where configuration relies on expert human knowledge of environments, modeling is based on mathematical approaches that assume detection tools can identify bad activity from good. Modeling begins from an automated approach, often using machine learning, to establish a baseline of the system activity and configurations. Then the detection engine automatically alerts on activity that differs from what it identifies as normal. This method also has



drawbacks; although system operators will get alerts on the malicious activity, modeling doesn't provide any additional context about the activity itself to help triage or further investigate an incident. It's also possible that when a company implements this method with a hacker already inside their environment, malicious activity can be included in the "safe" baseline.

**Indicator-based detection** can be created and deployed quickly. Indicators of compromise (IOCs) are what analysts use to identify malicious activity including hash values, IP addresses, domain names or malware signatures. This type of detection can provide some context to the threat and is most useful when paired with other methods – modeling can automatically detect a deviation from the baseline and analysts can use indicators to augment the data. However, an indicator must first be observed, so this method is somewhat reactive. Indicators can be found in the observed environment directly, incorporated into defensive mechanisms through automated detection tools or on open source directories like VirusTotal. Further, an indicator is only as good as long as it's relevant – an adversary can change their infrastructure, like command and control (C2) servers, thus rendering the C2 artifacts moot.

**Threat behavior detection** uses commonalities in adversary tools, techniques and procedures (TTPs) to create a comprehensive analytic capturing the observed threat. Defenders can then leverage the underlying behavior rather than individual IOCs to target variations of the observed TTPs, irrespective of changing IOCs. The behavior can be compared against known malicious activities. For instance, the specifics for activity group ALLANITE include targeting electric utilities using watering hole and phishing attacks leading to industrial control system reconnaissance. The group uses legitimate

Windows tools to conduct its activities. Indeed, this type of detection can detect seemingly legitimate behaviors as malicious. For example, an attacker using the VPN to access the network, creating and using new credentials, downloading a file on an engineering workstation, and then attempting to log into a PLC. While this approach is resilient against adversaries changing infrastructure and IOCs, it cannot be automated and is time-consuming to implement initially.

“  
However, it is a good idea not to rely on  
one method alone.  
”

To defenders wondering about the best approach, there isn't one. It's entirely environment-dependent and goes back to your threat model. What is most important? If you want to discover new activity and figure out the full scope of an incident, configuration detection checks those boxes. For good transparency, flexibility and resilience to the changing threat landscape, use threat behavior detection.

However, it is a good idea not to rely on one method alone.

As the threat landscape evolves and defenders can access increasing amounts of data and knowledge about how adversaries operate, we will build better tools and procedures to detect hackers that don't fall into these categories, or realize that some strategies don't work. Threat detection is not static, and the future is open for new innovations and mechanisms to defend ourselves.

#### ABOUT THE AUTHOR:

**Selena Larson** is an intel analyst for Dragos. As a member of the threat intelligence team, she works on reports for WorldView customers including technical, malware and advisory group analyses, and writes about infrastructure security on the company's blog. She works to combat fear, uncertainty and doubt surrounding malicious activity targeting ICS environments and help people better understand complex concepts and behaviors. Previously, Larson was a technology reporter, most recently at CNN. She reported on privacy and security issues within the technology industry including ICS threats. In 2017, she was a fellow at the Loyola Law School Journalist Law School program, the only cybersecurity reporter to be selected that year. Larson lives in San Francisco. She writes short fictional stories speculating on our technological future and how things like robots, virtual reality and increasing connectivity impact our brains, relationships and human behavior.

# INDUSTRY-SPECIFIC CYBER PROTECTION REQUIREMENTS: POWER INDUSTRY IN NORTH AMERICA





### **JENS PUHLMANN**

The last few decades have seen major advances in technology, resulting in significantly smaller devices, increased functionality and a new range of connectivity options. In general, the effect has been positive for everyone: Added convenience for consumers and industries alike; from online shopping and online banking, to increased productivity in all industries.

For the industrial manufacturing sector, change has come rather gradually over the last decade. In some cases, the manufacturing industry still relies on infrastructures based on isolated serial communication networks to connect PLCs, RTUs and other process control equipment. Although slower than Ethernet, these often proprietary network protocols are optimized for the real time communication requirements of process control equipment, which were not possible using half duplex Ethernet. With the introduction and widespread availability of full duplex Ethernet in the late 1990s, Ethernet became a viable option for real time communication in industrial control systems. Development on modern Ethernet-based process-control protocols started during the same period, but it wasn't until the mid-2000s that the technology was widely accepted, even for very latency sensitive process-control tasks. →

The introduction of Ethernet has brought many improvements to industrial control systems. Controls engineers no longer have to rely on adapters, cables and protocol analyzers for different proprietary communication protocols – a network cable and a spare network port are all that are needed for the troubleshooting and maintenance of many networked process-control devices. Common network troubleshooting tools, already well established in the IT world for years, now support this new infrastructure. In many cases, these tools are open source and free to use. Interested programmers added support for process-control protocols to these tools, which could then be used for most troubleshooting tasks. Adding new devices to the network is now easily accomplished, assuming that the design engineer had provided enough available spare ports throughout a facility. Improvements in networking concepts always find their way into the process-control environment, resulting in higher reliability and better performance. Two examples of this are the use of Ethernet redundancy protocols like Rapid Spanning Tree Protocol (RSTP) for fault tolerance and loop prevention, and the use of network time protocols for plant-wide time synchronization.

In short, Ethernet has had a tremendous and mostly positive impact in the process-control landscape. However, there is a dark side. The same technology that allows for convenient online shopping from home, as well as easy and convenient connectivity within an office or a manufacturing facility, can also be used to attack the infrastructure of all connected systems using the anonymity of the internet or from the inside of a network, potentially impacting all devices within that network.

This is not a new development, though. Industry experts have long tried to stop this trend and improve security measures by publishing standards and guidelines for more secure infrastructure protection. However, application of these standards is often voluntary and not monitored for most industries.

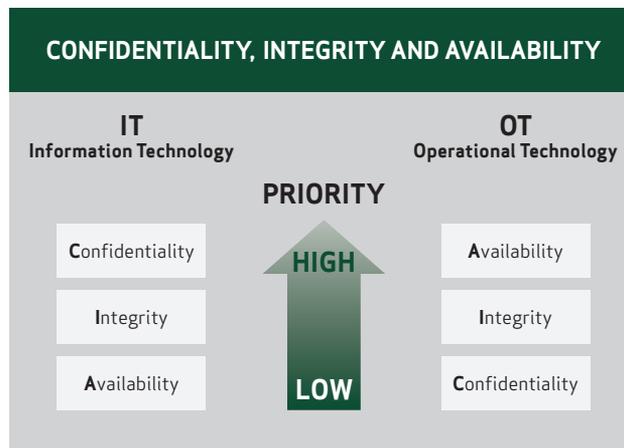
Also, many of these standards are very generic and do not take into account the specific requirements of different industries.

Banking infrastructure, for example, places the highest priority for data protection and integrity and therefore requires significant effort regarding data encryption, while the requirements regarding communication latency and speed are relatively low. Generally, it matters little if a financial transaction takes two or five seconds to complete, as long as the transaction is secure.

For the industrial sector, the requirements are typically reversed - usually, there are no databases with sensitive information, such as personal data, social security numbers or credit card information. Instead, the communication

interfaces within an industrial facility require real-time interaction between devices and are therefore very sensitive regarding latency and data throughput; a time delay of a single second during error detection can result in significant harm to personnel or equipment.

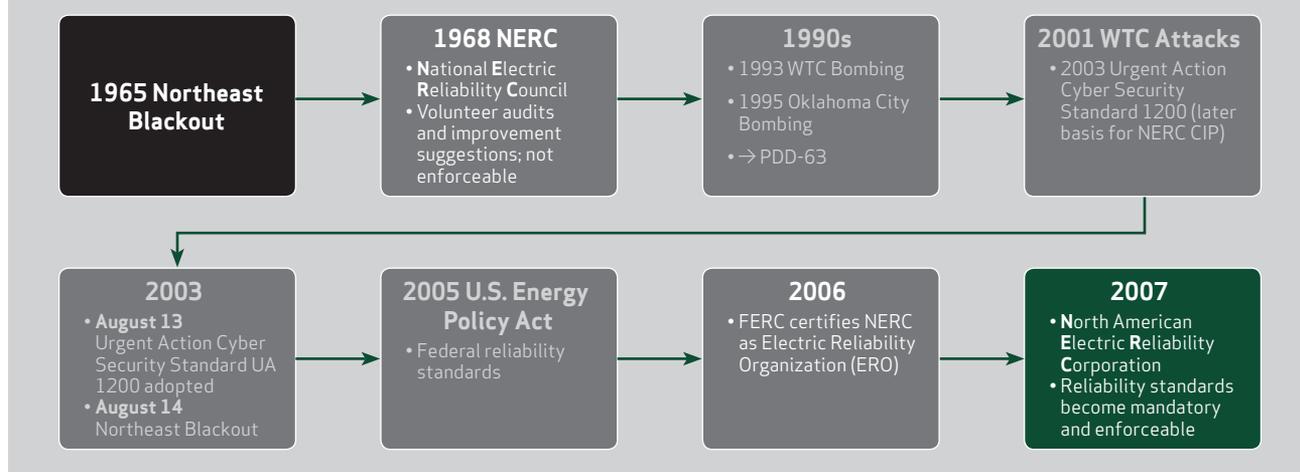
This can be visualized in the “Confidentiality, Integrity and Availability” relationship:



When comparing the priorities between IT and OT, it becomes obvious that a different approach is needed to protect each infrastructure. This has resulted in the development of industry-specific standards, independent of the more general standards published and maintained by IEC, ISA, ISO, NIST, etc.

For the North American Energy sector, NERC CIP is the mandatory set of standards for critical infrastructure protection and includes a wide range of topics to protect all critical cyber assets. NERC was founded in 1968 as the National Electric Reliability Council to provide voluntary operating coordination. The need for critical infrastructure protection was driven by a series of blackouts as well as several terroristic attacks, resulting in Presidential Decision Directive 63 (PDD 63) in 1998, with the goal to fully protect the critical infrastructure no later than 2003. The 2001 World Trade Center attack further heightened this need, resulting in the Urgent Action Cyber Security Standard UA 1200 in 2003, which later formed the basis for the first NERC CIP standard. Shortly afterward, the Federal Energy Regulatory Commission (FERC) certified NERC as the Electric Reliability Organization, making all NERC standards mandatory and enforceable. The agency, which was renamed the North American Electric Reliability Council in 1981, changed its name again in 2007 to its current name, the North American Electric Reliability Corporation.

## THE BEGINNINGS OF NERC CIP



Aside from CIP, NERC maintains a wide range of other standards, including EOP (Emergency Preparedness and Operations), BAL (Resource and Demand Balancing), TOP (Transmission Operations) and several more.

To clarify applicability and requirements of all NERC standards, a “Functional Model” is used. It describes each function in detail, the associated reliability tasks as well as the functional entity responsible for these tasks. These functions cover a range of 18 power industry functions, which are grouped into three functional areas:

- Standards and compliance functions
- Reliability service functions
- Planning and operating functions

Another important document is the “Glossary of Terms,” which describes specific terms in relationship to the standards documents. Without this information, the impact of some requirements might not be fully understood; an example of this will be provided when discussing the Electronic Security Perimeter (ESP).

Every NERC standard begins with an applicability list, identifying the functional entities to which the standard applies. Compliance is measured based on the definition of the reliability tasks in the Functional Model – violations occur if the reliability task assigned to a functional entity has been impaired.

Development of the standards is ongoing, with some older standards already retired while existing standards are continuously updated and new standards developed, resulting in an ongoing effort from all responsible entities to maintain standards compliance. The goal: A reliable energy infrastructure for North America.

The purpose of NERC CIP is the protection of all BES Cyber Assets – cyber assets which are a critical part of the Bulk Electric System and grouped together as BES Cyber Systems. This is achieved using three different types of controls:

- Administrative and procedural controls
- Physical access controls
- Technical controls

Since technology changes at a rapid pace, the technical controls are the most challenging requirements of NERC CIP and are the main focus of this article.

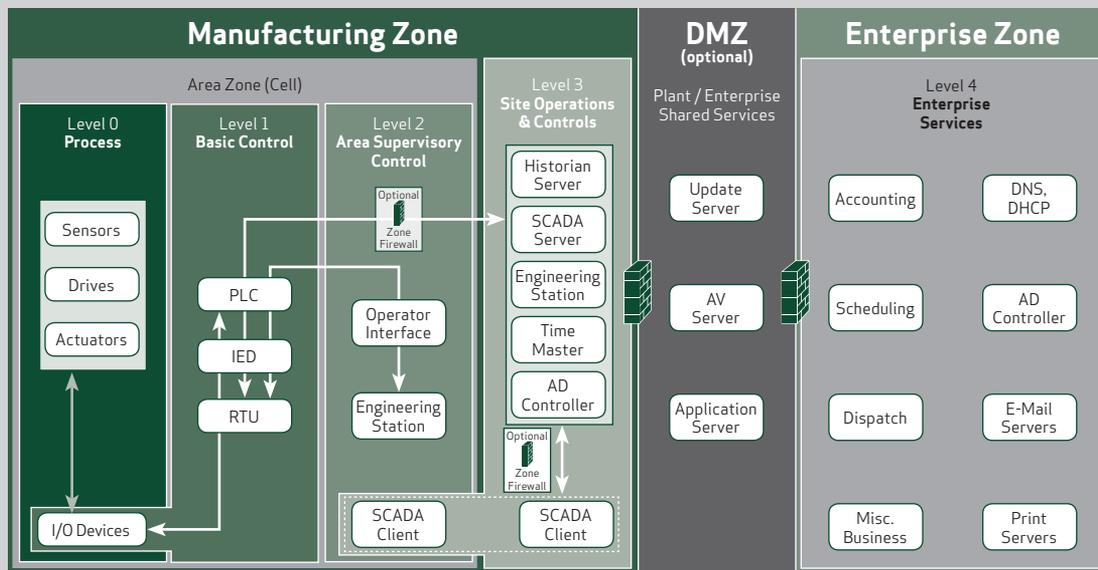
To understand the concepts and requirements of NERC CIP better, the Purdue Enterprise Reference Architecture can be used.

The original Purdue Enterprise Reference Architecture recognizes two main zones: The manufacturing zone (Levels 0 to 3, also known as operational technology) and the enterprise zone (Level 4, also referred to as information technology).

If data exchange between the manufacturing zone and the enterprise zone is required, the use of a demilitarized zone (DMZ) to separate both zones is strongly recommended. In this example, no direct communication between the manufacturing zone and the enterprise zone is possible; all communication requires data interfaces in the DMZ, which are controlled by a firewall at each border.

This basic architecture is very common for power industry facilities. The scope for NERC CIP standards in this example includes the manufacturing zone (Levels 0 to 3) as well as the firewall separating this zone from other zones. →

## THE PERDUE MODEL: A SIMPLIFIED VIEW OF THE PLANT NETWORK



Application of the NERC CIP standards is based on a list of functions and categorization criteria related to the reliable operation of the bulk electric system. Each functional entity is required to identify all associated BES Cyber Systems, resulting in an impact rating of low, medium or high. The individual NERC CIP requirements are then applied based on the impact rating of each BES Cyber System. It is possible to create multiple BES Cyber Systems, rather than treating the entire facility as single system. Depending on the system design, this can result in lower impact-rated individual BES Cyber Systems with fewer requirements and less management effort.

A central – and mandatory – figure for application of the NERC CIP standards is the entities' CIP Senior Manager, who has the responsibility to lead the NERC CIP standards compliance effort, including the authority to delegate CIP-related tasks.

As mentioned earlier, the NERC CIP standards cover many different topics, including administrative controls and operational procedures. Examples of administrative controls are the requirements for appropriate personnel risk assessment and personnel training as well as access management and access revocation. Operational procedures need to include system recovery, incident response and information protection. Physical access control requirements cover topics from physical facility access and a visitor control program, as well as requirements for access logging.

In many cases, these topics are already common practice for industrial facilities and will not be reviewed further; the technical cyber protection requirements of NERC CIP are usually the most problematic aspect of CIP compliance. These include requirements for:

- Electronic security perimeters
- Physical as well as logical port management
- Patch management and malicious code prevention
- Security event monitoring
- System access control
- Configuration change management
- Vulnerability assessments
- Handling of removable storage devices and transient cyber assets

These requirements create several technical challenges. Frequently, there is a mix of legacy devices and modern devices on the same network – PLCs, RTUs, power meters, protection relays, remote I/O racks etc. Many legacy devices lack even basic cyber security features for access control, port management or event monitoring. In some cases, the manufacturers for these devices no longer provide firmware updates, but replacing these devices with more modern versions might require a redesign of system interfaces. Also, proprietary communication protocols might make relocation of these devices behind a firewall impossible, due to special protocol requirements.

Patch management has the potential to disrupt system operation if there are compatibility issues. Proper planning, as well as accurate system recovery procedures in case of patch failures, is absolutely critical. The same applies to active vulnerability assessment, which has the potential for devices rebooting or locking up. Again, proper planning is absolutely vital for successful vulnerability assessment, combined with a full understanding of the system design and communication interfaces. Otherwise, the results of such assessments are useless, since the relationship between open ports and communication interfaces cannot be determined.

Presently, there is no standard concept for change management for these kinds of devices, so each device has to be managed manually using the management interfaces provided by the device manufacturer and based on the capabilities and features of the device. However, there is one critical concept that connects all devices: The ESP.

The requirement for the ESP is very specific: All cyber assets connected using a routable protocol shall reside within a defined ESP. This excludes any device connected using serial communication (RS232, RS422/485), but also excludes devices that use non routable Ethernet Layer 2 communication. Presently only TCP/IP qualifies as a mainstream protocol that supports routing, which means that any device that uses an IP address has to be considered as part of the ESP. However, there is another consideration here: Impact Rating Inheritance. Although not spelled out in the CIP standards themselves, the "Glossary of Terms" describes the term "Protected Cyber Asset" as any cyber asset within an ESP which is not part of the BES Cyber System, but will inherit the impact rating of the highest-rated BES Cyber System within the same ESP. So a printer in the same ESP as critical BES Cyber Assets would receive the same impact rating and thus the same requirements regarding patch management and vulnerability assessment.

This concept can now be used to simplify the system by applying proper network segmentation. For example, by placing all printers in a designated network separated from all critical BES Cyber Assets using a firewall, these cyber assets are now part of a new ESP without BES Cyber System, thereby reducing requirements significantly.

When properly used, the concept of Electronic Security Perimeters combined with appropriate grouping into individual BES Cyber Systems of different impact ratings can result in significantly reduced management effort for non critical cyber assets.

These challenges are not unique to NERC CIP – similar problems exist everywhere in the industrial sector. What makes the power industry special is its classification as critical infrastructure, resulting in these mandatory security standards and associated audits. While a non critical manufacturing facility might choose to ignore

appropriate cyber protection implementation due to the associated costs, this is not a choice for most Bulk Electric Systems. But, at its core, NERC CIP describes many common IT security concepts that help the OT landscape to become better protected and more reliable. The best approach for this integration is a strong convergence between IT and OT personnel, combined with the appropriate administrative controls and procedures.

One topic frequently neglected is the requirement for well-maintained system documentation. Combining the growing complexity of industrial control systems with the increasing security requirements of the IT interfaces within the system, good documentation is vital for plant maintenance as well as providing evidence documents during any NERC audit process.

To help with the implementation of the CIP requirements, the CIP standards provide expected measures and examples of evidence to confirm compliance, as well as explanations why specific requirements were included. For a responsible entity, this leads to a better understanding of the requirements – not only to pass an audit but actually resulting in better-protected BES Cyber Systems.

Presently missing from NERC CIP are requirements regarding maintenance contingency. As industrial control systems become more complex, the knowledge required to maintain those systems increases. Typically plant uptime requirements do not allow for the training of new personnel, which can lead to problems when experienced personnel leave. Hopefully, this is something that will be considered in future CIP standards.

Maintaining a fully NERC CIP-compliant facility is a tremendous task. As technology changes, so will the CIP standards, resulting in continuous changes to BES Cyber Systems. But with its current approach, NERC CIP is certainly a standard that will continue to improve our critical infrastructure, especially when applied during the design phases of new power industry facilities. Hopefully, this will also lead to a shift in all industries, demanding better system security designs even when not specifically mandated by regulation or law.

#### ABOUT THE AUTHOR:

**Jens Puhmann** is the Industrial Control Systems (ICS) security manager for Voith, North America. He has more than 20 years of experience designing, developing and implementing advanced automation systems. Puhmann is an expert who keeps up with the ever-changing world of technology and cyber security. Recently, he became one of the first people in North America to hold the GIAC Critical Infrastructure Protection Certification (GCIP).

# CYBER IMMUNITY: A HOLISTIC VIEW FOR INDUSTRIAL CONTROL SYSTEMS



## **JONATHAN AZARCON**

In the past few years, there has been a worldwide rise in cyber attacks on Industrial Control Systems (ICS), and experts have been warning utility executives around the world about the potential threats. Two examples of threats include the recent string of Russian cyber attacks targeting U.S. Government entities and multiple U.S. critical infrastructure sectors, including the energy, nuclear, commercial facilities, water, aviation and critical manufacturing sectors<sup>1</sup>, and the 2015 cyber attacks on the supervisory control and data acquisition (SCADA)'s distribution management systems of three regional electricity distribution companies in Ukraine resulting in several power outages across various areas<sup>2</sup>. This article addresses the greater issue at hand – the potential future of these attacks, and whether this has become the new warfare. Attacks such as these have led to an intensified concern in various industries surrounding the protection of operational technology (OT) environments.

### **IT Versus OT**

In a typical enterprise environment, protection of critical data is often seen as a top priority. This need is met by employing multiple Information Technology (IT)/IS personnel to protect and combat potential cyber security issues. However, the common practice of protection of critical data is often not translated over to establishing the security of Operational Technology (OT) environments. What is Operational Technology? It is software or hardware that controls processes, physical devices and events in an enterprise, and ultimately alters the state of a system; such system can include access control, process control, surveillance voice technologies, etc. OT is categorically used interchangeably as a part of or as an Industrial Control System. →

In mission-critical infrastructures, ICS such as power grids, mass transit transportation systems (e.g., airports, bus terminals, roadways or train stations), wastewater facilities and nuclear power plants, the emphasis should be not only on security for the IT assets but also on the often-overlooked OT assets. Let's take, for example, a power utility company which has implemented enterprise systems and has its IT department devoted to protecting these systems. On the flipside, the company has field assets – transmission and distribution stations – which generate and distribute power to the consumers, and these assets are essentially the main driver of the revenue stream and the lifeblood for that company.

Having spoken with many customers, some are surprisingly unaware of the threats faced by their OT systems, and such companies often believe that closed systems not connected to the public WAN are safe from threats. In reality, this is simply not the case; those systems are highly vulnerable and being exposed to a cyber-attack after functioning long term without the capabilities of early detection or containment, they can suffer detrimental and crippling consequences in the aftermath of a cyber-attack.

### Tactics and Techniques for Attacking OT Systems

For example, in the cyber attack of Ukraine's power grid, the attackers' tactics and techniques included:

- Spear phishing for gaining access to the business networks of the companies
- Different variants of the BlackEnergy 3 malware and manipulation of Microsoft Office documents that contained the malware to gain a foothold into the Information Technology (IT) networks of the electricity companies
- Theft of credentials from the business networks
- Use of virtual private networks (VPNs) to enter the ICS network
- Use of existing remote access tools within the environment or issuing commands directly from a remote station similar to an operator Human Machine Interface (HMI)
- Serial-to-ethernet communications devices impacted at a firmware level
- Use of a modified KillDisk to erase the master boot record of impacted organization systems as well as the targeted deletion of some logs
- Utilizing UPS systems to impact connected load with a scheduled service outage
- Telephone denial-of-service attack on the call centers the Human Machine Interface (HMI)<sup>2</sup>

### Air Gaps Between IT and OT Networks

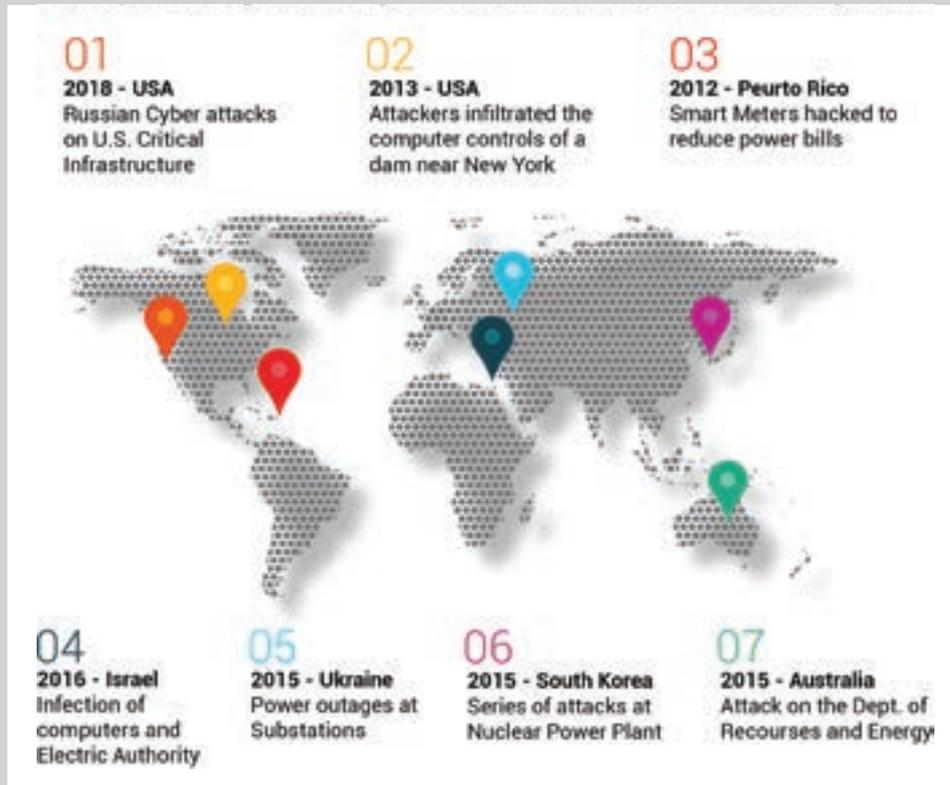
Historically and still in the present day, OT networks are legacy systems that were primarily isolated specialized systems using proprietary hardware and software. As such, they were not connected to the company's enterprise networks and run independently, thus resulting in "air gaps" between the IT network and the OT network. Air gaps occur when one network such as IT has security measures that segment the IT environment from their unsecured OT counterpart. The good news is that with the advancements in technology, OT networks are moving towards a more converged network environment and more efficient control of data transportation, storage, data analytics and monitoring processes. However, now as a part of the converged network environment, OT network users and administrators must put serious consideration into the cyber threat landscape. Even governments recognize the need for cyber protection and have legislated Critical Infrastructure Projects (CIP) to implement threat measures for protection of critical systems. For this article, let's focus on the OT environments and how to improve the resilience to cyber attacks.

### Why Cyber Resilience is so Crucial

When it comes to cyber resilience, the rise of cyber threats against ICS globally should always be on the top of the CEO's "to-do" list. OT networks have a different set of protocols from an IT environment. Availability or access to assets of a nuclear plant or power substation is a top priority for an OT network, versus an IT approach that prioritizes confidentiality as the number one concern. OT environments must have constant communications between devices monitoring or controlling critical functions. For example, critical assets in a nuclear plant that monitor thermal sensors could potentially prevent overheating and causing an explosion. Blocking of any virtual traffic due to security requirements to these critical assets may have severe consequences for the OT environment.

Simply put, blocking traffic in the IT world (e.g., in a bank) may cause the bank to lose some transactions. As a result, the bank can shut down that part of the system for containment and quarantine, but this will be by no means life-threatening. However, in the OT environment, blocking traffic can potentially lead to the death of an employee or others if the non-communicating device is responsible for process control and monitoring of a critical function such as cooling of a reactor at a nuclear plant. Even with accessibility as a top priority for OT networks, we can't conclude that OT networks should not be protected or can't be protected from cyber threats. Adversely, it is these types of systems that should be highly secure since they provide service with significant and immediate impacts on human lives that extend beyond the company's human resources.

## EXAMPLES OF SIGNIFICANT CYBER ATTACKS IN INDUSTRIAL CONTROL SYSTEMS



### Hackers in Mission Critical Systems

Ongoing activities of hackers continue to threaten mission-critical systems as they see vulnerabilities in industrial networks worldwide. Once hackers have infiltrated your corporate environment, they can traverse through other unsecured networks within the OT environments, target vulnerabilities, and propagate within the company. These types of threats have essentially become the new warfare in the present world whether by solitary hackers or state-sponsored. (See map with scenarios of cyber attacks on ICS applications and their onward trends.)

### Defense in Depth – People, Processes & Technology

When considering protecting your data, you need to look at a “Defense in Depth” multi-tiered or layered approach. There is no “out of the box security” that can provide a singular solution to stop cyber threats in today’s world. Security is not an isolated process but an ongoing process; hence, why a layered approach is needed to constantly protect your critical data. Using best practices,

an organization could limit future attacks, essentially creating an ecosystem to ensure Cyber Immunity with a holistic view. It is the sum of all parts working together to ensure optimum performance. Technology alone, while playing a vital part, will not prevent cyber threats in today’s modern world. Rather, the principals surrounding Cyber Immunity should be developed and balanced around the fundamental pillars – People, Processes & Technology. Security for your organization should always be transformational to keep up with the latest threats and adjust to those threats within the pillars.

- **People** within the organization need to be made aware of the sensitivity of data; therefore, training staff about the potential threats and how to secure the data is essential. To ensure competency and mitigate risks, staff’s knowledge or skills should always be updated to reflect the latest technologies.
- **Processes** are important for the effective execution of organizational strategies. They define how the organization will react and follow a documented protocol for data protection. →

- **Technology** is crucial for implementing controls for stopping and mitigating threats as well as logging and tracking user's activities.

If we draw parallels to how the human body works, people also get viruses, and often relying solely on a body's defense mechanisms and healing power may not be enough. A proper nutrition plan, along with adequate rest helps with the healing process, but at the end, a medication may be needed to start or bring to speed recovery. Generally, practicing good health, diet, exercise and proper rest daily could mitigate potential sickness down the road, improve immunity and make a person more resilient to sickness. In parallel, this holistic approach to wellness and health is not different from an organization's method of protection of their data and ensuring cyber resilience. So, to recap, if everyone in the organization implements and practices a cyber-resilient lifestyle, then the organization would have a better chance of preventing future sickness of their data. However, having said this, it doesn't guarantee an absolutely secure environment as the company operates into the digital landscape. Cyber threats have evolved in how to infiltrate or compromise systems, and as a result, organizations should continually strive to evolve and adapt their immunity to potential cyber threats as new strains of viruses, malware or hacking techniques are introduced to this landscape. With this, adding layers of security is a much more effective approach than relying solely on a single mechanism for data protection. All defense layers should work in unison to be effective and be validated throughout its lifecycle. So, what would those layers encompass?

### Approach for Cyber Resiliency

Let's start examining the layers of a company's approach to cyber resiliency. As per the author of this article, the most important layers on which a company needs to focus are as follows:

- **Full Visibility, Understanding and Up-to-date Record-keeping** of current inventory or what's connecting or connected to the company's network, servers, databases, mobile devices, PLC's, relays IED's, IoT devices or simply discovery of all company's assets
- **Risk Assessment**—after taking inventory of all assets connected to the company's network, they must be evaluated, and those needing protection determined. Next, threats are to be analyzed, risks identified and assessed and tolerances to those risks determined. After that, current network architecture must be evaluated, and the need to make the network more secure when corresponding to the needs of the OT application determined.

## A LAYERED APPROACH TO CYBER RESILIENCY



- **Penetration Test** on the company's current networks and establishing vulnerabilities and gaps. Conducting a penetration test is crucial for preventing data breaches and verifying effectiveness of the implemented security controls. For example, if a company performs a "brute force" attack as part of the penetration test, efficiency of passwords will be tested, and enforcing the use of a combination of letters, numbers and symbols with a minimum of eight characters will be included into the organization's security compliancy procedures.
- **Incident Response**—have you ever tested how well your organization responds to a cyber threat and manages its aftermath? The goal is to ultimately prevent data breaches of the organization's network. However, when the network has been breached, the organization needs to be able to contain the breach preventing it from further spreading into other areas of the network and ultimately taking down important process controls. An organizational emergency containment and recovery plan is a must for every organization and is also a crucial measure for mitigating outages and disruption in service to customers.

As per the Escal Institute of Advanced Technologies (SANS Institute), a private U.S. for-profit company that specializes in information security and cyber security training, the six key phases of an incident response plan are:

1. Preparation—preparing users and IT Staff to handle potential incidents should they arise
2. Identification—determining whether and if, indeed, the breach is a security incident
3. Containment—limiting the damage of the incident and isolating affected systems to prevent further damage

4. Eradication—finding root causes for the incident and removing affected systems from the production environment
  5. Recovery—permitting affected systems back into the production environment while avoiding remaining threats
  6. Lessons learned—completing incident documentation, performing analysis to learn from the incident and potentially improve future response efforts
- **Disaster Recovery**—an organization should be well prepared when situations arise. Proper procedures must be in place to prepare, react and recover from a disaster. Roles and responsibilities within the organization have to be clearly defined and communicated. The company should always have backup of their data in case of failures, and as per the best industry practices, the backup should be kept at a remote site, often referred to as a disaster recovery (DR) site. Once in a while, fire drills have to be conducted to test the effectiveness of the DR plan and modify risk tolerances accordingly while ensuring business continuity.
  - **Governance**—compliance within the organization typically surrounds policies, procedures and training for employees. There should be compliance controls in place so that employees are following the established organizational policies for data protection. Some compliance often is mandated by local or national authorities and regulations, and compliance with these authorities and regulations must be incorporated in the organizational compliance policies.

## Outlook

In retrospect, we speak of fundamental principles that encompass a holistic view to what organizations need to consider when looking at shaping for cyber resilience in their ICS application. The company's journey to cyber security should never stop at one singular aspect but employ an overall continuity of many moving parts. Of course, even while implementing a total security solution, nothing is absolute. Perpetual transformation, harmonizing and understanding of the needs of a converged network from both IT and OT peers while securing the environmental need to be top priority. Constant vigilance, review of new and potential threats and ongoing transformation of the organization in adapting to the ongoing threat landscape is paramount to the success of any company.

### ABOUT THE AUTHOR:

**Jonathan Azarcon** is currently the EVP of marketing and product management for iS5 Communications and has more than 22 years of combined experience in telecommunications technology, working in business enterprise and industrial control applications. He has designed and implemented networks for customers worldwide as a professional services consultant with Alcatel Networks and as a VP of global services & support at RuggedCom Networks and Siemens AG as instrumental in helping customers implement & support communications technology for their ICS.

### References

<sup>1</sup> United States Computer Emergency Readiness Team, Alert (TA18-074A), Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors, Last Revised March 16, 2018, <https://www.us-cert.gov/ncas/alerts/TA18-074A>, Last Accessed Oct 1, 2018

<sup>2</sup> Electricity Information Sharing and Analysis Center (E-ISAC), TLP: White Paper, "Analysis of the Cyber Attack on the Ukrainian Power Grid", Defense Use Case, March 18, 2016, Internet: [https://www.nerc.com/pa/CI/ESISAC/Documents/E-ISAC\\_SANS\\_Ukraine\\_DUC\\_18Mar2016.pdf](https://www.nerc.com/pa/CI/ESISAC/Documents/E-ISAC_SANS_Ukraine_DUC_18Mar2016.pdf), Last Accessed Oct 1, 2018

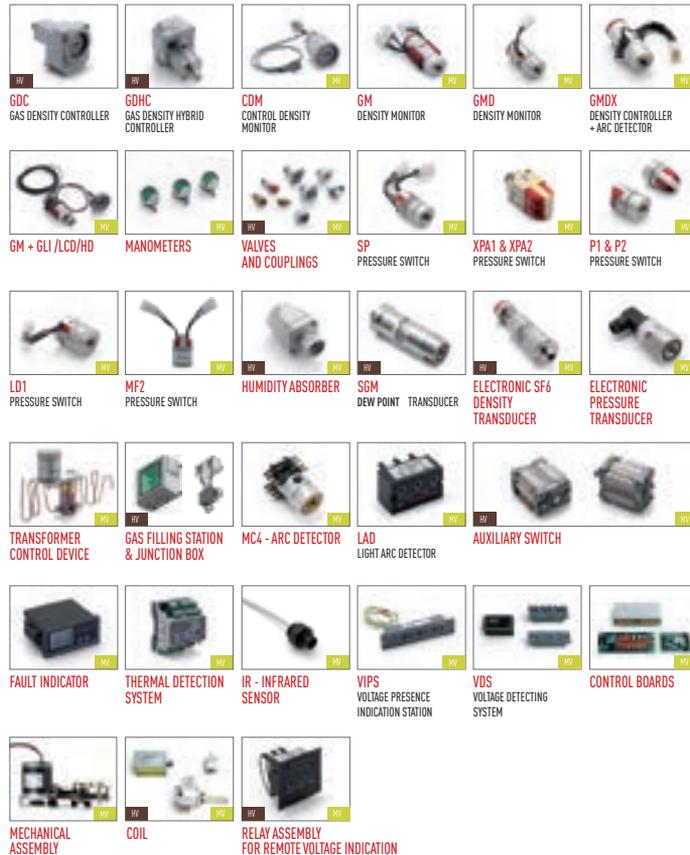
ELECTRONSYSTEM MD is a leading Italian Company who specializes in developing and productions a broad range of products for use on MV and HV switchgear. We have excelled in the marketplace since 1992 and pride ourselves on our commitment to:



- Staffing highly qualified engineers with over 30 years of experience in both field and factory environments.
- Providing innovative, safe, and reliable solutions to problems.
- Fluidly adapting to meet customers technical and financial needs.
- Maintaining a strong collaborative relationship during all phases of projects: design, assembly, testing, and marketing.

## PRODUCTS:

- ✓ Density Controllers
- ✓ Valves & Couplings
- ✓ Transducers for: Density; Pressure; Moisture; & Temperature
- ✓ Manometers
- ✓ Moisture Absorbers
- ✓ Manifolds & Tubing
- ✓ Gas Filling Station
- ✓ Arc Detector
- ✓ Light Arc Detector
- ✓ Auxiliary Switch
- ✓ Fault Indicators
- ✓ Thermal Detection Systems
- ✓ Voltage presence indicators
- ✓ Voltage Detecting Systems
- ✓ Touch Panel & PLC's
- ✓ Control Board
- ✓ Mechanical Assembly
- ✓ Coils
- ✓ Relay Assembly for remote Voltage indication



# DDIN<sup>®</sup> STRINGING BLOCKS

WHETHER YOUR NEEDS ARE FOR 7 INCH DISTRIBUTION BLOCKS  
OR 42 INCH HELICOPTER TRANSMISSION BLOCKS WE HAVE YOU COVERED

**FOR PURCHASE OR RENTAL**

AVAILABLE FOR THE TALLMAN EQUIPMENT STRINGING BLOCK TRADE IN PROGRAM



**FOR MORE  
INFORMATION CALL:**

**630-860-5666**

REMEMBER TO ASK ABOUT OUR TRADE-IN PROGRAM

[WWW.TALLMANEQUIPMENT.COM](http://WWW.TALLMANEQUIPMENT.COM)

TALLMAN EQUIPMENT IS AN EMPLOYEE OWNED COMPANY



# Making testing simple, safe & efficient

## *M7100 High Voltage Asset Analyzer*

---

### REVOLUTIONIZING HIGH VOLTAGE TESTING

The Doble M7100 High Voltage Asset Analyzer is a revolutionary solution for high voltage testing.

**Save on testing time:** Traditional transformer testing can be finished in a third of the time. That's because the Doble M7100 and DTA software work together to automate multiple tests that previously required several pieces of test equipment.

**Maximize your outages:** By reducing testing time, you can now maximize outage periods by performing more maintenance during the hours previously needed for testing.

**Limit safety risk:** The M7100's patented dual high-voltage leads can switch between source and measurement. This means you can perform multiple tests with one cable set up - and you reduce the number of ladder trips technicians are exposed to per job.

These are just some of the ways the Doble M7100 is helping to make testing simple, safe and efficient.



Learn more about how your testing program can benefit from the Doble M7100.  
[www.doble.com/M7](http://www.doble.com/M7)

