

electroindustry



www.NEMA.org | January 2017 | Vol. 22 No. 1

Blockchain: The new face of energy transactions

- 11 | Securing the Connected Environment
- 17 | Cities Commit to Efficiency
- 20 | Data Centers Go Flexible

NEMA

CONNECTING YOUR BRIGHT IDEAS



TE Connectivity (TE) is transforming technology and helping to inspire new designs in LED street lighting systems by enabling connected lighting. These “plug-and-play” lighting solutions allow creative designers to take advantage of increased functionality, modularity and efficiency to design lighting systems that offer faster installation, reduced costs and flexibility. TE works with designers, engineers and manufacturers on connectivity solutions for products used in innovative, efficient and more intelligent buildings.

Connect with TE at te.com

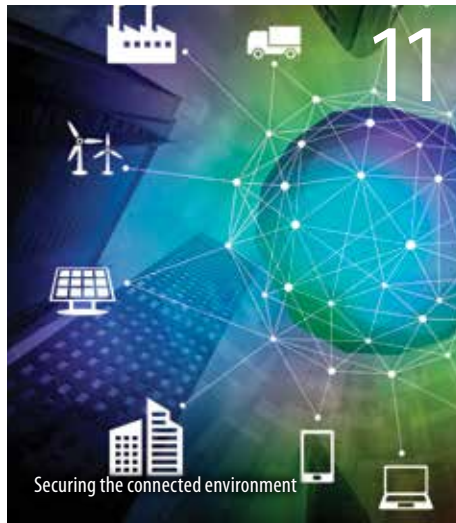
© 2016 TE Connectivity Ltd. Family of Companies. All Rights Reserved. TE, TE Connectivity, and the TE connectivity (logo) are trademarks of the TE Connectivity Ltd. family of companies. Other logos, product and Company names mentioned herein may be trademarks of their respective owners.



CONTENTS



4 Enhancing, coordinating, and improving security



Securing the connected environment



22 Focusing on Utah's on manufacturing sector

electroindustry

Publisher | Tracy Cullen
Editor in Chief | Pat Walsh
Editor | Christine Coogle
Contributing Editors | Ann Brandstadter,
William E. Green III
Art Director | Jennifer Tillmann
National Advertising Representative | Bill Mambert

electroindustry (ei) magazine (ISSN 1066-2464) is published monthly by the National Electrical Manufacturers Association (NEMA), 1300 N. 17th Street, Suite 900, Rosslyn, VA 22209; 703.841.3200. Periodicals postage paid at Rosslyn, Virginia; York, Pennsylvania; and additional mailing offices. POSTMASTER: Send address changes to NEMA, 1300 N. 17th Street, Suite 900, Rosslyn, VA 22209. The opinions or views expressed in *ei* do not necessarily reflect the positions of NEMA or any of its subdivisions. The editorial staff reserves the right to edit all submissions but will not alter the author's viewpoint. Every attempt is made to ensure that information is current and accurate.

Subscribe to *ei* at www.nema.org/subscribe2ei.
Contact us at ei@nema.org.

Follow NEMA:     

ECO BOX

electroindustry magazine text and cover pages are printed using SFI®-certified Creator paper using soy ink.

- SFI fiber sourcing requirements promote responsible forest management on all suppliers' lands.
- SFI works with environmental, social and industry partners to improve forest practices in North America.
- The SFI certified sourcing label is proof that *ei* is using fiber from responsible and legal sources.



Certified Sourcing
www.sfi-program.org
SFI 00284



8

11

14

17

3

4

5

20

22

23

25

27

28

Demystifying Blockchains

Patrick Hughes, Senior Director, Government Relations and Strategic Initiatives, NEMA

Securing the Connected Environment

Jim Gilsinn, Senior Investigator, Kenexis Consulting

Joshua Marpet, Senior Vice President of Compliance and Managed Services, CyberGRC

Scott Lyons, Executive Vice President of Business Development, WarCollar Industries

Medical Imaging: A Pioneer in Interoperability

Andrew Northup, Director, Global Affairs, MITA

Cities Commit to Energy Efficiency

Katie Weeks, LEED Green Associate, Director of Communications,
Institute for Market Transformation

Comments from the President

Views

Electric News

Trends

Advocacy

Code & Standards

International

Business Analytics

Spotlight



**PULL AHEAD WITH
LABOR-SAVING
PRODUCTS.**

We get it. Every pull you make equates to time and money. That's why **Encore Wire** continues to develop labor-saving products that make you more efficient on any job site. From our spool-free PullPro®, to the industry's first self-spinning and 360-degree maneuverable Reel Payoff®, our products are designed with your bottom line in mind. Get your next job done quicker, safer and smarter with Encore Wire.



ENCORE WIRE®

**GET
WIRED
UP!™**

1.800.962.9473 | encorewire.com

© 2017 Encore Wire Corporation. All Rights Reserved. Encore is a trademark of Encore Wire Corporation.



FROM THE **PRESIDENT**

Have you ever fast-forwarded through commercials or turned off cable in favor of streaming a movie? Just as technological advancements increase consumer control over media consumption, new technologies enable consumer control of electricity consumption.

What was a vertically integrated electric system—with monopoly utilities owning the entire system from generation to transmission to distribution—began changing about 30 years ago, and the rate of change has increased since then. Beginning in the 1990s, deregulation allowed some customers to choose from whom they purchased electricity. Today, driven in part by cost reductions in solar photovoltaics, energy storage, and energy-efficient technologies such as LED lighting (which have come down in cost by 64 percent, 73 percent, and 94 percent since 2008, respectively), customers have more choices than ever, including generating and selling their own electricity.

A more fully engaged customer base profoundly affects electrical manufacturers by allowing those who participate the opportunity to buy and sell electricity on a local, transactional basis, further blurring the lines between utilities and consumers.

Some of these transactions will be facilitated directly by NEMA members' products. A recently announced project in Brooklyn, New York, for example, will be the first in the world to pair a microgrid with a peer-to-peer electricity trading platform using blockchain technology—a way to securely track and store information about the sale and purchase of electricity from distributed generation systems (see page 8). That microgrid will allow distributed generation owners to sell excess electricity—much of it from rooftop solar systems—directly to their neighbors.

As customers add more distributed energy resources to the grid, utilities will be challenged to monitor and control those resources. NEMA is partnering with the National Renewable Energy Laboratory as part of our strategic initiative on the Internet of Things to develop the NEMA CommTest to determine whether distributed resources can communicate with existing control systems before they are installed. It will enhance the operability, interoperability, and security of grid-connected devices.

New technologies are changing the face of the electroindustry and enabling increased customer choice and control over energy use, just as telecommunication technologies have shaped our media choices. NEMA will continue to innovate and evolve along with our members to catalyze the transition to the future of the electroindustry. 🌐

Kevin Cosgriff
President & CEO

officers

Chairman

Michael Pessina
Co-CEO & President
Lutron Electronics Co., Inc.

Vice Chairman

David G. Nord
Chairman, President & CEO
Hubbell Incorporated

Treasurer

David G. Nord
Chairman, President & CEO
Hubbell Incorporated

Immediate Past Chairwoman

Maryrose Sylvester
President & CEO
Current, powered by GE

President & CEO

Kevin J. Cosgriff

Secretary

Clark R. Silcox

Generous Donation for the Future of Electrical Safety

As we begin the new year, we thank the Electrical Manufacturers Club (EMC) for its generous \$30,000 donation to the Electrical Safety Foundation International (ESFI). This gift—the final act of the 110-year-old EMC—will allow ESFI to continue to promote the future of electrical safety while fulfilling its mission to “reduce electrically related injuries, deaths, and fires, saving lives and property through public education and outreach.”

Find out more about the work that ESFI does at www.esfi.org.

Enhancing, Coordinating, and Improving Security



Congressman Robert Latta represents Ohio's Fifth Congressional District. He is a member of the House Energy and Commerce Committee where he plays an integral role in crafting the nation's energy, telecommunications, environment, health care, and interstate commerce policy.

Our nation's energy infrastructure—and specifically our electric grid—deserves more attention in the coming year.

The private sector is rapidly innovating and finding ways to update our grid and make us less vulnerable as a nation to cyberattacks. We must also protect against adverse weather and accidents that could significantly impact our economy and threaten public safety. A massive blackout, even for a short amount of time, would have serious repercussions.

As Congressional Grid Innovation Caucus Co-Chair, I've advocated for investment in upgrading our nation's electric grid for a number of reasons, with security being the most important. Our electric grid's vulnerabilities increase the likelihood that terrorist groups or unfriendly foreign governments can exploit weaknesses and cause harm.

More than just security, we need an electric grid that is reliable and resilient for energy consumers. According to the U.S. Energy Information Administration, power outages cost Americans more than \$150 billion annually. That's why I've supported legislation empowering the Department of Energy, local and state governments, and the private sector to enhance coordination and improve emergency response and recovery. Keeping our electric grid up and running, and keeping us connected, should be one of our top priorities.

CONGRESS EYES NEW TECHNOLOGIES

Likewise, it is essential that we look at emerging technologies and assess them according to our roles as policymakers. One area that I've focused on in Congress is what the Internet of Things (IoT) will mean for our economy and our way of life. Simply put, IoT is using connectivity in everyday devices to send and transmit data. A common example might be wearables in a shirt or watch that can send information to your phone or a computer about a workout or your health.

The IoT offers plenty of opportunities, including the potential for adding billions of dollars to our economy. IoT could also revolutionize our transportation, manufacturing, agriculture, and healthcare sectors by sending and interpreting real-time data to aid in decision-making and improving efficiency.

However, as with any new technology, there are obstacles to be addressed. While many concerns focus on sensor technology and how to transmit information, what keeps me up at night is the susceptibility of devices to cyberattacks. Bad actors have already used IoT devices—in one case, security cameras—to carry out denial of service attacks and shut down large segments of the internet. At the same time, we must be vigilant and develop ways to protect sensitive data from groups trying to illicitly access it.

Connectivity is changing the way we live for the better, but it will continue to present obstacles that we must overcome as a nation. The discussion should begin now about how we address the most pressing concerns. ☎

Grid Modernization Leadership Council Forms

The Grid Modernization Leadership Council, a joint assembly of the Utility Products and Connected Systems divisions, held its inaugural meeting in conjunction with NEMA's 2016 Annual Membership Meeting in Cleveland, Ohio.

This council was established to accelerate the adoption of a modern electrical grid by providing guidance and recommendations on new consensus-based standards, advocating for favorable government relations policies and positions, developing and driving messaging and educational materials, promoting voluntary cybersecurity and supply chain risk standards, and participating in relevant future grid activities.

Members manufacture the power equipment, monitoring, and control systems that are building the modern North American electric grid. This grid uses information and communications technologies—such as advanced metering infrastructure, consumer involvement technologies, and high-tech sensors—to isolate problems, minimize disruptions, and repair disruptions automatically and remotely.

The modern grid also recovers more quickly from extreme weather outages, and optimizes the efficiency, reliability, diversity, security, sustainability, and affordability of electricity.

Modern grid solutions can improve grid performance and accommodate the integration of diverse energy generation resources through energy storage, microgrids, distribution automation, demand response, voltage and reactive power optimization, distributed energy resources, and more. These solutions allow energy-efficient buildings and homes to produce and to sell power to the grid and to each other and can accommodate a growing number of electric vehicles.

The council will do several things to pursue its mission to modernize the electric grid, which is essential for promoting safety, security, electric reliability, economic productivity, sustainability, and a diverse energy generation mix:

- Provide a collective industry voice on legislative and regulatory matters
- Establish NEMA positions and promote policies that are favorable to grid modernization at the international, federal, regional, and state levels
- Promote voluntary industry consensus standards and guidelines to address the operation of the grid and to minimize cybersecurity and supply chain risk
- Encourage open collaboration and drive common messaging among utility organizations such as the Edison Electric Institute, Electric Power Research Institute, National Rural Electric Cooperative Association, and American Public Power Association
- Share information and develop an understanding of grid-edge and other discrete grid technologies as they pertain to NEMA member companies
- Share information and develop an understanding of well-defined interoperability points characterized by agreed-upon standards
- Participate in future grid modernization initiatives such as those being led by the National Institute of Standards and Technology and the U.S. Department of Energy

For more information about the council, contact Steve Griffith (steve.griffith@nema.org). ☎

Steve Griffith, PMP, NEMA Industry Director, NEMA

See "Demystifying Blockchain," page 8
and
"Grid Connectivity to Rely on EV Charging," page 18

Committee to Address Life Safety in Integrated Building Systems

In response to the need to address the rapidly advancing practice of integrating multiple technologies and systems into one cohesive building system, NEMA's Fire, Life Safety, Security & Emergency Communication Section (3SB) formed the new 3SB Systems Committee.

communication systems) with other building technologies, including HVAC, elevators, and communications.

The committee seeks members to join this committee and the section, to provide valuable knowledge and subject matter expertise.

For more information, contact Denise Pappas, committee chair (dpappas@valcom.com) or John Schertel vice chair (john.schertel@apollo-fire.com). ☎



The committee will address the life safety aspects of integrating systems that encompass the inspection, testing, and maintenance requirements of life safety building technologies (such as fire alarms, security systems, and emergency

New Class N Pathway

Listen to Denise Pappas discuss the new Class N pathway that appears in the 2016 Edition of NFPA 72 *National Fire Alarm and Signaling Code* and its importance in the convergence of building systems for designers, installers, code officials, owners, and users of fire and life safety systems.

podcast.nema.org/the-new-class-n-pathway



SAVE THE DATE

Emerging Opportunities Forum

February 15, 2017

10am–4pm

Reception to Follow

National Electrical Manufacturers Association
1300 N 17th Street, 1st Floor Conference Center
Rosslyn, Virginia 22209

This is your chance to discuss and debate the merits of the proposed 2018 Strategic Initiatives and to hear from invited experts about select topics. All NEMA Members are invited to attend.

RSVP by February 1 to letitia.thompson@nema.org or 703.841.3240. ☎

NEMA Natural Disaster Alert System Responds to Regional Events

15 Named Storms



7 Hurricanes



3 Major Hurricanes

2016 Atlantic Hurricane Season

- Tropical Storm Colin, Hurricane Hermine, Hurricane Matthew
- NEMA & ESFI guidance documents distributed to key contacts
- NEMA social media sites provided information and resources
- NEMA member facilities contacted in the impacted regions



Landfall Storms

South Carolina: Tropical Storm Bonnie and Hurricane Matthew

Florida: Tropical Storm Julia, Tropical Storm Colin, Hurricane Hermine

Takeaways & Comments

- The NEMA Natural Disaster Alert System meets members' objectives.
- *Evaluating Water-Damaged Electrical Equipment* is the "go-to" standard.
- The ESFI infographics are highly effective for social media viewing.
- Alternative messaging reaches areas affected by multiple events in a quickly.
- Local media and contacts are valuable sources of real-time information.

East Tennessee Fire

NEMA Outreach / Guidance

NEMA's *Evaluating Fire- and Heat-Damaged Electrical Equipment* was distributed to key contacts in East Tennessee.

- NEMA Southern Region Field Representative registered with the International Code Council Disaster Response Network and FEMA Regional Mutual Aid Program
- No NEMA member facilities were affected

15,000
acres burned

700
damaged or
destroyed buildings



Patrick Hughes,
Senior Director,
Government
Relations
and Strategic
Initiatives, NEMA

Mr. Hughes
leads NEMA's
Strategic Initiatives
program to
accelerate the
future of the
electroindustry.

Demystifying Blockchain: How It Will Grow Demand for Distributed Energy Resources

You may have heard the buzz about using blockchain technology to facilitate energy transactions, especially for distributed energy resources. Unless you are a bitcoin user, however, you may not know what a blockchain is, or its relevance to the electrical system.

This article should help demystify the concept of blockchain and give you an idea of how it might facilitate increased deployment of distributed energy resources like solar photovoltaic systems, microgrids, energy storage, electric vehicles, demand response, and similar technologies.

Blockchain technology provides a way of securely recording transactional data. Let's say, for example, that Janie sold 100 kilowatt-hours of solar-generated electrons to Howard on January 3, 2017, at 1:46 p.m. for \$10. The feature that makes blockchain networks more secure than traditional centralized databases is that the information is stored on distributed computers and servers; there is no single database of transactions that could be tampered with.

This makes it nearly impossible for a hacker to alter the transaction, because doing so would require editing

thousands of “blocks” stored on thousands of different computers to successfully modify the information. Otherwise, disagreement amongst the distributed records would clearly identify transactions that had been altered.

In the energy sector, this offers a secure, low-cost, and high-speed platform for monitoring energy transactions. There are currently more than one million solar installations in the United States, and that number is expected to double within the next two years.¹ Many of those solar owners will be looking to sell excess generation. Today, most excess electricity is sold back to electric utilities; however, through local markets facilitated by blockchain technology homeowners will be able to sell excess electricity to whomever they want.

This scenario is not far-fetched, nor far off. Siemens and LO3 Energy recently announced a project based in Brooklyn, New York, where they are pairing a microgrid with a blockchain-based energy trading platform to facilitate the sale of distributed generation at the local level.² With this project in operation,

neighbors will be able to buy and sell electrons just as easily as they can buy and sell sports memorabilia on eBay.

“There is no question about where you got your kilowatt-hour, where it came from, and how it was produced,” said Lawrence Orsini, founder of LO3, in an interview conducted by *Renew Economy*.³ “I was skeptical that people would have an interest in where [their] energy [is] coming from, but Brooklyn shook that up a bit. [...] In Brooklyn, they want their electrons to be Brooklyn electrons.”

³ reneweconomy.com.au/why-sharing-solar-is-the-next-big-thing-in-energy-industry-33652



Blockchain Lexicon

Block: A record of a transaction that includes a link to a previous block, creating a chain. Blocks are stored on distributed networks of computers, making it nearly impossible to alter the transactional information.

Chain: A set of connected blocks that reference each other, allowing easy identification of altered blocks and making it nearly impossible to change a transaction (because a hacker would need to edit all subsequent blocks that reference the hacked block, and those blocks are stored on separate computers).

¹ www.seia.org/research-resources/solar-industry-data
² <https://www.siemens.com/press/PR2016110080EMEN>

Energy trading is not the only potential use case of blockchain technology in the electricity sector. Blockchain technology could be integrated with devices to facilitate payment for energy services, such as charging an electric vehicle or doing laundry. But before we get to that point, more pilot projects will be needed and some concerns will need to be addressed—especially related to privacy.⁴

One of the fundamental principles of blockchain technology is that records are publicly available, which increases transparency and security. Blocks must be visible to everyone in the network, because the veracity of a specific block is verified by checking it against all the other blocks in the chain.

This could cause some privacy issues. For example, Jesse could know how much electricity Kate is buying if the blockchain network is broadly accessible. However, access to the blockchain could be limited to a limited number of approved participants (this is the approach favored by some financial institutions), ameliorating some of the privacy concerns.⁵ It is also possible to

limit or encrypt the information included in the blocks, so that viewers would not have access to the names or addresses of market participants.

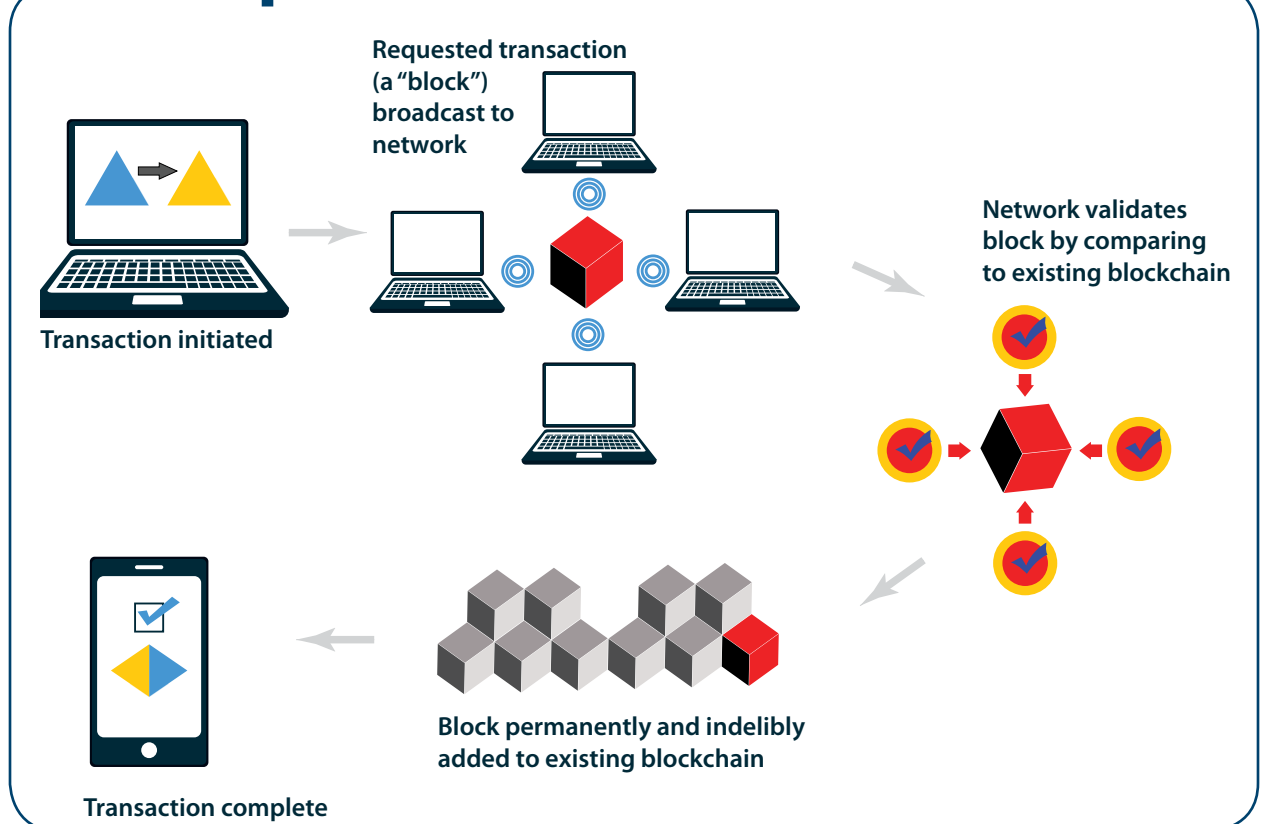
Assuming the privacy and other issues facing the widespread use of blockchain technology in the energy sector are resolved, blockchain networks have the potential to revolutionize how electricity and energy services are bought and paid for. Markets could be decentralized, and consumers could have full control over where their electricity comes from (at least financially). New markets for distributed electrons could spur investments in distributed energy resources, necessitating upgrades to distribution grid infrastructure. A shift from central-station to distributed generation could have implications for utility-owned assets, utility business models, and likely a plethora of unintended and unforeseen consequences.

Manufacturers should pay close attention to this trend over the coming years because, in one form or another, blockchain technology is going to impact your business. ☺

⁴ ieeexplore.ieee.org/document/7589035

⁵ www.ft.com/content/eb1f8256-7b4b-11e5-a1fe-567b37f80b64#axzz3qWZ8Giy1

Sample Blockchain Transaction





Securing the Connected Environment

Internet of Things (IoT) technology is included in an unprecedented and increasing number of new devices. From smart meters to light bulbs and refrigerators to thermostats, the prevalence of IoT devices continues to grow.

Many companies in the industrial control system (ICS) and supervisory control and data acquisition (SCADA) environment are trying to take advantage of the wave of development in this field, even creating terms such as “industrial IoT.” Due to the number of devices

already in the marketplace, the inexpensive nature of those devices, and the ubiquity of simple development kits for those devices, this growth rate is not likely to slow down anytime soon.

Unfortunately, security in many of these devices has not kept pace with the push to get functioning products to market. It is not that these organizations don’t know what security is or that it is an important issue, but, when it comes to security, raising the price of a 50- or 100-dollar device by 20 dollars to add complex security may not be justifiable.

Jim Gilsinn, Senior Investigator, Kenexis Consulting

Joshua Marpet, Senior Vice President of Compliance and Managed Services, CyberGRC

Scott Lyons, Executive Vice President of Business Development, WarCollar Industries

Continued on page 12

Continued from page 11

About the Authors:

Mr. Gilsinn co-chairs the International Society of Automation (ISA) 99 committee, which is developing the ISA/IEC 62443 series of standards.

Mr. Marpet is a board member for Security BSides Delaware, a pre-eminent information security conference.

Mr. Lyons is a graduate of the school of hard knocks. He has worked throughout the IT industry.

IoT and ICS/SCADA devices and systems are making use of more common platforms and environments that have exposed them to a wider variety of security threats than ever before. They are increasingly using common operating systems, network interfaces, software libraries, and communication protocols. This has been important for the reach of these devices and systems into a broader number of places, but it has also created a much larger attack surface.

While we are encouraged to keep computers and software up to date, IoT and ICS/SCADA devices have lifetimes of 10, 15, 20, or more years. The ability to upgrade many of these devices in place is not an easy process, so many are never upgraded once installed. Imagine trying to protect a DOS 6.0 computer controlling a chemical plant from the likes of Stuxnet¹ or other nation-state attacks. Connecting every device to the internet, including toasters, home electronics, and toilets may not be a good idea either.

However, there are some relatively simple steps that can be taken to secure both IoT and ICS/SCADA systems. For many, these steps may seem like commonsense IT practices, but when combined in devices and systems they can provide substantial gains in security.

The following are security steps and best practices that the authors believe should be applied to both IoT and ICS/SCADA. These steps should apply to all types of organizations, including device vendors, system integrators, contractors, and end users.

ARCHITECT FOR SECURITY

The earlier security is introduced into the design process of a device or system, the earlier a design issue can be addressed to improve overall security. Designing for security may also improve overall reliability and performance of a device, since hardening a device often involves thinking about the core functionality that is needed and stripping away extraneous pieces.



The same can be said for systems. Going through the process to design a system securely will often provide many side benefits to network architecture and segmentation, system interactions, and incident response.

SEGMENT NETWORKS

Segmenting the network where IoT and ICS/SCADA devices are connected goes hand-in-hand with architecting the system for security. Creating a number of small segments inside a network may seem like more work, but it often provides better security, easier maintenance, and more robust networks. The benefits to network segmentation include the following:

- **Reducing network load:** IoT and ICS/SCADA devices do not generally have as much processing power as normal computers. When the amount of network traffic they see is reduced, they are not forced to process the extra traffic not intended for them.
- **Reducing incident impact:** Segmenting traffic allows an organization to isolate parts of their network in response to an incident, containing the spread and allowing the process to continue, albeit in a reduced capacity, until the incident has been resolved.
- **Providing monitoring points:** Monitoring the network for anomalies is important, and that means that there need to be well-defined locations in the network where monitoring can take place. Network segmentation provides natural collection points through which traffic can be routed, providing easier monitoring.

¹ The computer worm Stuxnet is believed to have been created by U.S. and Israel in 2009 to sabotage Iran's nuclear facilities.

UNDERSTAND DATA TYPES AND FLOWS

Knowing what data should flow through a network, where that data typically goes, and what or who should be able to access it allows an organization to better identify potential malicious activity.

IoT and ICS/SCADA networks are relatively static in the amount and types of data that they send and receive. They follow regular patterns, for the most part, and only communicate with a small subset of other devices. This is both for the real-time communications related to the process and the non-real-time communications related to things like maintenance, programming, historical data collection, and user interface.

When new communication paths are introduced or actions occur that are outside the norm, alarms should go off to indicate that something may be wrong. It may be nothing more than an out-of-band task by a valid user or a component malfunction, but it could just as easily represent malicious activity that needs to be investigated.



MONITOR DEVICES AND SYSTEMS

It does no good to provide the best security in the world without monitoring that security in some way. For example, a physical security system installed in a building is only as good as the response time by the security company in the event of an incident. If no one is monitoring the system, then it is effectively rendered useless. The same can be said for IoT and ICS/SCADA devices and systems.

Devices need to be designed to allow centralized monitoring of their performance, network statistics, core functionality, and security features. End users need to configure monitoring systems to collect log and event information from as many devices as possible and report that information. At first, this will lead to a large number of false positive results, so the system will take time to tune. Once tuned, it should remain stable for long periods of time since IoT and ICS/SCADA systems don't change often.

CHANGE DEFAULT PASSWORDS

Default passwords are very useful for both vendors and users in order to quickly configure a device from its out-of-box state. Users know when they get a device that it will have a certain set of parameters, allowing them to more easily create setup procedures and automation scripts. Issues arise when users choose not to change those default passwords or vendors either don't provide an easy mechanism to change default passwords or include hard-coded passwords in their devices.

The recent Mirai botnet that crippled the website of Brian Krebs² and took down Dyn³ are good examples of how not changing default passwords affect others. More than 300,000 IoT devices using default or weak passwords were used to create nearly 600 Mbps of traffic to the different sites being affected because someone figured out a way to get all of those devices to launch an attack simultaneously.

² <https://krebsonsecurity.com/2016/09/krebsonsecurity-hit-with-record-ddos>

³ <https://dyn.com/blog/dyn-statement-on-10212016-ddos-attack>

Continued on page 14

Continued from page 13



HARDEN DEVICES

A term used in security is the M&M security model. It means to create a hardened shell surrounding a sweet target inside.

At one time, this model worked. Hackers tried to brute-force their way through the outer defenses trying to reach the protected systems. A harder shell meant more protection. Attackers' tactics have changed over the years, since they couldn't easily break through the

outer defenses. They now look for entry points that take them directly inside the shell into the protected and, more important, trusted environment.

Hardening the devices on the inside of your network helps to prevent systems from being compromised if someone does manage to make it into the protected environment. Hardening usually consists of turning off unused applications, network ports, and services if they are not needed. In order to do that, end-users need to understand how those devices will be used, and vendors need to provide mechanisms to turn off those applications, ports, and services.

For example, almost all IoT and ICS/SCADA devices have an Ethernet or wireless connection that is often used for configuration and diagnostics, but is not necessarily required for functionality.

Medical Imaging: A Pioneer in an Interoperable World

Interconnectivity, interoperability, and the Internet of Things (IoT) are buzzwords more likely used in reference to an internet network or home theater system rather than medical imaging. However, the Medical Imaging & Technology Alliance (MITA), NEMA's medical imaging division, has been and continues to be a pioneer in connectivity and interoperability.

Digital networks—devices connected to each other over the internet—rely on a basic principle: once you define the “how” and the “what” between devices, anyone willing to design and manufacture devices that communicate just has to use the same definitions.

The first practical, real-world application of the IoT was in the hospital radiology department. The first imaging scanners capable of transmitting information digitally were only capable of being networked—that is, connecting to, communicating with, and understanding other digital devices—with equipment from the same manufacturer. Manufacturers soon realized that the costs far outweighed the benefits and, through MITA, published the first digital interoperability standard, Digital Imaging and Communications in Medicine (DICOM), in 1985.

When possible, these types of services should be turned off, or at the very least, administrative access should be locked down in some way.

UPDATE DEVICES

Updating systems, where possible, to keep up with recent functionality and security improvements is an important step that often gets overlooked for various reasons. In most cases, it's just that end users do not plan for updating when they architect their system. It can also be due to the complexity of managing updates in different environments.

As networks are segmented to protect them from external attacks, updating devices becomes more of an issue. Devices can no longer pull updates directly from a vendor's website. Another mechanism needs to be developed by the vendor in order to accomplish

updating on isolated network segments. Many operating system and antivirus vendors have found a solution to this in corporate environments by creating localized update servers.


The same pulling mechanism can be used by the end devices; however, instead of pulling them from the internet, they are pulled from the local server. That way, the updates can be brought into the protected environment in a secure manner and tested before being implemented in the production environment.

Continued on page 16

By defining the necessary characteristics of files to be exchanged and the method by which they would be transmitted between devices, DICOM entered the "what" and the "how" into the digital equation. DICOM set the "what" (the file format) and the "how" (the data transmission protocols), freeing manufacturers and developers to focus on innovating for the sake of public health.

Anyone willing to follow DICOM's rules for digital interoperability could manufacture magnetic resonance imaging (MRI) and computed tomography (CT) scanners, ultrasound machines, image viewing systems, healthcare data storage devices, workstations, and peripherals such as printers that could communicate with each other over the internet. DICOM introduced the world to interoperability, starting with CT and MRI scanners, and unleashed the digital revolution that has transformed nearly every aspect of life over the past 30 years.

How interoperability will change our lives in the next 30 years is impossible to know. However, the past can give us valuable perspective. Think back to the days of the newfangled incandescent light bulb in its novel Edison base, or plugging a transistor radio into an electrical outlet. Consider that not long ago retrieving the results from your x-ray scan meant someone had to bring you the images on 10" x 12" sheets of film from wherever they were stored to wherever you needed treatment.

Challenges like data privacy, cybersecurity, and network reliability are—and must remain—a top concern for governments, industry, and consumers alike. But if the past teaches us anything, it's that connectivity breeds innovation, innovation leads to more innovation, and that exciting, world-changing potential is never far off. 

Andrew Northup, Director, Global Affairs, MITA

Continued from page 15

“KNOW THE ENEMY AND KNOW YOURSELF”

These words of wisdom come from Sun Tzu, whose classic *Art of War* was written in the fifth century BCE.

It is important to try to stay as informed as possible. Keep track of security news. There are multiple websites, blogs, news sources, and government agencies that have news feeds related to security in different industries. Develop a list of a few different trusted news sources that can easily be scanned each day for issues that may affect an organization. It is important to understand what risks an organization and its devices and systems possess, the consequences of an incident, and the reasons someone may attack an organization.

In addition to understanding the current situation, it is important to try to understand what potential solutions may be coming to help mitigate the risks. New technologies are being developed every day. Understanding how these new technologies can potentially be applied is important so that an organization can properly plan for them and architect their systems when they make the choice to implement those technologies.



PLAN TO TEST, TEST THE PLAN

Testing is a well-established step in many ICS/SCADA organizations. Factory acceptance testing (commonly known as FAT), site acceptance testing (commonly known as SAT), commissioning, startup validation, etc., are all regular steps in bringing any plant online or deploying a new system. Similar steps are usually conducted by vendors with unit testing, integration testing, and final certification.

Security testing should also be an integral part to each of these steps. In addition to pre-testing the devices and systems, they should also be tested in situ

periodically. Whether it is during a plant shutdown, or on a test system, security functional testing should be conducted on a regular basis against the running configurations in order to ensure that vulnerabilities have not been introduced into the system inadvertently or intentionally. It is important to also consider third-party assessments conducted by an organization familiar to the risks associated with the operating environment.

Proactive Preparation and Response

These low-cost, effectively zero-barrier-to-entry devices are amazingly capable, useful, and fantastic to use to prototype processes, control types, and other bleeding-edge applications. But when those processes go to a production environment, a hardened, industrial-grade system should be in place.

Under the premise that IoT will never be in the production hardened environments we deploy using industrial-grade ICS/SCADA components, why do we need to worry about IoT security? Because many of the same mitigations will work to add security maturity to ICS/SCADA environments, and those IoT devices will be put in those hardened environments in the near future. Better to architect it properly the first time than to wait for potential consequences. ☎

Questions to Ask Your IT/ Security Organization

1. Was security considered during the design process?
2. Are the IoT/ICS/SCADA devices on a separate network segment?
3. Has a network baseline been conducted?
4. How often are performance/security logs monitored?
5. When was the last time a password audit was performed?
6. Have the systems been hardened?
7. Has an asset inventory been developed? When was it updated?
8. Are people updating their knowledge and skills?
9. How are devices and systems tested before integration?



Cities Commit to Using Energy Efficiency to Support Jobs and Local Economies

In nearly every major American city, buildings consume more energy than any other end-use sector, costing Americans more than \$400 billion in annual energy bills. However, studies have shown significant potential to save energy and money by increasing building energy efficiency while also creating jobs and boosting local economies. The knowledge and technology exist to make buildings vastly more efficient, and increasingly cities are stepping up to lead the charge toward unlocking these benefits.

Recognizing this potential, in November 2016, 10 new cities joined the City Energy Project (CEP), a multiyear, national initiative to create healthier and more prosperous cities by improving the energy efficiency of large buildings. A joint initiative of the Institute for Market Transformation (IMT) and the Natural Resources Defense Council (NRDC), the project is now working with 20 participating cities to craft and deploy suites of energy efficiency programs and policies that are tailored to local market needs in order to maximize effectiveness. Together, the potential impact is huge: by 2030, the 20 participating cities have the power to save more than \$1.5 billion annually in energy bills and reduce carbon pollution by more than 9.6 million metric tons, equivalent to taking two million cars off the road for a year.

New additions to the project include Des Moines, Iowa; Fort Collins, Colorado; Miami-Dade County, Florida; New Orleans, Louisiana; Pittsburgh, Pennsylvania; Providence, Rhode Island; Reno, Nevada; San Jose, California; St. Louis, Missouri; and St. Paul, Minnesota.

They join 10 pioneering cities who signed on to the project in January 2014: Atlanta, Georgia; Boston, Massachusetts; Chicago, Illinois; Denver, Colorado; Houston, Texas; Kansas City, Missouri; Los Angeles, California; Orlando, Florida; Philadelphia, Pennsylvania; and Salt Lake City, Utah.

Each of the first 10 CEP cities has launched innovative, building-focused policies and programs that drive investments in energy-efficient technologies and systems, with a number of these efforts also addressing water efficiency. Six of these cities joined a growing trend to increase market awareness of how buildings are using energy by enacting energy transparency policies covering almost 12,000 buildings totaling more than 2.3 billion square feet.

Katie Weeks, LEED Green Associate, Director of Communications, Institute for Market Transformation

Ms. Weeks has a Master's degree in sustainable design studies. Prior to joining IMT, she was the chief editor for sustainability at Hanley Wood Media.

Continued on page 18



Grid Connectivity to Rely on EV Charging

The electric grid has changed, but the change isn't finished. With state and federal requirements to incorporate more renewable energy—primarily wind and solar—as part of our power generation mix, the grid must also incorporate a massive amount of energy storage to continue to provide stable and low-cost power. Electric vehicle (EV) charging is an excellent contributor to the suite of energy storage we'll need for connectivity in the future grid.

The U.S. grid provides electricity with exceptional reliability—notwithstanding sporadic power outages—at a relatively modest price. It balances power generation precisely with a multitude of loads, but has almost no reservoir of energy storage. The grid can do this because of load balancing.

Renewable energy sources such as wind and solar are generally unpredictable and can't be ramped up (dispatched) if the grid's load changes. If the grid uses traditional power generation to compensate for the fluctuations of renewable energy, the cost advantages of the renewables is lost.

That's where energy storage comes in. Grid-scale energy storage techniques include pumped hydro, which uses gravitational potential to pump water from a lower elevation to a higher one to cover peak demand; compressed air, which is similar to pumped hydro; and grid-scale batteries that store electricity at off-peak periods to cover peak demand.

The problem with these technologies is that they are expensive, in terms of capital investment and operating costs. They also have an inherent roundtrip energy efficiency loss. If the grid can use EV charging for energy storage, the cost and roundtrip efficiency loss problems go away. The idea is to charge an EV in a conventional manner, but with grid intelligence to compensate for fluctuations and non-dispatchable renewables.

With EVs as a small percentage of all the vehicles on the road today, the potential for them to provide meaningful grid services just isn't there. But when EVs reach 10 percent, 25 percent, or even 100 percent, the value of EV charging to the grid may overshadow every other type of grid storage.

Most advantageously, since people will buy EVs to drive anyway, the storage cost is almost nothing. Ⓔ

Charles Botsford, PE, Chemical Engineer, AeroVironment



New Orleans

Continued from page 17

Additionally, more than 1,600 buildings in these cities, representing more than 270 million square feet of space, have voluntarily joined in CEP-supported challenge programs encouraging energy efficiency improvements and recognizing leadership. Many of the pioneering 10 cities are exploring new financing models that will make over \$1 billion available to finance energy efficiency improvements.

Participating cities hope to catalyze building retrofit markets by making data, information, and financing available, while engaging citizens and educating people about the benefits of energy efficiency to power demand for high-performing buildings. More efficient buildings create a win-win scenario for cities and their residents and businesses.

Policies such as benchmarking and transparency programs encourage better knowledge of how buildings are performing, recognizing that you can't manage what you don't measure. Retrofitting buildings, which is strongly supported by the policies and programs of the CEP, incorporates new technologies and creates jobs at all skill levels. Reducing operating expenses by improving building efficiency frees up money currently spent on utility bills, so that it may be put back into local economies.

New financing models make it easier to invest in efficient, new equipment, while setting up market drivers that encourage innovation in the development and adoption of new technologies.

To learn more about the efforts of the CEP, visit www.cityenergyproject.org. Ⓔ




U.S. Cities Enact Building Efficiency Legislation

Over the course of two weeks in December, four cities became the newest additions to a diverse cadre of municipalities that have adopted building energy benchmarking and transparency policies.

Los Angeles, Denver, Orlando, and Evanston (ranked in order of population) joined more than 20 cities, counties, and states that now require large and public buildings to measure their energy performance with ENERGY STAR® Portfolio Manager and publicly disclose that information. This transparency encourages building owners with low energy scores to upgrade their buildings to remain competitive in the marketplace.

Studies have found that energy service companies in New York City and San Francisco reported a 30 percent increase in energy efficiency projects after benchmarking and transparency laws were put in place. In California, 62 percent of building owners that benchmarked their properties invested in energy-efficiency improvements, while 84 percent either planned on improving or had already improved their energy performance after benchmarking.

A separate survey conducted on behalf of NEMA found that 77 percent of New York City facility managers made changes to how they operate their buildings as a result of New York's benchmarking policy, and 75 percent invested in new energy-efficient equipment like lighting systems, building controls, heating and cooling systems, and plug-load controls.

NEMA has worked diligently over the past few years to support local building energy benchmarking and transparency ordinances, because they increase adoption of energy-saving technologies and support manufacturing jobs in the United States. Los Angeles, Denver, Orlando, and Evanston are leading examples of cities promoting energy efficiency in buildings as a way to boost their local economies, and we encourage all other cities, counties, and states to follow their lead. 

Patrick Hughes
Senior Director,
Government
Relations and
Strategic Initiatives,
NEMA



Los Angeles

Data Center Colos Respond to Need for Flexibility and Speed to Market

As data center power distribution equipment evolves to address the changing needs of data centers, it is growing and becoming more competitive.

Underlying drivers such as the Internet of Things, cloud-based applications, rapidly growing video storage and transmission, and the migration of media from cable to streaming are driving double-digit annual growth in storage and computing capacity.

In 2015, enterprises saw a tipping point, as many changed their business models to make their offerings available through the cloud. Companies that had previously resisted offering their products through the cloud realized that they had to embrace delivery of their offerings in a cloud-based model, especially as usage on mobile devices surpassed usage on PCs.

One growing area for competition is the colocation (colo) space. A colo is a type of data center that bundles space, cooling, electrical power, computing and storage equipment, bandwidth, and physical security to retail customers who often provide their own servers and storage. Some colos may also offer managed services.

The market has become more competitive. Many new entrants are competing in the colo space, relative to 2012–2013 when the model was getting established. Many went public in 2013–2015 to tap into the capital markets for expansion. As the model gained acceptance in Europe, Latin America, and Asia, colos globalized. U.S. colos are acquiring competitors in Europe and Asia to rapidly build their global footprint and be able to serve multinational customers. Some Asian and Latin American telecommunications companies and colos are expanding into the United States, viewing it as a high-growth market.



Evolution of Technology and Offerings

Manufacturers have introduced various innovations in recent years to address data center customers' needs.

Static transfer switch (STS) manufacturers:

- Enable a capture of downstream branch circuit monitoring and have the STS serve as a hub, thereby providing a low-cost monitoring option outside the building management system
- Offer higher-ampere STSs as power requirements are increasing

- Offer line-and-match with a higher power distribution unit (PDU) since power requirements are increasing
- Provide more contractor-friendly installations to reduce installation time and cost and decrease time to market

PDU manufacturers:

- Introduce higher-power products in small footprints
- Compartmentalize low- and high-power sections
- Provide full front access for more efficient maintenance, including supporting infrared scans of

transformer bus bars from the front by welding bus bars and avoiding hidden bolted connections

- Provide flexibility in service entrances for line and load connections from the top or bottom of the PDU
- Provide more sub-feeds than earlier-generation products
- Provide multi-output transformers so that secondary voltage can be changed within minutes, if a colo needs to change between 208/400/480V applications to meet customer needs
- Incorporate intelligent power monitoring

Anand Krishna	Mingbo Zhao, PhD	Vlad Gulkarov	Dave Mulholland
Vice President for Business Development, PDI	Vice President of Engineering, PDI	Director of Engineering, PDI	Vice President of Service, PDI

As practices to run colos efficiently became widely disseminated from 2014 to 2015, it became harder for the players in the top quartile to differentiate themselves. One differentiator is speed to market. Driven by the rapid growth in storage and computing requirements, as well as by the widespread acceptance of the outsourcing model around the world, colos are building and deploying data center capacity rapidly, increasing asset efficiency, and reducing operating expenses. At the same time, the time interval from spending capital to generating cash flows is reduced. As the colo supply market has become more competitive, even privately owned colos and real estate investment trusts (REITs) have to compete for capital to a greater extent than in 2010–2013.

In order to increase their return on capital to ensure stock price growth and to be able to attract capital, privately owned colos maximize efficiency from capital spending by squeezing more rack capacity out of a given amount of floor space, reducing energy consumption (i.e., increasing their power usage effectiveness), and optimizing the skill level required for various tasks (e.g., not employing certified electricians when equipment can be engineered to enable work by less skilled personnel).

As the supply market becomes more competitive, business models become less distinct. The lines increasingly blur between offering only space, power, and cooling versus offering value-added services.

Colos want equipment that enables them to cost-effectively tailor their offerings for the businesses that they win. As some colos go global, for example, they try to determine the extent to which they can cost-effectively standardize equipment and designs across continents to accommodate different output voltages.

Safety regulations are increasingly stringent: colo and enterprise data centers must comply with OSHA guidelines and with arc-flash and safety guidelines. Colos want to be able to comply with safety guidelines without having to deploy their most expensive personnel more often than necessary. They also want to minimize negative productivity impacts due to having to don personal protective equipment for all maintenance activities. Furthermore, U.S. colos that expand into Europe have to meet European regulations and guidelines. ☞

Remote power panel (RPP) manufacturers:

- Engineer products that are very flexible, i.e., that can be configured in any of multiple wall and floor mount options using a unit with a 12" x 24" footprint
- Have very flexible panelboard distribution with multiple manufacturers and styles to maximize flexibility in deploying branch circuits
- Isolate low- and high-power compartments
- Incorporate intelligent power monitoring
- Adapt service entrances, e.g., top/bottom entry/exit that are changeable in the field

- Prevent error by using trapped key interlocks to ensure that users follow the correct sequence to switch power sources when using the RPP as a mission-critical unit

Overhead busway manufacturers:

- Engineer products to allow additions of tap-off boxes (from which power is dropped to server racks) in live systems
- Increase the power that can be dropped from each tap-off box
- Reduce the space taken up by the coupler that joins two rails to reduce the length of rail that is unavailable for tap-off boxes

- Engineer an open-channel design that eliminates energy-wasting hot spots commonly found in electrical cable congestion points
- Qualify their hardware for 60° C environments

Power distribution manufacturers facilitate retrofit and reuse by offering monitor upgrades by adding branch circuit monitoring systems for equipment already in place and offering pre-engineered monitoring solutions with installation speed as a key design criteria. ☞

Utah Roundtable Focuses on Manufacturing Sector



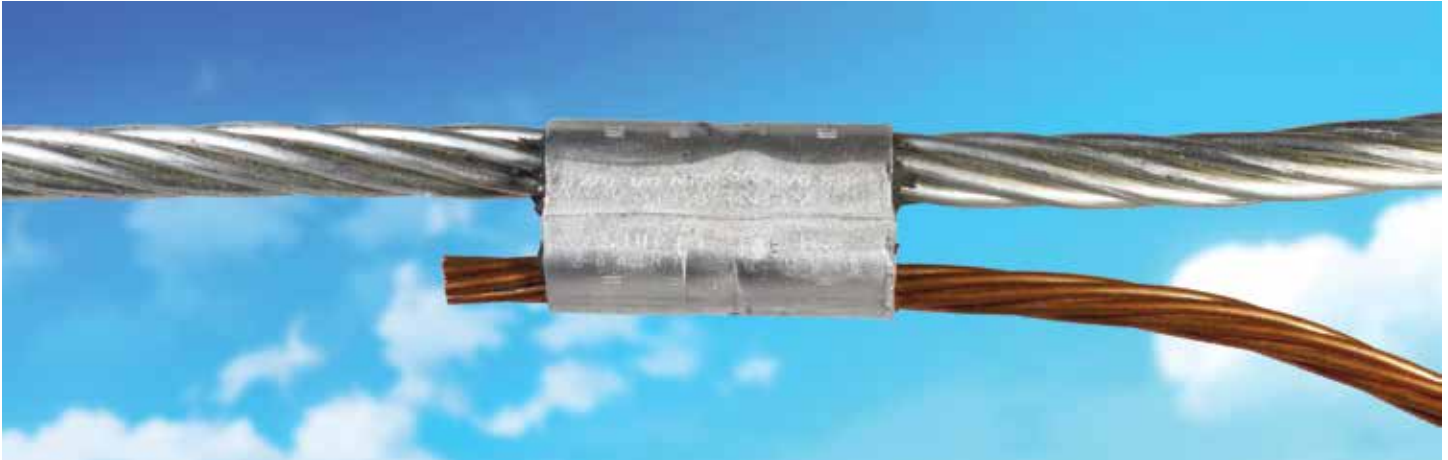
Pictured above at the meeting are Bryce Morris of Siemens, NEMA President and CEO Kevin J. Cosgriff, Scott Hansen of Cerro Wire, Jason Eubank of Huntsman Corporation, Reid Cram of Vantage Controls, Gov. Herbert, Harold Jepsen of Vantage Controls, Anna Pavlova of Schneider Electric, Mike Houston of Acuity Brands, Lindsay Stovall of American Chemistry Council, and Dan Finnegan of Siemens. Photo by Jeff Skalla

A recent industry roundtable with Utah Governor Gary Herbert (center), whose leadership has elevated the state as a hub for advanced manufacturing, provided an opportunity for industry leaders to share success stories and provide recommendations to help advance the governor's efforts to prepare and train Utah's future workforce, increase market access, and grow a diverse energy portfolio.

NEMA member Vantage Controls, founded in Governor Herbert's hometown of Orem, hosted the event at a new facility where many of its energy-efficient products are designed and manufactured.

Governor Herbert reiterated his commitment to supporting the electroindustry and his administration's goal of growing and expanding the state's manufacturing sector 🇺🇸

ANSI C119.4 Updates Requirements for Connectors



With the support of NEMA's Electrical Connector Section, the ANSI C119 Accredited Standards Committee (ASC) for Electrical Connectors recently revised ANSI C119.4-2016 *American National Standard for Electric Connectors—Connectors for Use between Aluminum-to-Aluminum and Aluminum-to-Copper Conductors Designed for Normal Operation at or below 93° C and Copper-to-Copper Conductors Designed for Normal Operation at or below 100° C*.

Extensive editorial changes were made to the standard, which covers electrical and mechanical requirements for connectors used to make connections between aluminum-to-aluminum, aluminum-to-copper, and copper-to-copper conductors on distribution and transmission lines.

Significantly, testing methods and equipment requirements were removed, since all testing methods and equipment are now addressed in the new ANSI C119.0-2015 *Testing Methods and Equipment Common to the ANSI C119 Family of Standards*, a complimentary copy of which comes with ANSI C119.4-2016. The remaining performance standards and requirements unique to the C119.4 standard were reorganized under a new numbering format.

This revision also includes the addition of an optional set of performances requirements: shunt class connector devices in Annex E. The ANSI C119 SC4 subcommittee provided these requirements as a reference in response to users who have requested guidance for testing shunt devices.

This connector standard is the first of the ANSI C119 series to be published in the new format with the common tests now contained in ANSI C119.0 *Testing Methods and Equipment Common to the ANSI C119 Family of Standards*.

Aluminum-to-copper connector. Courtesy of Burndy



Aluminum-to-aluminum connector. Courtesy of Hubbell Power Systems

The ANSI ASC C119 committee develops and maintains standards for overhead connectors, sealed insulated underground connectors, insulation-piercing connectors, and non-sealed multiport connectors systems, and is also working on a new high-temperature utility connector standard. It actively seeks additional membership from the user and general interest membership categories in order to provide proper balance among the participants.

If you are interested in applying for membership, contact Paul Orr at pau_orr@nema.org. ●

West Coast Acts on National Codes



With the publication of the 2017 *National Electrical Code*® (NEC) in September 2016, code adoption activity has begun in several states in the West Coast region.

The Idaho Electrical Board voted in July to recommend the adoption of the 2017 NEC. This recommendation will be forwarded to the state legislature to be considered during its next session. Recommendations for the adoption of the 2015 International Code Council codes (I-Codes) also were forwarded to the legislature. If approved, the 2017 NEC and the 2015 I-Codes will go into effect in Idaho in July 2017.

Oregon began its adoption cycle for the 2017 NEC. The period to submit public comment on amendments closed on October 15. The state's Electrical Code Review Committee has meetings scheduled to review the changes in the 2017 NEC, as well as all submitted public proposals. The projected effective date for the 2017 NEC with Oregon amendments is October 2017. Other code review committees are considering the adoption of the 2015 I-codes on a similar timeline as the NEC.

Washington has begun its adoption cycle for the 2017 NEC. The public comment period closed on October 31, 2016, and the state Electrical Technical Advisory Committee met on December 14 to review 2017 NEC changes and proposed amendments. The projected effective date for the

2017 NEC in Washington is July 1, 2017. A separate agency, the Washington State Building Code Council, adopts all other codes. The 2015 I-Codes became effective in Washington on July 1, 2016.

Hawaii held a public hearing on December 8, 2016, to finalize the adoption of the 2014 NEC and the 2015 *International Energy Conservation Code*® (IECC). Hawaii is currently using the 2008 NEC and the 2006 IECC. With the adoption of the 2014 NEC and 2015 IECC, they will skip over the 2011 NEC, as well as the 2009 and 2012 editions of the IECC. The effective dates for these codes will be in early 2017.

NEMA members are well aware of the rapid pace of technological change in the electroindustry. The 2017 NEC recognizes this with the addition of five new articles, including ones on utility scale photovoltaic installations, microgrids, and energy storage. Several states that adhere to older codes, including California and Nevada, and individual jurisdictions such as Las Vegas and Los Angeles County are considering adopting parts of the 2017 NEC to allow for new technologies to be safely installed.

As always, NEMA is directly involved in all of these code adoption activities and promotes NEMA member interests during public hearings and comment periods. ☎

Recently Published Standards

ANSI C84.1-2016 *American National Standard for Electric Power Systems and Equipment—Voltage Ratings (60 Hz) establishes nominal voltage ratings and operating tolerances for 60 Hz electric power systems above 100 V.* It is available in hard copy or electronic download for \$88 on the NEMA website.

NEMA 107-2016 *Methods of Measurement of Radio Influence Voltage (RIV) of High-Voltage Apparatus* covers the methods of measurement of radio influence voltage in the frequency

range of 0.015 to 30 MHz that may be associated with high-voltage power apparatus used on transmission and distribution systems at line voltages of 0.6 kV and above. It is available in hard copy for \$67 or as an electronic download at no cost on the NEMA website.

NEMA SG-AMI 1-2009 (R2015) *Requirements for Smart Meter Upgradeability* defines requirements that include secure, local, and remote upgrades of smart meters. It is

available in hard copy for \$63 or as an electronic download at no cost on the NEMA website.

NTCIP 1103 v03 *Transportation Management Protocols (TMP)* was published as a joint effort with the American Association of State Highway and Transportation Officials and the Institute of Transportation Engineers. This revision incorporates expedited functionality. It is available in hard copy or as an electronic download for \$175 on the NEMA website. ☎

DITTA Report Underlines Commitment to Cybersecurity

DITTA, the global voice for the diagnostic imaging, radiation therapy, healthcare information communication technology, electromedical, and radiopharmaceutical industry, reemphasized its commitment to cybersecurity in the recently published report, “Cybersecurity of Medical Imaging Equipment.”

DITTA builds on the cybersecurity white paper MITA’s MII Section published in November 2015 and will raise awareness and highlight the increasing importance cybersecurity holds for our industry.

This publication comes at a time when breaches in security may have compromised patient safety and confidentiality of patient data.

According to DITTA Chair Satoshi Kimura, “The medical imaging equipment industry takes its responsibilities in cybersecurity very seriously. The insights delivered by big data analysis are placing us at the threshold of major advances in care. If we are to realize this opportunity, then stakeholders must be convinced that their personal data is being handled safely and securely.”

He stressed that DITTA would act as a resource for cybersecurity standards and regulations in the sector, in collaboration with IT professionals and regulators and professional organizations that represent medical imaging.

The DITTA white paper sets out the principles of current best practices for manufacturers and suppliers. It stresses that responsibility for cybersecurity cannot lie with a single stakeholder. Manufacturers and hospital IT departments need to work hand-in-hand to implement these approaches.

This paper also points to security risks from increased connectivity. Medical imaging equipment, in line with all computer systems, is increasingly networked through hospital intranet and the internet. This poses its own security risks in the form of network intrusions.



The report strongly recommends establishing clearly defined processes for effective cyber prevention and training all relevant staff to implement and maintain them effectively.

The paper is available for download at globalditta.org/wp-content/uploads/2016/11/ditta-cybersecurity-paper-29-Nov.-2016-final-clean.pdf 📄

NEMA: Engaged on Trade

U.S.-CANADA-MEXICO TRADE

President-elect Donald Trump has called into question the 1994 North American Free Trade Agreement (NAFTA) and proposed renegotiation of the pact. In November and December, NEMA increased the pace of consultations with member companies and counterpart organizations about the future of trade in North America and how the agreement could be improved. According to U.S. government statistics, Mexico and Canada, respectively, remain the top two destinations for U.S. exports of products within NEMA's scope. ☎

RENEWABLE ENERGY AND ENERGY EFFICIENCY ADVISORY COMMITTEE



Jonathan Stewart participated in the first meeting of the Fourth Charter of the Department of Commerce's Renewable Energy and Energy Efficiency Advisory Committee on December 1, 2016.

Three panels of government officials representing every federal agency involved in promoting exports of power generation and electrical equipment briefed the committee, which is made up of representatives

from U.S. businesses and trade associations. Panel members encouraged the committee members to use U.S. government resources to inform its recommendations for export growth.

With the new administration assuming office this month, the committee decided its first action would be a letter to President-elect Trump and his nominated Secretary of Commerce Wilbur Ross to explain the domestic renewable energy and energy efficiency industry. The letter will highlight job growth, revenue, and other economic strengths. ☎

IMPORT COMPLIANCE AND ENFORCEMENT

This month, NEMA is launching a strategic initiative aimed at improving U.S. efforts to enforce compliance with product regulations and intellectual property rights. The first step will be a survey of members to gauge the scope and magnitude of the problem posed by non-compliant imports.

The results of the survey will be used by a council of member company representatives to determine priorities and advise U.S. Customs and Border Protection and U.S. regulatory agencies. ☎



WTO ENVIRONMENTAL GOODS AGREEMENT

The Trump administration is poised to inherit negotiations launched in 2014 aimed at eliminating import tariffs on products with environmental benefits.

A ministerial meeting at the World Trade Organization (WTO) in Geneva, Switzerland, in December failed to bridge differences between China and the other 16 negotiating parties—including the United States, the European Union, Japan, and

Korea—on what types of products should be included the Environmental Goods Agreement (EGA).

NEMA and the China Association of the Lighting Industry (CALI) have advocated for inclusion of LED lighting. In other product areas within NEMA's scope, however, China has opposed using the EGA to reduce its tariffs. ☎

Pro-Business Tilt Boosts Confidence

NEMA's Electroindustry Business Conditions Index (EBCI) panel members, all of whom responded to the November survey after the election results were known, pushed the current conditions index further into positive territory, moving it from 55.6 in October to 57.9. While a relatively small share of our panel, 11 percent, rated conditions worse in November, it marks an increase over the six percent responding similarly in October.

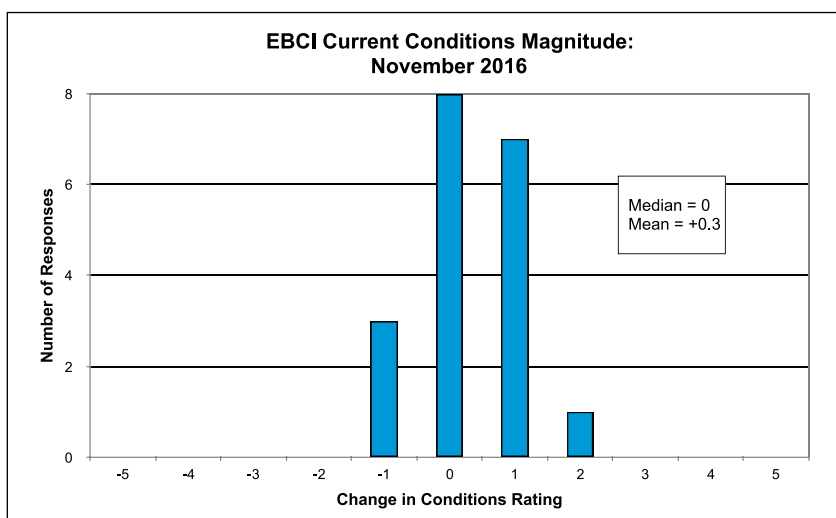
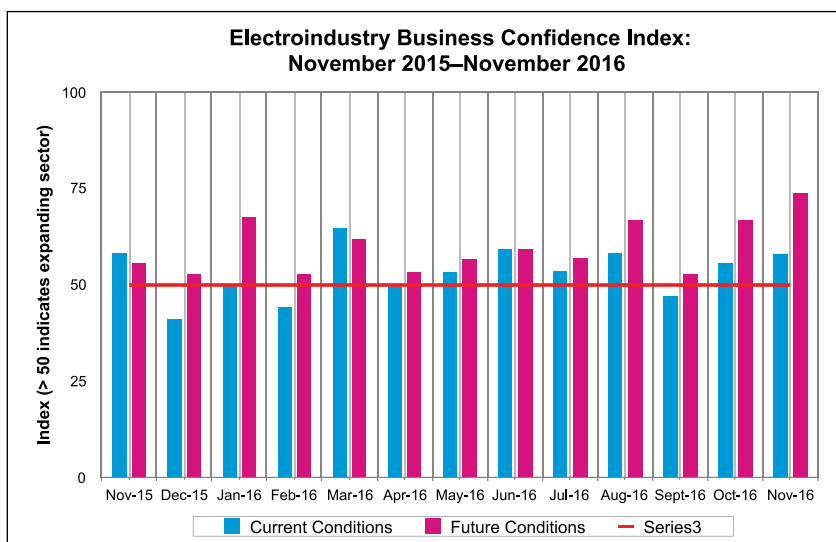
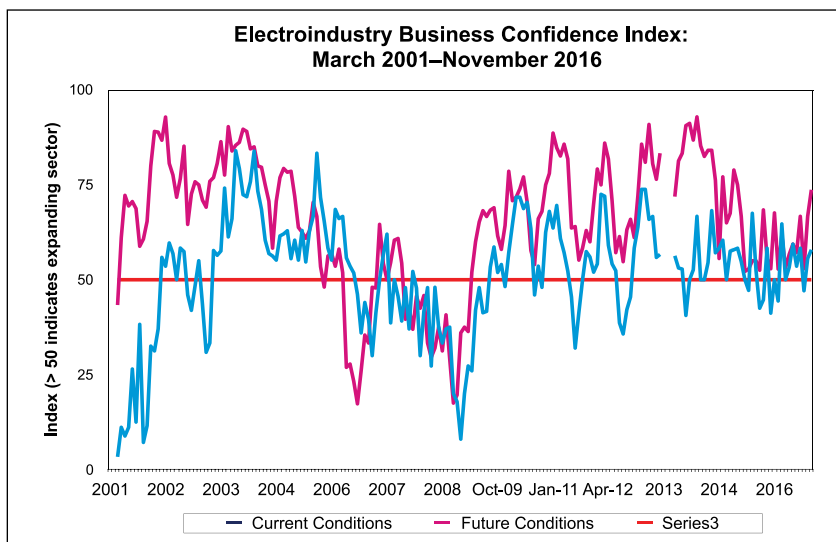
The share of respondents that noted unchanged conditions dropped 15 points, from 78 percent the previous month to 63 in November. Twenty-six percent of survey respondents reported better conditions, compared to 17 percent in October.

The survey's measure of the intensity of change in electroindustry business conditions pushed ahead to a slightly more positive rating, as the mean rating edged up to +0.3 this month compared to +0.2 in October. Panelists are asked to report intensity of change on a scale ranging from -5 (deteriorated significantly) through 0 (unchanged) to +5 (improved significantly).

At 73.7, this month's future conditions index eclipsed October's reading of 66.7. Although the share of respondents expecting unchanged conditions dropped from 44 percent in October to 21 percent, those anticipating worse conditions ticked up slightly from 11 percent last month to 16 percent in November.

The greatest mover among future conditions components was the share of panel members expecting better conditions. That number jumped 19 points, from 44 percent in October to 63 percent in November.

Visit www.nema.org/ebci for the complete November 2016 report. 📄



SPOTLIGHT

I Am NEMA



Mark Shoemaker,
Meter Socket Engineering Manager
Durham Company

I have seen and read many of the “I am NEMA” articles and thought it was a section to introduce NEMA staff. Then I realized that I am NEMA, too!

As a NEMA member of the 08EI3 Section, Meter Mounting and Test Equipment, I have represented my company, which manufactures meter sockets and electrical enclosures. There are other aspects of membership I appreciate, however, such as having an equal voice regardless of company size, focusing on consensus, working with knowledgeable people with common technical

insight and vocabulary, and being exposed to new technologies.

As an industry, we are in the midst of waves of new technologies and trends, including the smart grid, renewable energy, and home generation. We have the privilege, opportunity, and responsibility to shape and guide these waves through consensus standards.

Although new technology may not be in meter mounting devices specifically, we ensure system-wide interoperability and interchangeability as technologies and components emerge. We have guidelines and policies for field examination of equipment in situations such as natural disasters or system conversions.

I also appreciate for the NEMA staff. Because of them and NEMA guidelines, competing businesses can meet together in order to develop consensus standards and policies. They guide the waves surrounding us. Along with the staff, I am NEMA. ☺

John Marcario and Stephen Vastaugh Retire



John Marcario, posing here at his retirement party with Shlyneice Davis, senior administrative assistant in NEMA Operations, retired from NEMA after 22 years in the Operations Department. Photo by Joann Marcario



The Digital Imaging and Communications in Medicine (DICOM) Standard Committee bid farewell to Harry Solomon, past co-chair of the committee, and Stephen Vastagh, general secretary of DICOM, during the committee meeting at the Radiological Society of North America conference in Chicago in November. Mr. Vastagh retired after 24 years with NEMA. Mr. Solomon retired from GE Healthcare earlier this year.

Pictured are (from the left) Jim Philbin, American College of Radiology, co-chair of DICOM Standard Committee and DICOM Working Group (WG) 27; Harry Solomon; Stephen Vastagh; and Jeroen Medema, Philips Healthcare, co-chair of DICOM Standard Committee, DICOM WG 29, and DICOM WG 31. Photo by Luiza Kowalczyk

STOCK ART CREDITS

cover: @istockphoto.com/PeopleImages

5: @istockphoto.com/image_of_life

6: @istockphoto.com/kevinjeon00

8: @istockphoto.com/FernandoAH

8: @istockphoto.com/alubalish

8-10: @adobe stock/kentoh

9: @istockphoto.com/zstockphotos

11-16: @istockphoto.com/chombosan

17-19: @adobe stock/panimoni

19: @istockphoto.com/Ron_Thomas

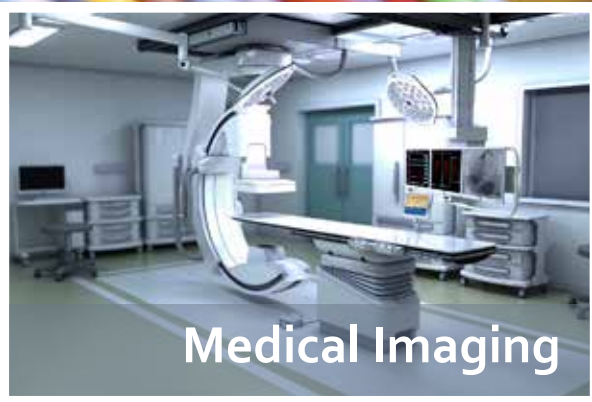
20: @istockphoto.com/grybaz

25: @istockphoto.com/traffic_analyzer

26: @istockphoto.com/Airubon

26: @istockphoto.com/janda75

Gain the NEMA Advantage with Standards



From wiring, enclosures, and switchgear to lighting, motors, and medical imaging, NEMA publishes more than 600 electrical standards that increase market demand, improve safety, and mitigate risks for millions of unique products.

All-new NEMA Standards Store at
www.nema.org/standards-store

Visit the NEMA Standards Store



LEARN MORE | 703.841.3200

www.nema.org



TESTED.

PROVEN IN YOUR WORLD.



CSA Group understands the impact energy storage testing has on the safety of your products and end users. As an OSHA Nationally Recognized Testing Laboratory (NRTL) and through our accreditations by the Standards Council of Canada (SCC), we are fully qualified to confirm portable and stationary energy storage systems meet U.S. and Canadian national standards for safety or performance. Whether your batteries are being used in watches, power tools, hoverboards or as part of a home solar panel system, we can help you get the certifications needed to install and use your batteries in North America and around the world. It's the support you need to contribute to a safer society and a more sustainable planet.

Phone: 1.866.797.4272

Email: certinfo@csagroup.org

North America | Europe | Asia



CSA
Group

www.csagroup.org

© 2016 CSA Group. All Rights Reserved.