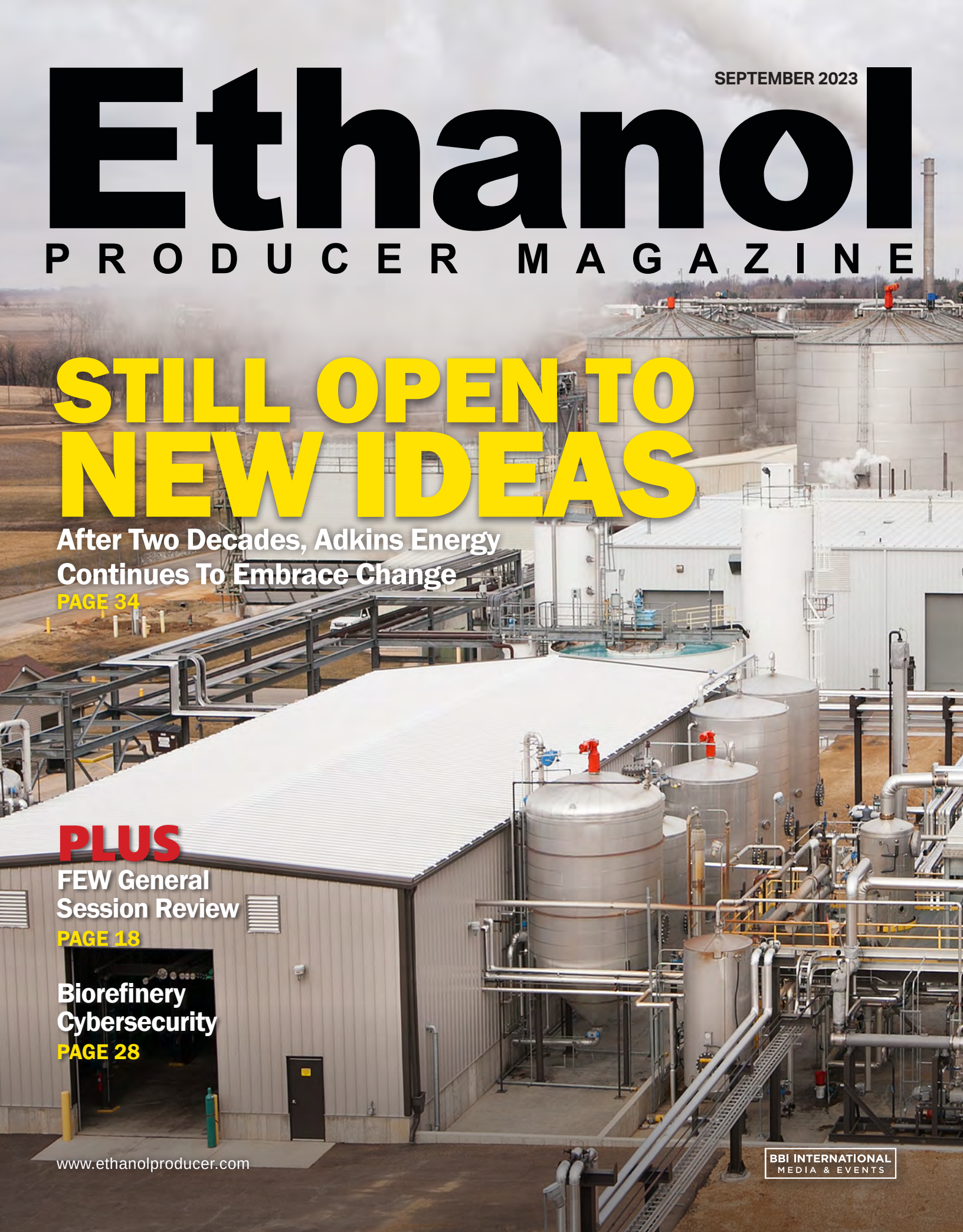
SEPTEMBER 2023

Ethanol PRODUCER MAGAZINE



STILL OPEN TO NEW IDEAS

After Two Decades, Adkins Energy Continues To Embrace Change

PAGE 34

PLUS

FEW General Session Review

PAGE 18

Biorefinery Cybersecurity

PAGE 28

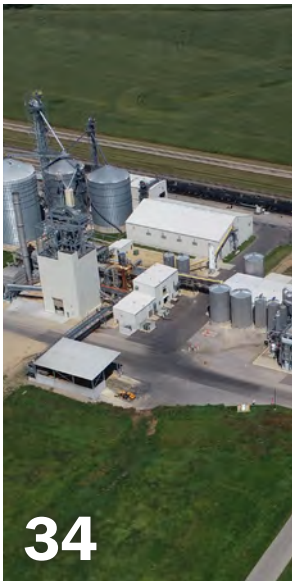
www.ethanolproducer.com

BBI INTERNATIONAL
MEDIA & EVENTS

Contents

18


28


34

SEPTEMBER 2023 VOLUME 29 ISSUE 9

DEPARTMENTS

FEATURES

SPOTLIGHT

ON THE COVER

Adkins Energy LLC in Lena, Illinois, turned 20 years old last year, but even after two decades of production, the management and veteran staff of the 60 MMgy corn ethanol plant continue to embrace innovation, growth and the potential of change.

PHOTO: ADKINS ENERGY

Ethanol Producer Magazine: (USPS No. 023-974) September 2023, Vol. 29, Issue 9. Ethanol Producer Magazine is published monthly by BBI International. Principal Office: 308 Second Ave. N., Suite 304, Grand Forks, ND 58203. Periodicals Postage Paid at Grand Forks, North Dakota and additional mailing offices. POSTMASTER: Send address changes to Ethanol Producer Magazine/Subscriptions, 308 Second Ave. N., Suite 304, Grand Forks, North Dakota 58203.

Facing the Future Head On

Acknowledging the energy transition that's occurring right now is a good way to ensure that we're a big part of it. That is, talking about what's happening is a smart strategy for the ethanol industry, but also a tricky one. Not everyone wants to openly discuss what's coming—decarbonization, yes—but this whole thing is really about electrification, the rise of EVs. And frankly, our industry's true concern should be ethanol's role in the predicted EV world.

Fortunately, it looks like we have a plan. The posture we've taken as an industry is, first, that higher blends of ethanol can accomplish things EVs can't—right now. Second, low-carbon liquid fuels will be needed for decades to come as electrification faces obstacles. And third, ethanol can be paired with electric (flex-fuel/EV hybrids) to achieve what neither can alone. So, we're challenging assumptions about electrification while advocating for technology-neutral policy and sharing a vision of how ethanol and EVs might work together. This and other bright concepts about our industry's future were discussed in detail during the general session of the 39th annual International Fuel Ethanol Workshop & Expo in June, which is recapped in "Front and Center at the FEW," on page 18.

The tone of this year's FEW, held in Omaha, Nebraska, was set by keynote speaker Geoff Cooper, president and CEO of the Renewable Fuels Association. Cooper engaged conference attendees on ethanol's role in the energy transition and the hazards of ill-conceived policy moves toward universal electrification. He pointed out the true carbon intensity of EVs (and no, they are not net-zero) and called for a market-based approach to decarbonization instead of tipping the scales toward electric.

"Rather than trying to force prescriptive technologies onto a market that may not be ready for them, energy transition policy should adopt a technology-neutral approach that embraces the diverse portfolio of low-carbon transportation options," Cooper told FEW attendees. "Let the marketplace do what the marketplace does. Let the market go to work, let the market solve its problem."

While we keep challenging assumptions about the carbon intensity of EVs, U.S. ethanol producers continue to inch closer to their own net-zero future. And what's cool about this is that a lot of innovation is happening at older, legacy plants. In our cover story, "Staying Power," on page 34, we profile Adkins Energy LLC, which celebrated its 20th anniversary last year but is doing anything but slowing down. Since 2002, the facility has continually gained new efficiencies and production volume, expanding from a nameplate of 33 MMgy to 60 MMgy today. Adkins has always been a trailblazer. The plant was built with the ability to generate its own electricity with CHP, and it made the bold move to integrate biodiesel production in 2014. Now, its management team is evaluating another daring venture—CO_2-to-methanol production. It could be an interesting new chapter for Adkins, and potentially other producers. As Bill Howell, the plant's general manager, tells us, "There are a lot of people hoping that we are successful."

Finally, be sure to check out "Squaring Up Cybersecurity," on page 28, which delivers a stark reminder that it's not just your business systems that are at risk of cyber crime, but your actual plant operations. If you haven't already done so, it's time to shore up your cyber defenses.

CREATING SEPARATION: When working with ethanol plants, IT/OT solutions provider Novaspect Inc. follows the guidelines of IEC 62443, a set of standards created by the International Society of Automation for implementing and maintaining electronically secure, zone-based industrial automation and control systems.
PHOTO: STOCK

Across nearly every major industrial sector—from healthcare to education to energy—news reports, whitepapers and entire business symposiums are echoing the same warning about cyberattacks: "It's not a matter of if but when." And, unfortunately, it's a very real threat that applies directly to every modern, connected ethanol plant.

Knowing what a cyberattack looks like, how they usually occur, where they can do the most damage, and who to work with to manage all things cyber is critical to preventing and mitigating potential attacks.

Meet the Cyber Experts

Spencer Banister is the operational technology group manager at Novaspect Inc., an Emerson Impact Partner company that provides engineering and service of industrial process controls. For Banister, cybersecurity work in the ethanol space is very active right now. After working on program control systems and server installations, Banister began focusing on cyber security in 2019. Since then, he and his team have become go-to experts in the industry.

"Within the ethanol space right now, I would say cybersecurity is a buzz word, Banister says. "What we find, though, with a lot of ethanol customers is that they don't know where to start."

It's not just the abundance of warnings coming out about the rise of cyberattacks that have ethanol plant IT teams on high alert. The new and increasingly sophisticated ways attacks are happening are also alarming. Phishing, malware and spoofing are now well-known entry points for cyber criminals. But now, more intricate—and potentially harmful—forms of attack are happening, like denial-of-service, code injection and (hopefully not) ransomware.

As Banister explains, insurance providers have been helping to inform businesses about the full spectrum of cybercrime, and how to deal with it all. Insurance companies want to know what a plant's cyber security management plan includes. According to Banister, they want to know what a plant will do to get back on track after an attack, if the plant has the right procedures or policies, and how the facility will keep

Squaring Up Cybersecurity

IT/OT professionals can help safeguard biorefineries from cyberattack by understanding criminal tactics, backing up data and being ready to act when bad things happen.

By Luke Geiver

its employees safe. Often, those responsibilities can fall on a small team or even one in-house IT professional working for the producer.

"If they come in and you don't have that plan of action and ability to implement it, your insurance premium will go pretty high, and your risk to personnel will be pretty high," he says.

Ethanol plants need to consider the impact of cyber on both their IT and OT operations. IT commonly refers to the internal informational data and storage capabilities at a plant, while the OT refers to the process and operations controls used to run production.

As Banister points out, if a bad actor gains access to a control system, like the distillation process, things can break, processes could go seriously wrong and even cause injuries. Novaspect specializes in the OT part.

"That is what foreign actors want to do," he says, talking about the physical disruption that could occur at a plant following a cyberattack.

In addition to insurance concerns and the fallout from foreign actors, Banister says most ethanol plants need to consider their staff. Most plants have staff rotation. There are always people coming in or out. General maintenance and policies around cyber need to start with that in mind.

Trent Vanderheiden, a network administrator for South Dakota-based IT Outlet, shares a similar sentiment to Banister. Vanderheiden and his team have established their firm as a go-to provider of IT services and supplies by creating custom solutions for a range of clients from school systems, healthcare, energy, and even ESPN.

For Vanderheiden, staff security or education about cyber attacks is an often overlooked component of cybersecurity. He says that, depending on the report, 91 to 93 percent of all Ransomware attacks (the kind that demand a ransom in return for releasing a system back to the original operator) are delivered via email. These attacks are crippling not only financially, but encryption algorithms now know industrial machinery and can completely destroy things. Vanderheiden makes a simple statement about it all, saying, "If you look at your environment and it has a blinky light on it, it's at risk."

Solutions, Considerations, Ethanol Plant IT/OT Needs

Banister now has a team of 15 that focuses on control system upgrades, virtualization and reliability. Every member of his team participates in cyber security installations. The focus of their work centers around a set of requirements becoming popular across industries: they follow the guidelines and direction of IEC 62443. The number refers to a set of standard requirements created by the International Society of Automation for implementing and maintaining electronically secure industrial automation and control systems (the things with those blinky red lights). According to the ISA, "the standards set best practices for security and provide a way to assess the level of security performance. Their approach to the cybersecurity challenge is a holistic one, bridging the gap between operations and information technology, as well as between process safety and cybersecurity."

The IEC 62443 standard has been a big change across the industry for industrial manufacturers, Banister says. In the next five years, everyone will be familiar with it. Some customers have already adopted the basics from the standards and Novaspect is even certifying its engineers in the process. In summary, the standards create a multi-stakeholder approach to creating, manufacturing, applying and maintaining industrial components organized and installed in a zone-based scheme that enable the best chance of mitigating the most risk from a cyberattack.

Cybersecurity solutions in the ethanol plant have to deal with what Banister calls a flat-network. Everything across a plant is typically on the same network. Everything can talk to everything.

"We have to create a good separation of network traffic," he says. Novapsect does that by creating a proper way to pass data from the business systems to the process systems.

Vanderheiden puts it another way. "At the end of the day, you're an IP address to a threat actor," he says.

And, although most industries think they are unicorns not exposed to cyber threats, Vanderheiden explains that the ethanol space is no different than a school or mom and pop coffee shop. Every entity needs to start somewhere with cyber.

Banister's team starts with cyber threat assessments. They go in with a toolkit, scan the entire system and determine where a plant is at with risk to cyber. Then they go hit the "easy things" first including OT systems hardening, blocking USBs from being used on computers, making sure people can't remotely access in to machines they shouldn't have access too, making sure everyone at the plant doesn't have access to operate machines or make control changes and more. In addition, the team will provide a user permission workshop to provide clarity and confidence to the staff.

BEYOND CLOUD BACKUP: These days, ethanol producers are being advised to protect their critical data in multiple ways and not let that data stay in one location. Without good backups, reprograming a system to its previous version prior to an attack that ruined or corrupted essential data could cost tens of thousands of dollars.
PHOTO: STOCK

DOE Bioenergy Cybersecurity Workshop Announced

The U.S. Department of Energy's Bioenergy Technologies Office (BETO) will host a Bioenergy Cybersecurity Workshop on September 11. The virtual event, organized by Sandia National Laboratories, will identify cybersecurity risks in biofuel and bioproduct manufacturing, and develop approaches to addressing these risks.

The workshop will focus on the importance of cybersecurity in biomanufacturing safety, operational continuity and competitiveness. The event will include panel presentations by bioprocessing and cybersecurity experts, along with participant discussions. Participants will discuss the state of biofuel and bioproduct cybersecurity practices and the security of biobased processes to help identify and define cybersecurity technologies and research needed for cybersecure bioenergy production.

Visit **www.energy.gov/eere/bioenergy/articles/bioenergy-cybersecurity-workshop-announced** to register for the event.

After that, the team looks at hardening the system more with backup recovery and essentials. "If you get ransomware, backup recovery is your best friend," Banister says.

Vanderheiden and his IT Director Dusty Sperlich have become well versed in backup recovery and creating a reliable, efficient system. Sperlich has helped create intricate and effective systems for major healthcare providers, small schools and even the territory of Guam. One of the interesting topics he is currently looking at is a spin on what most non-IT people might think about data storage.

"Now the trend is that you have to back up your cloud data," Sperlich says. "It is almost ironic that we moved from backing up stuff to the cloud to having complete cloud infrastructures to backing up that cloud environment back locally or to another cloud." The thing to remember, Sperlich says, regardless of all that data backup work, is that you have to protect your critical data in multiple ways, and you can't let that data stay in one location.

Without good backups, Banister says, reprograming a system to its previous version prior to an attack that ruined or corrupted operating essential data could cost tens of thousands of dollars.

The last thing is patch management, which is related to applying the latest hotfixes. "Process disruptions at an ethanol facility can be thousands of dollars per minute," Banister says. "We understand all of the pieces and parts from the switches to the servers."

Generally, hardware is recommended to be swapped out every five to seven years. Servers from 2022 are the current generation, and should last until 2027 to 2029 before becoming outdated.

For control systems to have the latest and greatest features, Banister says the newest options are always the best because that is what all the newest connected tech is built off of.

Recently the Novaspect team has been highly focused on developing network threat detection solutions. It is based off a software that allows Novaspect to mirror the network traffic and identify irregularities. When put in an online mode, it will start to identify things that are not normal. For instance, when you watch a control system, most changes occur between the hours of 8 a.m. and 5 p.m. If someone is downloading info at 1 a.m., it generally means something is happening that shouldn't be, Banister says. For cybersecurity, both Banister and Vanderheiden believe knowing what is happening is important.

"The sooner you can get a notification, the sooner you can take action," Banister says.

Author: Luke Geiver
Contact: writer@bbiinternational.com