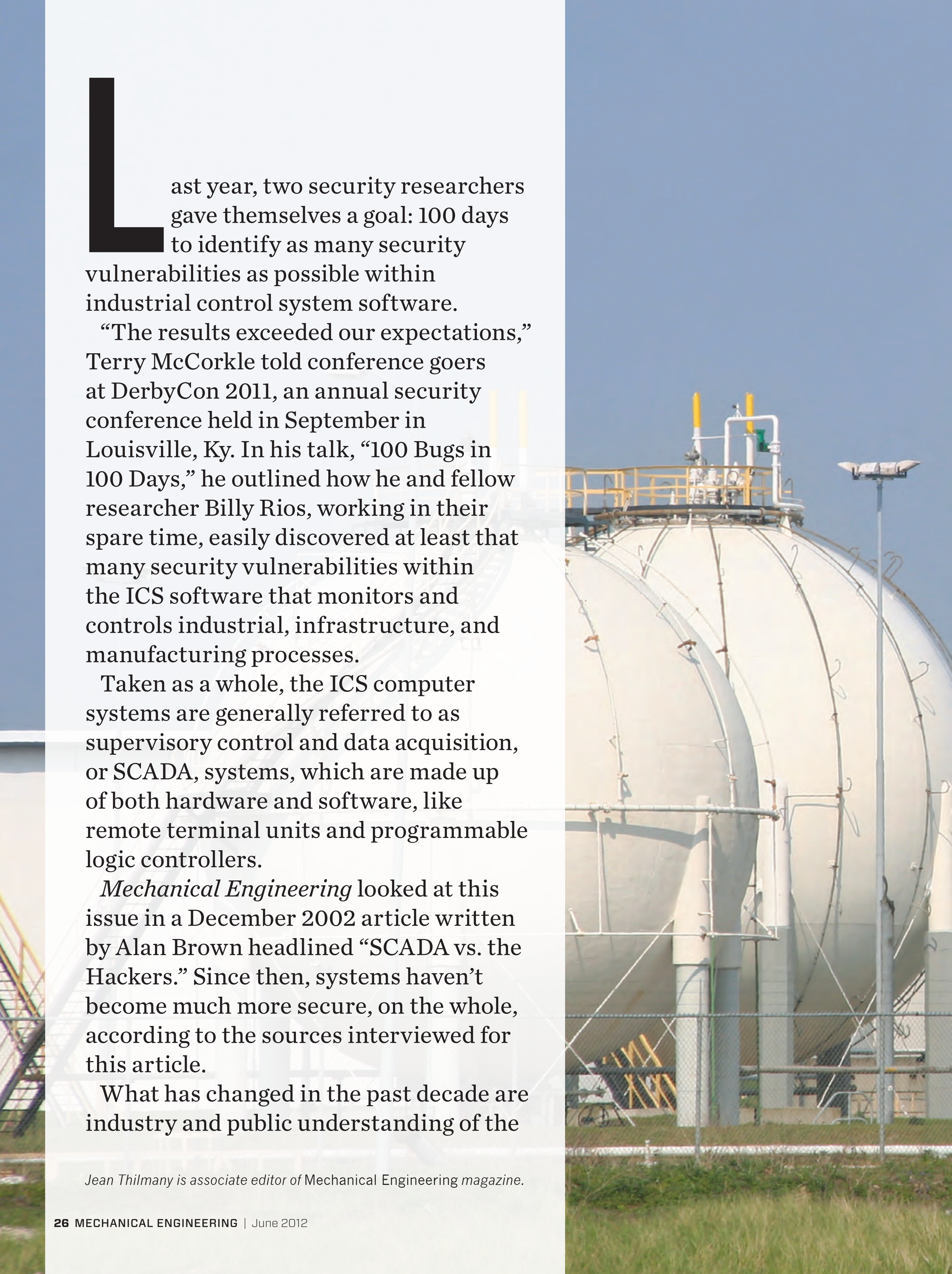


Last year, two security researchers gave themselves a goal: 100 days to identify as many security vulnerabilities as possible within industrial control system software.

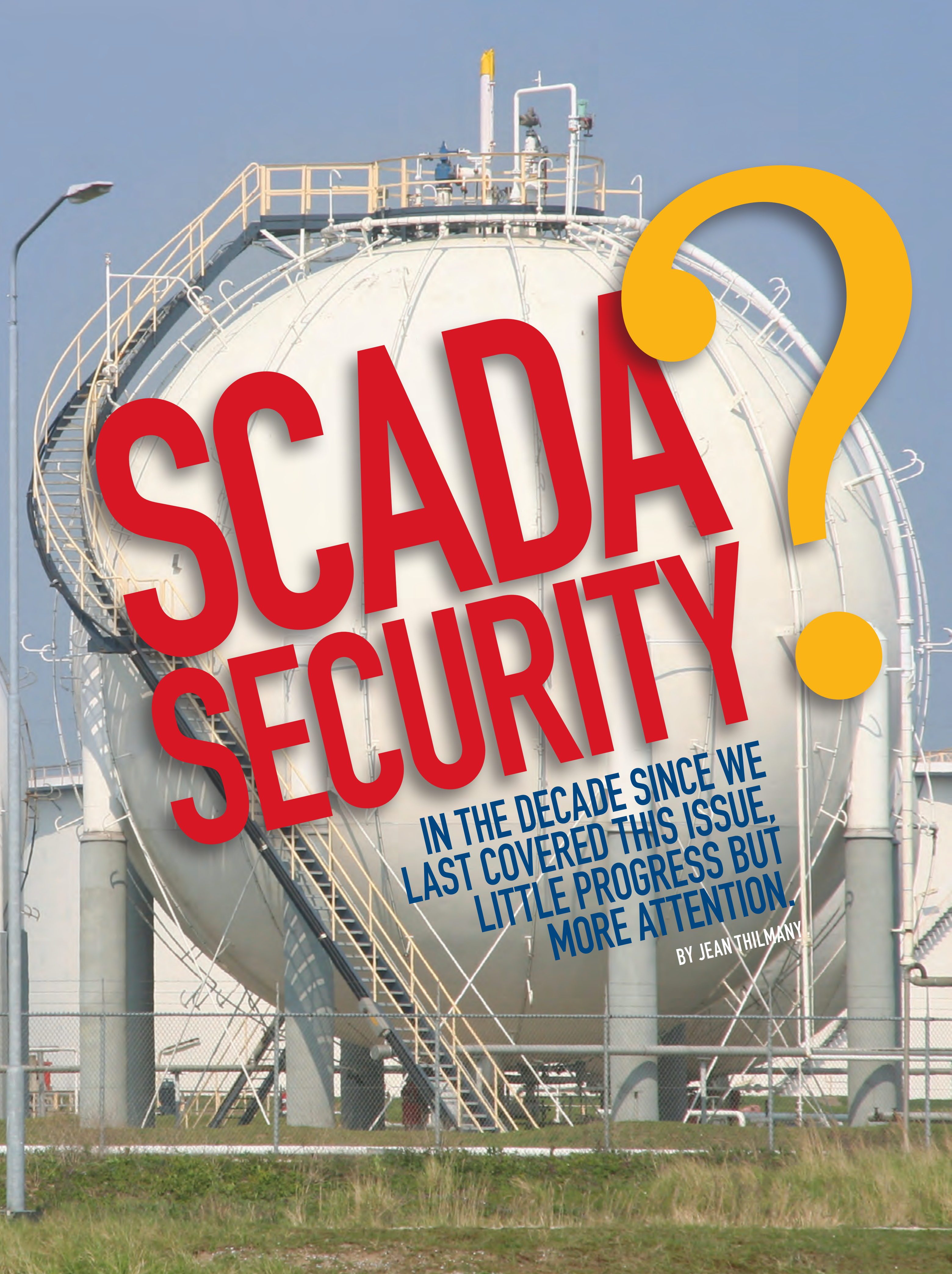
"The results exceeded our expectations," Terry McCorkle told conference goers at DerbyCon 2011, an annual security conference held in September in Louisville, Ky. In his talk, "100 Bugs in 100 Days," he outlined how he and fellow researcher Billy Rios, working in their spare time, easily discovered at least that many security vulnerabilities within the ICS software that monitors and controls industrial, infrastructure, and manufacturing processes.

Taken as a whole, the ICS computer systems are generally referred to as supervisory control and data acquisition, or SCADA, systems, which are made up of both hardware and software, like remote terminal units and programmable logic controllers.

Mechanical Engineering looked at this issue in a December 2002 article written by Alan Brown headlined "SCADA vs. the Hackers." Since then, systems haven't become much more secure, on the whole, according to the sources interviewed for this article.

What has changed in the past decade are industry and public understanding of the

Jean Thilmany is associate editor of Mechanical Engineering *magazine.*



SCADA SECURITY?

IN THE DECADE SINCE WE LAST COVERED THIS ISSUE, LITTLE PROGRESS BUT MORE ATTENTION.

BY JEAN THILMANY

issue and attempts at SCADA regulation and legislation.

Within the past decade, security experts along with SCADA vendors and users have woken up to the fact that the systems aren't nearly as secure as the information technology software running on desktops and networks at businesses across the nation, said the sources interviewed for this article.

The SCADA security concerns have come to be seen as a big deal because the systems can be found within power plants, refineries, pipelines, water treatment plants, and the telecommunications industry, where hackers could do great damage that would affect the public.

YOU CAN'T TELL YOUR CUSTOMERS, 'YOU WON'T BE ABLE TO TURN YOUR LIGHTS ON WHILE WE UPDATE OUR SOFTWARE.'

And a number of high-profile attempted or successful system breaches have brought the issue to the public's attention. Usman Sindhu, senior research analyst at IDC Energy Insights, mentioned Stuxnet, for instance. It is a computer worm discovered in June 2010 that made international news. It spreads via Microsoft Windows and targets Siemens industrial software and equipment.

Sindhu follows the energy and oil and gas industries at the analysis firm based in Framingham, Mass.

Stuxnet is the first discovered malware that spies on industrial systems, including the programmable logic controller. Security experts have since discovered the malware had been calibrated in a way that would cause nuclear centrifuges to spin out of control, Sindhu said.

Then, in November 2011, a twentysomething hacker told news outlets he hacked into a South Houston, Texas, water utility to show that it can easily be done. The hacker said he had hacked other SCADA systems too and followed that assertion by tweeting links to public postings with what he identified as PLC configurations for a Polish waste-water treatment plant, SCADA data from a human-machine interface box possibly used at a generator at Southern Methodist University, and what may be water metering control system files from Spain or Portugal.

In news interviews at the time, the hacker, who called himself "pr0f," said he breached the water utility system and tweeted the links because he feels the Department of Homeland Security downplays the vulnerability of the national infrastructure.

As enterprise technology security matures—IT employees at global banks down to small businesses now have the tools and expertise to protect their systems—attackers are now turning their attention to lesser-protected SCADA networks, said Jacob Kitchel, senior manager of security and compliance at Industrial Defender in Foxborough, Mass. The company makes infrastructure security tools.

"Attackers have had the past decade to learn and refine their craft on IT; then they moved on to automation," he said.

SCADA attacks do appear to be on the rise, according to the U.S. Department of Homeland Security. In March, the *New York Times* reported on numbers from the DHS. During five months from October 2011 through February 2012, there were 86 reported attacks on computer systems in the United States that control critical infrastructure, factories, and databases, as compared with 11 over the same period a year earlier.

In light of SCADA security concerns, security researchers have stepped up efforts to find and to call attention to the systems' vulnerabilities. McCorkle told those at the conference how to find and correct the SCADA software vulnerabilities that he and Rios had discovered.

Both McCorkle and Rios work as security professionals by day—at Boeing and Google, respectively. They spent more than three months looking in their off hours for SCADA system security breaches. They found many SCADA security vulnerabilities by running Internet searches for phrases common in the ICS world, McCorkle said.

"This was something we did in the evenings while having a beer," McCorkle said in his talk, emphasizing that he and Rios didn't need to devote incredible amounts of time, resources, or even much research to isolate SCADA security issues.

Rios had taken his own research even further. According to his blog, at xs-sniper.com/blog, he has worked with the Industrial Control Systems Cyber Emergency Response Team, or ICS-CERT, and various SCADA vendors to find nearly 1,000 security breaches within systems. ICS-CERT works with the Department of Homeland Security's U.S. Computer Emergency Readiness Team and conducts ICS vulnerability analyses—using researchers like Rios. It provides support for dealing with attacks as well as forensic analysis into how an attack happened and from where it came.

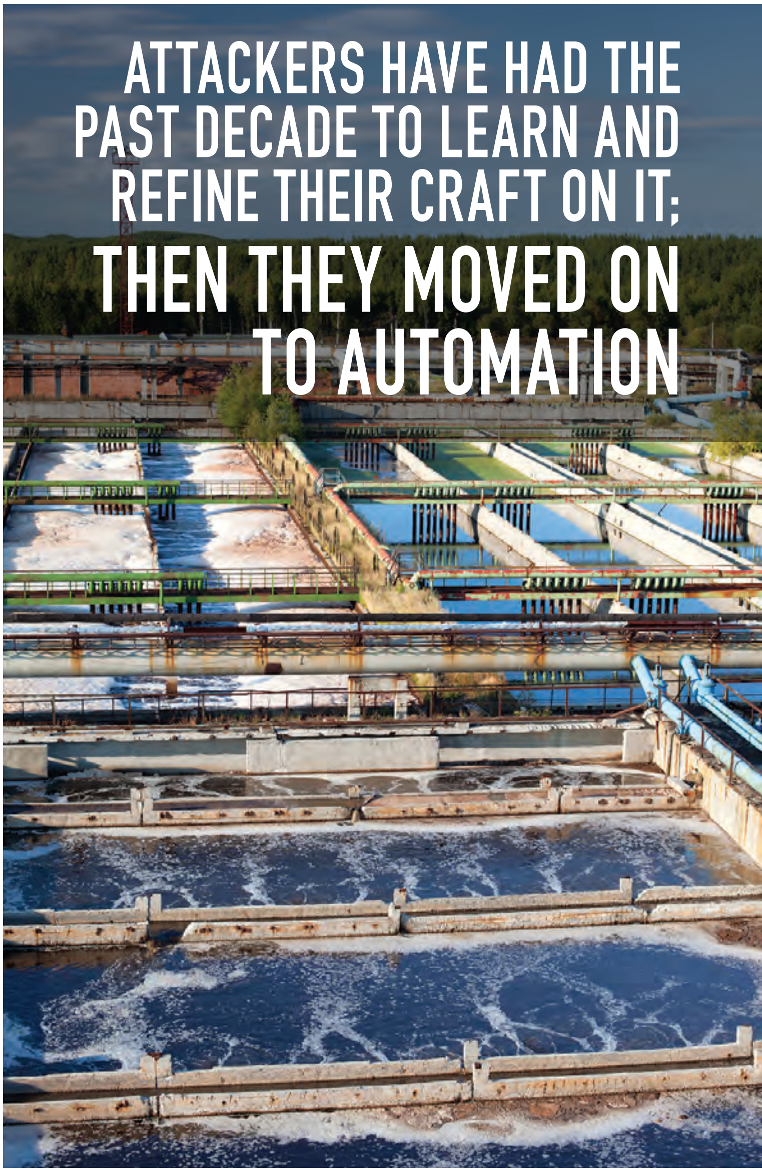
SOMEWHAT LOCKED

In response to these reports, many SCADA users have taken steps to secure their systems during the past decade; many others are unaware of the issues or simply lack the personnel, knowledge, or funds to do much about security, said Ajit Sancheti, vice president of business development at Mu Dynamics in Sunnyvale, Calif. The company makes security-testing software, including tools for federal SCADA systems.

Before the rise of the Internet, SCADA systems were composed of devices communicating with each other, Sancheti said. As the Internet and wireless communication networks have evolved, the systems began communicating through the corporate network and then through the Internet, which has left them vulnerable to security attack.

While security issues surrounding information technology software came to public attention early in the Internet age—with a subsequent rise in security software and IT expertise on the issue—the same hasn't been true with ICS software, according to Kitchel at Industrial Defender.

SCADA security—in terms of awareness and protection—is where IT security stood in the late 1990s, when the Internet was growing quickly and users became aware of hackers, Kitchel said.


ATTACKERS HAVE HAD THE PAST DECADE TO LEARN AND REFINE THEIR CRAFT ON IT; THEN THEY MOVED ON TO AUTOMATION

"It's really back to the future in terms of SCADA security," Kitchel said.

For that reason, technology professionals employed by the companies that use SCADA may not be up to date on how to best protect against invaders, he added. On a positive note, IT security experts have been able to cross industries, to help those who rely on SCADA systems.

"So when experts put a discerning eye on the SCADA software, they're going back in time because they can put everything they learned in the past ten years to the present-day situation," Kitchel said. "It's 2001 or 2002 in the connected nature of systems, maturity, and attention to security in building and deployment of SCADA software."

But other security factors unique to SCADA also come into play when trying to secure those systems, he added.

SCADA software and hardware can be difficult to update and refresh, Kitchel added.

"ICS are supporting a high-availability physical process that you don't want to tinker with," Kitchel said. "Utilities have a maintenance window on the power supply, and they plan for that downtime outage sometimes years, but at least six to eight months, ahead of time."

As he put it: "You can't tell your customers, 'You won't be able to turn your lights on while we update our software.' "

The processes SCADA systems help run are becoming even more sophisticated, in light of customers' demands for real-time information. For instance, meters that continually monitor home energy use are hitting the market, said Mahesh Patel, director of product management at Sixnet Solutions in Ballston Lake, N.Y., a maker of industrial networking software.

"End users are demanding real-time information too, for meeting environmental reporting requirements," he added. "Also, the utility itself wants real-time information on remote leaks, like at a well-head site of a power distribution center, so it can quickly fix them to keep its assets running and increase uptime."

POTENTIAL NEGATIVE PUBLICITY IS THE ISSUE DRIVING MOST SECURITY CHECKS

All this makes for more sophisticated SCADA systems tied closer to Internet networks, making them more vulnerable to security issues, Patel added.

GROWING OVERSIGHT

Because national attention has only recently turned to SCADA security, system users have few regulatory specifications by which they must abide, Sancheti said.

"But the industry is starting to find ways to police itself before anything formal comes out," he added. "Still, what we've found is change has been slow and difficult for many. Oil and gas and other users are run by regulations, so because there's no SCADA regulation, there's been no need to do it. I think they're setting themselves up for negative press."

His company has worked with the International Society for Automation's Security Compliance Institute to develop an embedded device security assurance certification. The ISA defines an embedded device as a special-purpose device that runs embedded software designed to directly monitor, control, or actuate an industrial process.

SCADA suppliers can now have their products certified to the organization's ISASecure designation for embedded devices. Further ISASecure standards—for supplier practices and for user practices—will be forthcoming from the ISA.

Certification isn't regulation, though it will show customers their suppliers meet ISA security requirements, according to an ISA statement.

In June 2011 the National Institute of Standards and Technology issued its *Guide to Industrial Control System Security*. According to a statement issued by NIST, the guide is intended to help pipeline operators, power producers, manufacturers, air traffic control centers, and other managers of critical infrastructure secure their systems.

The guide is targeted to federally controlled systems. "However, the guide's potential audience is far larger and more diverse than the federal government, since about 90 percent of the nation's critical infrastructure is privately owned," according to the NIST statement.

The electrical power industry, unlike the chemical, manufacturing, and oil and gas industries, does have a relatively new SCADA regulatory standard, according to Sindhu at IDC Energy Insights.

In 2006, the federal government charged the North American Electric Reliability Corp., or NERC, with defining and implementing standards for critical infrastructure protection within the industry. The result is NERC-CIP, which is applied to all electrical utilities generating power at 120 kilovolts and above, Sindhu said.

The reliability standard includes more than 40 requirements a utility must meet.

"SCADA systems hold the keys to the kingdom for the util-

AS THE INTERNET AND WIRELESS COMMUNICATION NETWORKS HAVE EVOLVED, THE SYSTEMS BEGAN COMMUNICATING THROUGH THE CORPORATE NETWORK AND THEN THROUGH THE INTERNET, WHICH HAS LEFT THEM VULNERABLE TO SECURITY ATTACK.

ity professions because they monitor, control, and manage important processes for electrical transmission and generation," Sindhu said. "NERC-CIP helps them oversee these systems and report vulnerabilities."

NERC audited large utilities last year under the program; in 2012, more utilities will be audited. Spot checks and self-assessment will continue throughout the year, he said.

"Electricity is a little more advanced in this regulation—I wouldn't say blessed, because it's more work for operations professionals to get ready for the audit. In contrast, oil and gas, chemical, and manufacturing industries don't have a regulatory mandate equal to NERC-CIP," Sindhu said. "Other industries take feeds from mandates like NERC; they'll look it up to see if something within it can help them out.

"Across the board, I see some of the other industries, like manufacturing and chemical, lagging a little behind oil and gas in implementing security practices because they may not have the technologies to do so or there may not be good communication among the stakeholders," Sindhu said.

A number of pieces of legislation have been passed and proposed to address software security. The big one right now is the Cybersecurity Act of 2012, which has been introduced by Senator Joseph Lieberman of Connecticut. Among its provisions, it would give the National Institute of Standards and Technology an active role in assessing risk and developing standards and guidelines for software security. NIST would collaborate with the Department of Homeland Security, as well as other government agencies, the private sector, and academia.

"So you'll see NIST doing what NERC is doing today," Sindhu said. "It would mean that NIST takes the central control from an implementation perspective."

As currently written, the proposed legislation is quite broad, said Chris Eng, vice president of research at Vera-Code, a Burlington, Mass., maker of application security software.

"There's a concession that we need to protect critical infrastructure, but it is not clear yet what the software security side will look like in legislation," Eng said.

Issues of federal SCADA security enforcement are for future debates. Meanwhile, SCADA users around the nation struggle in their own way to ensure their systems are safe from security attack.

Right now, potential negative publicity is the issue driving most security checks, Sindhu said.

"In general I think there's acknowledgement about security threats," he said, "and leadership recognizes security is a brand-name issue, because when a security breach puts a bad name to your company, there's a trickle-down effect to your business partners." ■