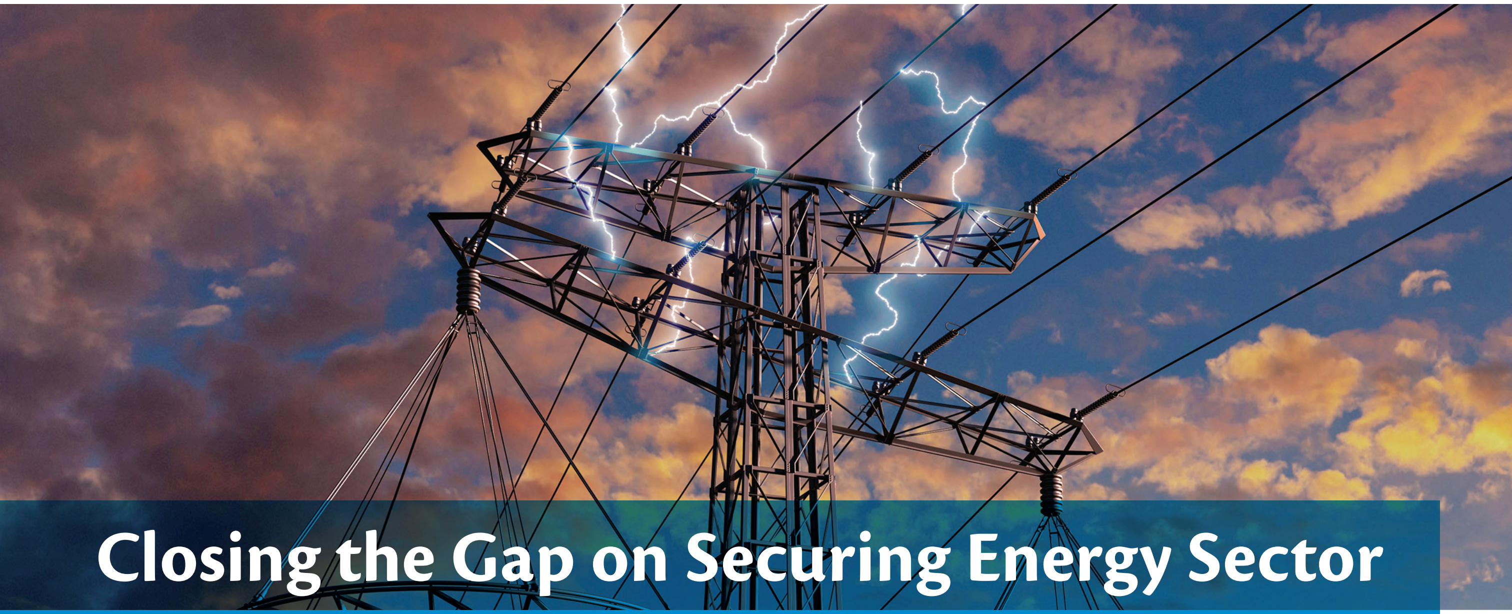

Closing the Gap on Securing Energy Sector Control Systems

Sean Peisert | Lawrence Berkeley National Laboratory and University of California, Davis
Jonathan Margulies | Qmulos

When policy experts expound on the importance of cybersecurity, they often invoke attacks against the power grid as a worst-case scenario; disabling the grid is the trump card that makes laypeople sit up and take notice. But for all the attention this problem has garnered over the past decade—including a war of words between the US and China, a *60 Minutes* story, and of course Stuxnet—the state of energy security might not be appreciably better than it was when the conversation began. For every step forward we've taken in terms of improved technology and best practices, we've taken one back in terms of increased connectivity and automation.

The slow progress has many causes: the control system community's concern that improved security features threaten system reliability; an imbalance of economic incentives, with whole nations sharing the risks but only energy companies bearing the costs of mitigating them; and lack of mutual understanding between the people who work on energy control systems and those who create security products. This last cause is the primary one we hope to address in this issue.

What passes for progress in the field of energy security today is the application of existing enterprise security best practices in a control system context—and even that has proven extremely difficult. The people who build commercial security products understand the needs of enterprises, but too many know nothing about control systems' peculiar requirements.

In This Issue

We hope the articles we selected for this issue will help our readers understand enough about the state of energy cybersecurity to begin making a difference in the field. We start with a survey piece. In "Control Systems for the Power Grid and Their Resiliency to Attacks," Carlos Barreto and his colleagues provide an introduction to power grid cybersecurity and its unique challenges. They

1540-7993/14/$31.00 © 2014 IEEE

explain the basic control system components, how those components are used in the grid, and common measures for maintaining grid stability. Next, they introduce the more recent advances collectively known as the *smart grid*. Finally, they propose a control theoretic model to help designers make control systems more resilient to attack. For readers who've never studied the power grid, this article is an excellent place to start.

Our next few articles focus on prototype solutions for control system security, which we believe will give readers a strong sense of where gaps remain. Moses Schwartz and his colleagues describe several new control system security solutions in "Emerging Techniques for Field Device Security." The authors lay the foundation by describing the anatomy of field devices, including hardware, firmware, operating systems, and security features. They then define several features that would be desirable for enhanced security—inspectability, trustworthiness, and diversity—and provide an overview of research projects that have begun adding such features to field devices.

In "Monitoring Security of Networked Control Systems: It's the Physics," Chuck McParland, Sean Peisert, and Anna Scaglione demonstrate intrusion detection systems' (IDSs') potential to impact the control system environment more than they ever could in an enterprise. Because control system behaviors are more limited and predictable than their enterprise counterparts, the authors were able to build a model of acceptable command behavior for a small control system into an IDS. Although generalizing this approach to work on real-world complex control systems is a major challenge, the possibility that we could build network-monitoring tools to account for control system context is intriguing.

Saman Zonouz, Julian Rrushi, and Stephen McLaughlin take a similar tack in "Detecting Industrial Control Malware Using Automated PLC Code Analytics." Their work closes an important gap in control system security by providing insight into the code running on control system devices, and they, too, attempt to automatically identify behavior that would send the control system into a dangerous state. The article details their technical approach to modeling the execution of programmable logic controller (PLC) firmware and formally verifying that the code doesn't lead the overall system to an unsafe state.

Ryan Ellis looks at power grid cybersecurity from a policy perspective in "Regulating Cybersecurity: Institutional Learning or a Lesson in Futility?," analyzing US regulation of the field as a potential model for other nations and industries. He notes that the US has taken a novel approach to developing its critical infrastructure protection standards in that the regulations are drafted by industry but approved by the government. He then details the history of how those standards have evolved in specificity and scope since the process's inception. Finally, he argues that the results suggest that the chosen approach was appropriate for the circumstances.

In our roundtable, "Control Systems Security from the Front Lines," we interview four experts from the energy cybersecurity community—Eric Byres, Paul Dorey, Dale Peterson, and Zach Tudor—about some of the major challenges facing the field. We begin with a discussion about the current state of off-the-shelf control system products, many of which are still being built without basic cybersecurity features. The panelists then explain how a focus on extreme reliability and long life spans for control system components has resulted in an unusual relationship between energy system operators and product vendors, with both good and bad consequences. Finally, they describe open research topics that could result in breakthroughs for energy cybersecurity.

Finally, in "Experimenting with Incentives: Security in Pilots for Future Grids," Francien Dechesne, Dina Hadžiosmanović, and Wolter Pieters argue that the power grid community is missing an important opportunity for security improvement by failing to take security into account when piloting smart grid components. They detail their findings from interviews with grid operators currently involved in Dutch smart grid pilots, which suggest that although stakeholders are concerned that new grid architectures and increased customer involvement will present unforeseen security issues, none of the pilots explicitly experiments with such issues. They then propose an incentives-based approach to studying and mitigating emerging smart grid vulnerabilities.

One of the challenges of cybersecurity is that it comes up in so many different domains of expertise. Security products can't be bolted onto business systems, medical devices, or control systems. Security must be integrated, and the people who effect that integration must successfully overlap two completely unrelated fields.

Control system operations staff are highly specialized. They're a healthy mix of deep, narrow experts—power engineers and petroleum engineers, for example—and less educated technicians who slowly evolve from field workers to supervisors. For an industry in which 50-year-old equipment remains commonplace, cybersecurity is a brand new requirement, and there's a shortage of qualified experts available to address it. It will be up to our community to bridge the gap. ■

Sean Peisert is jointly appointed as a staff scientist at Lawrence Berkeley National Laboratory and as an assistant adjunct professor at the University of California, Davis.

Jonathan Margulies is the chief technology officer at Qmulos. Contact him at jonathan@qmulos.com.