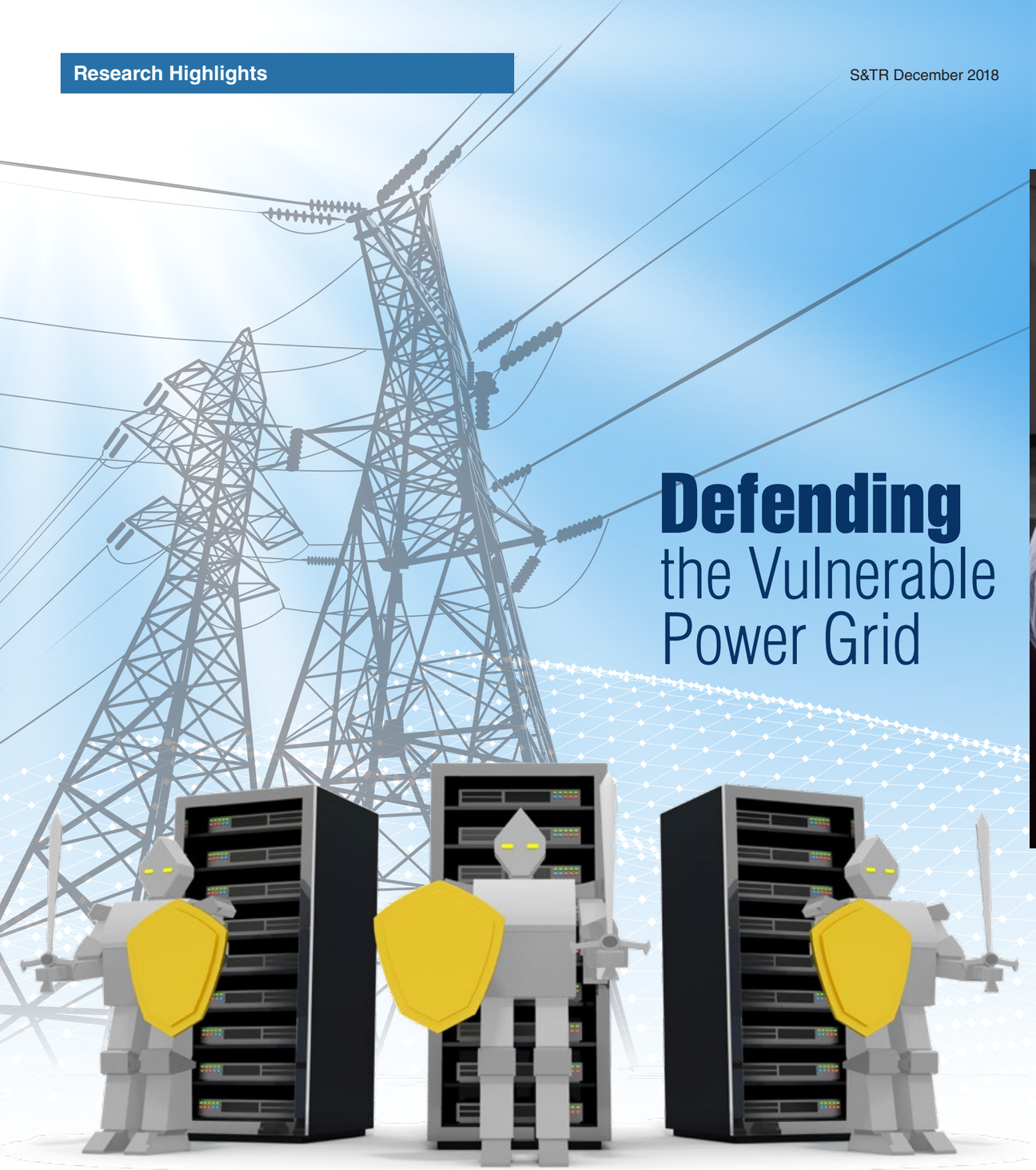

Defending the Vulnerable Power Grid

Nate Gleason (seated) studies electrical sine waves on a monitor at Livermore's Skyfall test bed facility. Behind him, Vaibhav Donde (left) and Jovana Helms examine the interior of Skyfall's in-house relay substation. (Photo by Randy Wong.)

IN 2015, just before the holidays, hackers shut down electricity for more than 230,000 people in and around Kyiv, the Ukrainian capital. The event is understood to be the first successful cyberattack on a power grid, but infrastructure vulnerability is everywhere. The next attack could be just over the horizon, and Lawrence Livermore's Skyfall laboratory is working hard to blunt its force.

Skyfall is a combined cyber–physical hardware-in-the-loop test bed that connects real-world equipment with high-performance computers, strengthening the fidelity of simulations that help the United States prepare for disaster. The name "Skyfall" comes from the James Bond movie of the same name, in which villain Raoul Silva uses a cyberattack to destroy a gas pipeline in London.

Although the film is fictional, the threat of cyberterrorism to many infrastructure networks is very real.

"If security is not part of the inherent design, the system will be vulnerable," says Jovana Helms, an associate program leader in Livermore's Global Security principal associate directorate. "One thing we hope to use Skyfall to do is understand how we can make security part of the design, rather than an afterthought. Our motto is 'security built-in, not bolted-on.'"

Simulating a Hodgepodge

Power grids are immensely complex, interconnected systems. In Ukraine, the attack involved exploiting human weaknesses—phishing passwords from system administrators. Thankfully, the attack's effects were kept relatively limited by reverting to manual control. In the United States, phishing is a vulnerability, but more aspects of the grid are controlled by automated systems, broadening the risk. "The power grid is a very old system," says Vaibhav Donde, Skyfall's principal investigator. "With a mix of legacy and new equipment, the system always has issues and challenges on how to make everything work together, and fitting on top of all that is a cyber system."

Skyfall's power substation is the same as one that would be found on a real-world power grid. By using such hardware alongside sophisticated computer simulations, Skyfall can analyze a cyberattack from beginning to end.

Past accidents can be instructive. In August 2003, a software bug led to a series of procedural mistakes that failed to correct for a simple voltage fluctuation in rural Ohio. A few hours later, an estimated 55 million people on the East Coast and in Canada were plunged into darkness. This event illustrates how small problems can rapidly cascade into a massive outage. Although the 2003 event was caused by a software error, a similar event could also be triggered by a deliberate cyberattack. The system only needs to "think" it is malfunctioning for such problems to arise.

Hardware in the Loop

Sophisticated simulations, such as those run on Lawrence Livermore's high-performance computers, can help power providers plan for cyber–physical incidents on the grid, including accidents and attacks. However, an important difference exists between a purely software-based simulation model and a hardware-in-the-loop model. Helms explains, "Some customers may say, 'That's just a model, and there's no perfect model,' but with hardware in the-loop, we are adding a whole new level of realism and fidelity to our simulations. We can incorporate an actual device in the laboratory and mimic that behavior across a grid."

At Skyfall's center is a full-fledged power substation that behaves as if connected to an actual power system. A computer feeds the substation a set of conditions—such as voltages and currents—just like the signals that would be received in the real world. The researchers can then see how the Skyfall substation responds to an unexpected power surge, for example, and then extrapolate the results across the wider network. "Let's say you have a simulation with 5,000 relays, two of which are physically represented in the laboratory," says Helms. "Instead of talking to a modeled relay in a computer, our simulation actually talks to the physical relays." In some ways, the difference is the same as that between trying to understand a forest with a computer and understanding a forest by growing a real tree. The resulting high-fidelity simulations are detailed, realistic models of cyber–physical systems at scale.

What sets Skyfall apart from other hardware-in-the-loop facilities is its ability to simulate a cyberattack from beginning to end, providing a realistic view of system behavior during an attack. Skyfall can cosimulate power flow and communication across the grid. Donde says, "Today, all these systems—distribution, transmission, and communications—are so tightly coupled that one cannot simulate any single system correctly without considering its connections to the other layers." Because of this interconnectedness, the Department of Energy has made cosimulation a priority. Future evolution of the Skyfall platform will include equipment used in the other layers, including solar panels and electric car chargers.

Protecting Infrastructure

One of the newest monitoring devices being incorporated into power grids are phasor measurement units (PMUs), which track power flow between locations by measuring electrical sine waves. Each PMU is calibrated to look for a shift in the wave—a change in waveform phase—to determine how differently the grid is loaded at the PMU's specific location relative to others. A PMU in Livermore will measure Livermore's phase, but the same PMU model in Chicago or Virginia Beach will measure a different phase there. All such PMUs will collectively use this information to accurately calculate the power that people are using at that instance of time across the grid and estimate the chances of an overload or power surge.

To determine the correct phase for its location, each PMU is synchronized to a GPS satellite clock. However, if the PMU gets an incorrect GPS signal, every resulting calculation will be wrong, creating unforetold problems. A recent outage in the Pacific Northwest was traced to such an incorrect signal, which had been supplied accidentally by the wrong satellite. Led by Helms, Skyfall was used to prove that such a "spoofed" signal could be reproduced relatively easily by malicious agents. This finding, bolstered by the improved accuracy of the hardware-in-the-loop simulation, has helped the Department of Homeland Security work with vendors to guard PMU hardware and software against future accidents and attacks.

Another component of Skyfall is the Malicious Code Analysis Center (MCAC), which focuses on understanding the vulnerabilities in firmware and software for cyber–physical systems. MCAC is a library of malicious code and analysis tools, kept totally isolated from other networks, that could someday be used against cyber–physical systems. When used against Skyfall, researchers can safely gain critical insight into the worst-case scenarios for the nation's infrastructure. Donde explains that power relays such as the one connected to Skyfall have computer chips that run code. He says, "If someone hacks in and changes the logic of how the relay should operate, essentially the user would not know until the code were executed and something bad happened on the grid." With MCAC, researchers can see how bad software can affect power delivery and potentially damage the integrity of grid systems. "MCAC is like a sandbox where you can play and understand how code changes would work out on the actual grid," says Helms. "It's a realistic but safe environment."

Power Grid Security S&TR December 2018

The nation's power grid is integrated coast to coast by modern devices connected to an aging infrastructure. An accident or attack on one component could create cascading problems for huge segments of the grid. Skyfall is designed to model the network's behavior in such cases.

The Sky Isn't Falling

Cyberattacks will target the nation's infrastructure and accidents will happen, but Livermore's Skyfall test bed is constantly adding capability to strengthen its predictive powers and connect more closely with the Laboratory's missions and core competencies. In the future, Helms and Donde agree, Skyfall will further capitalize on the speed and efficiency afforded by Livermore's high-performance computing resources and continue expanding its hardware-in-the-loop approach to more types of critical systems. With the rise of automated vehicles, telecommunications, and renewable sources of power, the need is increasing for sophisticated, realistic simulation capabilities to help protect the complex infrastructure upon which the nation depends.

—Ben Kennedy

Key Words: cosimulation, energy, cyberattack, cyberterrorism, high-performance computing, electric grid, hardware-in-the-loop simulation, malware, Malicious Code Analysis Center (MCAC), phasor measurement unit (PMU).

For further information, contact Jovana Helms at (925) 423-3877 (helms7@llnl.gov).