The Internet of Things brings a web of promises and perils to the smart grid, experts say

October 27 2020, by John Roach

,

Credit: Timothy Holland | PNNL

The innocuous microwave on a shelf in a laboratory at the U.S.

Department of Energy's Pacific Northwest National Laboratory (PNNL) in Richland, Wash., is anything but ordinary.

"Weird," is how Penny McKenzie, a cybersecurity engineer at the laboratory, describes the device.

The microwave arrived at PNNL with the capability to be controlled through a smart speaker connected to the internet, a connection McKenzie and her colleagues declined when they plugged it into the wall.

"We have an energy measurement sensor connected to the microwave and at certain times of the day, the energy will spike up really high," McKenzie said. "We are looking at the network communications and it is constantly trying to [connect to the internet]."

McKenzie runs the Internet of Things Common Operating Environment (IoTCOE) at PNNL. The recently established lab focuses on solving current and future challenges in the cybersecurity of connected devices. The microwave is one of several dozen household devices McKenzie and her colleagues are researching in a growing list of things that can connect to the internet and the electric power grid.

PNNL scientists and engineers research energy and security issues, so they are well aware that Internet of Things (IoT) combined with technologies such as 5G telecommunications and artificial intelligence (AI) are ushering in an era of fine-grained insight and control over infrastructure from smart microwaves to the entire electric power grid.

"With a profusion of connected smart devices, you can gain a lot more insight quickly because you are making more measurements at a much higher resolution than you ever could before," said Bill Pike, a senior research scientist at PNNL. "You can spot trends and issues very early

and act quickly at a very local level to increase efficiency or mitigate risks."

For example, he explained, IoT sensors connected via 5G telecommunications are poised to unlock the promise of the smart grid, communicating with appliances in individual homes, such as clothes dryers and dishwashers about when to power on and off according to real-time price signals and lifestyle preferences.

On the flip side, he added, the growing number of connected devices increases the attack surface from a cybersecurity perspective. McKenzie's IoTCOE is one of several efforts within PNNL, throughout Washington State and around the country that are exploring how best to leverage the benefits of IoT while mitigating the risks.

IoT is everywhere and spreading

The first thing to know about IoT technologies is that no single thing defines them, noted Joseph Williams, director of PNNL's office in Seattle. Prior to joining PNNL in June 2019, Williams served as the Information and Communications Sector lead for the governor of the State of Washington. PNNL, he explained, is part of a broad IoT-related research and development ecosystem that spans academia, government, and industry in Washington.

This ecosystem, he noted, includes the autonomous trucks cruising around a test track at PACCAR's Technical Center in Mount Vernon, Wash., and Seattle-based Sentinel Healthcare's recently launched Sentinel Fever Tracker, a smartphone application that integrates with a digital thermometer to track people exposed to the novel coronavirus that causes COVID-19.

The smart water meters that the city of Walla Walla, Wash., deployed at

its 11,000 water accounts are also part of the IoT ecosystem. The meters detected more than 2,000 leaks in a single year, helping the wine grape growing region conserve water. Meanwhile, researchers at Washington State University are working with wine producers to use IoT sensors, big data analytics, and other hardware to optimize irrigation in vineyards.

PNNL is among several national laboratories and industry partners working with GE Global Research on cybersecurity research and development efforts based on GE's Digital Ghost platform. The platform uses IoT sensors and AI systems to create digital twins of high value assets, such as gas turbines to develop digital immune systems based on the physics of the assets.

The Digital Ghost is a novel way to monitor and optimize asset performance, as well as to detect, isolate and neutralize threats. The IoT-enabled AI technology, for example, can keep a power turbine and associated systems operating during a cyberattack.

"The ability to review the control logic and autonomously maintain operations without losing availability of critical systems is a potential game changer to cyber-physical resilience," said Michael Mylrea, a director at GE Global Research focused on cybersecurity research and development. He was previously the deputy director of grid cybersecurity research and development at PNNL.

McKenzie's IoTCOE looks to shore up the cybersecurity of the electric power grid from the other end. Consider, for example, the threat posed by the network-connected microwave. Without proper defenses, a cybercriminal could hack the device and use it as a portal to wreak havoc on the grid, she noted.

One goal of IoTOCE is to develop security measures and tools that can be installed on top of existing infrastructures, such as firewalls and virus

protection software to identify and block these types of malicious threats.

Managing the smart grid

IoT devices within homes and commercial buildings, such as sensors and controls for rooftop solar panels, security systems, and heating and cooling systems are transforming how the electric power system is controlled, according to Ronald Melton, who leads several PNNL projects related to smart grid technologies.

"We see a change in the whole nature of the electric power system," he said.

For example, instead of managing consumers' power supply from central sources, such as industrial-scale hydroelectric dams and coal-fired power plants, grid managers increasingly need to account for and manage the variation in supply and demand within the distribution system, including rooftop solar panels, storage devices and new uses like electric vehicle charging.

While distributed generation and storage resources increase complexity from a grid management perspective, they also provide grid operators with options to maintain electric service even if a disruption occurs to a bulk power station.

"To do this, we have to start distributing the control of the system out into the distribution system and we need to engage with assets behind meters," said Melton. One of his smart grid projects, GridAPPS-D, is an open-source software platform that allows researchers and utilities to develop and test grid architectures that efficiently offer this level of interaction.

According to Melton, grid operators are unlikely to control individual systems inside of homes and buildings, but rather could coordinate their behavior through economic or other incentives. For example, they may use data from whole buildings, office campuses, or other regional networks to facilitate energy transactions, such as paying a building to use less energy for half an hour to make up for demand elsewhere on the grid.

"We are working on technologies that can take advantage of more sophisticated control opportunities of buildings and homes to enable a more rich and robust interaction with the electric power system and the need to harness flexibility to offset variability," he said.

Cybersecurity of distributed energy

The growth of distributed energy resources brings with it the potential for increased cybersecurity risk, according to Adam Hahn, an assistant professor of computer science at Washington State University who studies cybersecurity for the smart grid.

Hahn and his colleagues are researching the potential impacts to grid operations if IoT devices like solar inverters or smart thermostats are compromised.

In the near term, his team has found that the risk is manageable, given the flexibility built into the grid that accounts for disruptions, such as the flow of electricity from rooftop solar systems. The greater the penetration of these devices, however, the greater the risk.

"It is great having more renewable energy," he said, adding that, "We just want to make sure that people who are thinking about deploying these devices are aware of the risks and are making sure that they have protections built in."

Convergence on the road ahead

On the road ahead, IoT will converge with 5G telecommunications and AI, further enabling the promise of systems such as smart grids, smart homes, and smart cities, according to Scott Godwin, general manager of corporate partnerships and alliances at PNNL.

Among the projects in Godwin's portfolio are PNNL's participation in the Washington State Department of Commerce's Innovation Partnership Zone focused on 5G and a recently announced partnership with Verizon to explore opportunities for 5G to impact national security and energy efficiency.

Given PNNL's expertise in energy and security, Godwin noted that these are natural areas for researchers to focus on at PNNL, especially as millions, perhaps billions, of hackable smart devices are connected to networks—including the electric power grid.

"That becomes a challenge for our cybersecurity professionals," he said.

The partnership with Verizon will allow McKenzie and her colleagues to set up a 5G network in the IoTCOE to explore how the transition to the next generation of telecommunications impacts IoT.

The microwave on the shelf in her laboratory serves as both a warning sign and a beacon of hope.

"It is very promising to know that with the devices we have, we will be able to do network mapping of IoT within a facility," she said. "We want to see what type of impacts those devices have."

Provided by Pacific Northwest National Laboratory