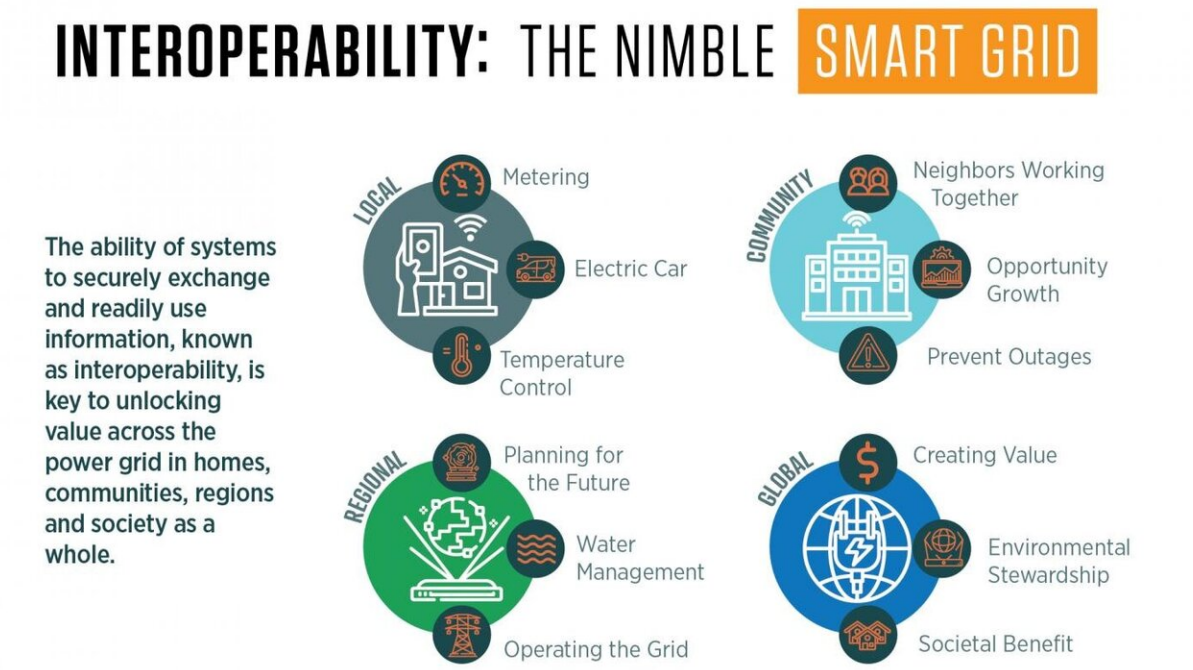
New NIST framework strives for cleaner, more secure power grid

February 18 2021



The ability of systems to securely exchange and readily use information, known as interoperability, is key to unlocking value across the power grid in homes, communities, regions and society as a whole. Credit: B. Hayes/NIST

Whether it's a new set of solar panels glistening on a neighbor's roof or a freshly installed smart thermostat at home, burgeoning renewable and

smart technologies represent steps toward a sustainable future. But much of their potential will remain untapped unless the power grid is managed in a much more flexible way.

The ability of systems to speak the same language and exchange information securely, known as interoperability—think syncing your phone to the cloud or your computer—is key to unlocking flexibility on the grid.

Researchers at the National Institute of Standards and Technology (NIST) aim to push interoperability on the grid further than before with the fourth and latest release of the Smart Grid Framework. The 4.0 version of the framework describes the economic and environmental benefits that could stem from enhanced interoperability and outlines a new strategy for supporting the development of interoperable devices and equipment. The authors also provide guidance and resources for grid cybersecurity, which is becoming increasingly important as greater numbers of devices connect with the grid.

A recent analysis has indicated that, even if all new power generators were zero carbon, continuing to operate the grid as we have for decades will cause us to fall short of a major goal of the Paris Agreement, which is to limit global temperature rise to 1.5 C (2.7 F). This finding underscores the need to displace emission sources with renewables. But several hurdles remain that make renewables a challenge for the current system to manage, such as how spread out they are and their fluctuating supply.

"Flexibility is needed to accommodate all of these new clean energy technologies," said NIST smart grid program manager Avi Gopstein, lead author of the framework. "The wind doesn't always blow, the sun doesn't always shine, and people change the amount of electricity they use depending on their activities. Well, interoperability is all about

providing flexibility."

Interoperable sensors and smart controls could give the grid the flexibility it would need to maintain service during rapid changes in supply and demand. And part of how they would get the job done is by allowing communication on the grid to become more of a two-way street (between customers and utilities and everything in the middle), making information about current power usage and anticipated need readily available to different parties. This way, customers would be able to expend resources more intelligently and help utilities route them to the right place at the right time.

An example of interoperability already at play is voluntary rewards programs offered by utility companies, Gopstein said. By using smart thermostats and water heater controllers that are interoperable with their utility's operations centers, participating consumers are able to contribute to reducing energy consumption during peak demand and receive financial rewards in return.

One of the framework's major offerings is the concept of interoperability profiles, detailed requirements for specific devices that could provide industry with clear targets for interoperability. The ultimate goal of the profiles would be to guide the development of testing and certification programs—a critical ingredient for the widespread use of technology.

"The reason Wi-Fi works on everybody's phone and computer and everything else is because the Wi-Fi Alliance has an effective testing and certification program," Gopstein said. "They established specific performance requirements and validation tests. For interoperability, we don't have that."

While there are many standard tests for physical performance (for

example, a way to check if a 5-volt power supply puts out 5 volts), interoperability is a much more difficult trait to test for.

Hundreds of communication standards exist, meaning there are a multitude of languages devices can speak and myriad ways they can package their messages to other systems. Rather than develop new standards, Gopstein and his team seek to bring subsets of existing standards for both physical function and communication together in profiles suited to specific types of devices.

If tests are developed based on profiles and widely accepted, manufacturers would have explicit guidance on how to make their devices interoperable with the grid. These tests could check for proper communication of information such as timing, which, for equipment like smart devices in substations, needs to be synchronized down to the millisecond for conversations between the machines to get off on the right foot.

Over time, as products become certified, the grid would become more of a plug-and-play ecosystem, giving customers more options to choose from.

Because the benefits of an interoperable grid would stem from greater connectedness and an increased flow of information between various parties, elements of the grid may become more vulnerable to malicious actors.

The North American Electric Reliability Corporation (NERC) provides a set of mandated security requirements for the high-voltage elements of the grid, such as transmission lines. But for everything else, formal guidance for cybersecurity is scarce, Gopstein said.

The framework offers resources to help fill in these gaps, including a

cybersecurity risk profile for the smart grid, which the authors made using NIST's Cybersecurity Framework. The profile, containing numerous security considerations specific to the grid, provides utilities and others with a structured method of assessing their current practices and identifying areas in need of beefed-up security. The authors also refer organizations to a previous NIST report on smart grid cybersecurity for more detailed guidance at the level of individual device interfaces.

Another important resource the framework recommends is a free tool that highlights overlap between NIST's Cybersecurity Framework and NERC's standards to help organizations improve their cybersecurity practices while ensuring they remain in compliance with mandated requirements.

More information: Avi Gopstein et al, NIST framework and roadmap for smart grid interoperability standards, release 4.0, (2021). DOI: 10.6028/NIST.SP.1108r4

Provided by National Institute of Standards and Technology