MICROGRID KNOWLEDGE

What's Ahead for the Future of Microgrids?

March 6, 2020
By Stephanie Pine

S&C Electric's Stephanie Pine describes the future of microgrids as they become more advanced, renewable, standardized, scalable and cybersecure.

Over the last few years, microgrid deployments throughout the world have increased. We should expect this trend to continue as **market projections point to steadily increasing annual microgrid capacity and spending**. U.S. microgrid growth could be further expedited by new opportunities emerging in California.

At this juncture, **microgrids** have practically become mainstream. But what does that mean for future microgrids? As they become more prevalent on the grid, what will these systems look like? Indeed, various important questions should come to mind for players in the market:

- Should we expect our development approach to change?
- What next steps will there be for the microgrid market in 5, 10, or 20 years?
- How can we expect systems to change and evolve?

Answers to many such questions will come in time, but the inquiries illustrate the challenges and opportunities the market should be prepared to address.

One major change we should expect is a sweeping transition from basic to advanced microgrids. We have seen

Stephanie Pine, manager, federal microgrid segment, at S&C Electric

a large portion of initial microgrid deployments fall into the basic microgrid definition, where they primarily serve as standby generation with the capability to island from the main grid.

With increasing legislation mandating more communities and states reach net-zero carbon emissions, paired with a greater integration of renewables to the grid, we are seeing a larger adoption of renewables and distributed energy resources (DERs), and this is influencing a shift toward more advanced microgrid development. And this brings up another key question: Is the increased complexity of microgrids linked to the growth of renewables?

The short answer is, yes. To successfully, and safely, integrate more renewables and DERs into the grid, microgrids must fulfill advanced operational criteria. But, is this push led by the integration of additional renewables, or by the capabilities of advanced microgrids? While this is a bit of a chicken-or-the-egg scenario, the sheer volume of microgrid deployments we are seeing, in conjunction with the complexities of the grid, are driving advanced microgrids to become the norm.

> *To best protect future microgrids, comprehensive cybersecurity standards must be considered. Leveraging lessons learned from U.S. Department of Defense cybersecurity requirements, including the implementation of third-party validation and testing, should be a standard practice for all microgrids, not just federal ones.*

As these advancements continue, the market will shift toward a standardization for microgrid deployment. We have already accepted a microgrid controls standard, IEEE 2030.7-2017, and other standards related to microgrids also are being developed. Systemic microgrid standardization is the next logical step. These standards have wide-ranging benefits, supporting everyone in the market, from developers to users.

continued on next page

The combination of more microgrids and standardization should make scalability simpler. It's not difficult to imagine a time soon when the industry has so many deployed microgrids that scalability will be basic requirement, saving developers from having to "start from scratch" each time they begin a new microgrid project.

To best protect future microgrids, comprehensive cybersecurity standards must be considered. Leveraging lessons learned from U.S. Department of Defense cybersecurity requirements, including the implementation of third-party validation and testing, should be a standard practice for all microgrids, not just federal ones.

The trend toward standardized microgrids will follow a similar path to that of microgrid controls. As microgrid development has progressed, we have seen real-time operations and have learned more about how these systems best operate. In turn, control systems have evolved to best meet these needs. Through this evolution, more assets are integrated within each system as controls and microgrid development have grown in parallel. With the industry's increased experience, the market can move past basic controls and develop new industry standards to integrate more sophisticated controls into future microgrid designs.

A positive result of this shift to microgrid standardization and controls advancement will naturally lead to more standard use cases. Today, microgrids are often designed to meet a limited number of use cases available, only achieving a microgrid's basic functionality.

Increased microgrid deployments will bring broader sets of standard use cases, shifting the fundamental expectations of what a microgrid could and should deliver. Standard use cases will address storm preparedness, additional renewables, bidirectional charging, cyber intrusions, and economic optimization. As control systems evolve, these future standard use cases will encompass even more sophisticated applications.

With microgrid growth, more market challenges and opportunities will emerge, leading to increased uncertainty. Will we see a push to use new technology to update existing basic microgrids to advanced microgrids? Will we see more vehicle-to-grid solutions as microgrids and electric vehicles come together to provide power in a bidirectional way — helping charge the vehicles and support the grid at the same time?

Transportation and vehicle electrification continue to be important factors for cities striving to achieve their carbon emissions goals. Thus, the increased integration of electric vehicles and associated charging stations will certainly have an impact on the microgrid market.

Indeed, when microgrid growth brings more and more of these systems into large urban areas, the conversation around cybersecurity requirements will need to change from what-if conversations to establishing new and rigorous requirements. Moreover, when considering utility or commercial and industrial microgrid installations, cybersecurity requirements vary substantially.

To best protect future microgrids, comprehensive cybersecurity standards must be considered. Leveraging lessons learned from U.S. Department of Defense cybersecurity requirements, including the implementation of third-party validation and testing, should be a standard practice for all microgrids, not just federal ones. To have microgrids successfully serve as a new backbone for the grid, we must ensure all assets involved are protected. As microgrids continue to evolve, it will be interesting to see whether this progression promotes broader applications for other non-wires alternatives solutions as well. As the grid continues to change, more and more "non-conventional" solutions, like microgrids, will be critical to meet future power demands.