For more information: jeffprice@gridoptions.com

RESILIENT COMMUNITY GRIDS AS A GRID PROTECTION MEASURE

The electric power industry has long strived to ensure that its operations at both the bulk power and distribution levels are not interrupted and, if interrupted, are rapidly restored so that customers experience only rare and short power outages. Until recently, efforts to ensure uninterrupted service focused almost exclusively on reliability[1] as measured by various statistical metrics, and the preponderance of those effort have been on the distribution system where most outages occur. Such outages have typically been short, in the range of a few minutes to a few days.

Since the mid-2010s events such as Superstorm Sandy, major damaging hurricanes, sniper attacks on substations, threats of Electromagnetic Pulse (EMP) attacks, and continuing cyberattacks have taken place. All this raises concern about the potential for widespread, long-lasting—and unexpected—outages creating "black sky days" during which the electric power is lost for communities and critical infrastructure that provides vital services. Resilience, defined by the Federal Energy Regulatory Commission (FERC) as "the ability to withstand and reduce the magnitude and/or duration of disruptive events, which includes the capability to anticipate, absorb, adapt to, and/or rapidly recover from such an event,"[2] became an industry goal, but with widely different interpretations of exactly what resilience is and how to achieve it.

Resilience concerns are increasing as the electric power sector undergoes its most significant transformation in a century. This transformation includes increased penetration of distributed energy resources, evolving wholesale and retail power markets, new industry participants and business models, changing regulatory mandates, power flows changing from one-way to two-way, decarbonization, digitization, and use of cloud computing. These changes complicate the quest for resilience, which is also constrained by legacy systems for both physical and data systems.

Against all this background, four protective measures consisting of various systems and practices are used to improve both the reliability and resilience of the electric grid[3]:

1. Protection systems,
2. System restoration practices,
3. Threat hardening, and
4. Remedial action schemes.

Each of these measures was developed to assure system reliability, not resilience. The challenge is how to adapt or add to them to address resilience, especially for black sky days. Resilient Community Grids provide a means of effectively meeting that challenge.

1. Protection Systems

Protection systems safeguard electric grid components from conditions that could cause damage to those components or to a section of the power system until those conditions can be corrected, for example, equipment being reset, fixed, or replaced or by grid conditions being stabilized.

---

[1] Operating reliability is defined by the North American Electric Reliability Corporation (NERC) as "the ability of the electric system to withstand sudden disturbances such as electric short circuits or unanticipated loss of system components."

[2] As defined in FERC Docket No. AD18-7-000, the most relevant definition for the power industry.

[3] Microgrids, by contrast, protect individual facilities, campuses or small communities and are not designed to protect regional grids.

Typically, protection systems consist of devices distributed throughout the electric grid, often at substations. These may include:

- Protective relays which detect abnormal system conditions and initiate with a control response;
- Circuit breakers that open and close electric lines based on commands;
- Communications systems for protective functions and to inform grid operators;
- Sensing devices for parameters such as voltage, current, phase, impedance, or system stability;
- Redundancy with overlapping zones of protection or alternative circuit paths;
- Direct current supply to most protective functions (e.g., batteries, battery chargers, etc.); and
- Control circuitry for the protective functions.

Usually, protection devices automatically and rapidly initiate action locally and without central control, although, especially with modern digital protective devices, the action and its location and timing are communicated to system operators so that any further corrective actions needed can be promptly taken. One challenge is that many legacy devices still in common use are electromechanical and less flexible, while modern digital devices can be more readily monitored, reset, or reprogrammed.

2. System Restoration Practices

The electric power industry routinely restores power from outages caused by the types of incidents with which it has had experience. The industry has extensive contingency plans and experience with routine outages, even some that are quite severe. Repair crews are sent out, spare equipment is stockpiled, and utilities cooperate with each other during severe outages. Priority loads are identified and, if possible, have power restored first.

If a section of the transmission grid including power generation facilities is affected by an outage, "black start" procedures may be implemented. Black start is the restoration of an electric power station or part of an electric grid to operation without relying on outside electric power. Black start involves systematically re-energizing circuits that are not operating and then restarting and resynchronizing electric generators by providing cranking power to rotating machinery.

Restoration is only possible if the damage to the grid is limited to what can be addressed by existing resources. This may not be the case during black sky days.

3. Threat Hardening

Threat hardening consists of constructing, modifying, or replacing key components of the electric grid endangered by one or more threats so that the new or hardened equipment can withstand incidents involving one threat or combination of threats. Examples include:

- Cybersecurity for both information technology (IT) and operational technology (OT);
- Geomagnetic storm and EMP hardening of key components and control systems;
- Hardening substations from physical attacks;
- Microgrids which are often implemented by consumers;
- Vegetation management historically to protect power lines, increasingly to prevent wildfires;
- Raising equipment above potential flood levels; and
- Storm hardening of transmission towers.

4. Remedial Action Schemes

Remedial Action Schemes[4] consist of equipment and procedures designed to detect predetermined harmful system contingencies, and then automatically and rapidly take corrective actions at a larger scale than protection systems before those conditions can harm the power system. These are essentially hardwired contingency plans. They may include, but are not limited to, curtailing or tripping generation or other power sources, curtailing load, reactive power compensation, and reconfiguring or sectionalization of the power system. NERC requirements for Remedial Action Schemes are that they meet its Reliability Standards for system stability, system voltages, acceptable power flows, limiting cascading, and other bulk electric system reliability concerns. They are individually tailored to the specific grid design and conditions and can be quite complex.

Unique Aspects of Resilient Community Grids

The four protective measures have historically been designed to provide reliability, <u>not resilience</u>. They do not individually protect the grid from the extreme threats that cause black sky conditions, especially combined threats involving a strategic adversary. All four are needed together and must be organized strategically and operated systematically to address the extreme and unexpected. That is what Resilient Community Grids achieve, and that is a key difference.

Another key difference is a separate, cybersecure, control and communication system "invisible" during normal grid operation that is ready to take over for an extended period, if needed, and able to operate independently of the grid for long periods. Multiple such systems vastly complicate any hacker's ability to damage on the grid.

The four current protective measures enable the electric power system to continue to operate normally or to restore normal operation after relatively short periods of interruption, typically a few days or less. They address well-known and routine causes of outages, often internal to the power system and are primarily focused on reliability. By contrast, a Resilient Community Grid is designed for long-term operation of a vital grid section throughout extended black sky events.

Resilient Community Grids uniquely combine each of these four measures to enables a section of a regional electric grid containing a community's critical infrastructure to stay operating. Although having other functions, they can be thought of as a new type of Remedial Action Scheme designed to keep in operation the critical infrastructure that makes communities and the nation safe during extreme events. Unlike most Remedial Action Schemes, they are customer facing in that they are specifically designed to serve and selectively prioritize critical loads. In addition, many Remedial Action Schemes protect the electric grid from damage that its own components may cause through their improper operation, that is, from inside the grid. By contrast, a Resilient Community Grid keeps a section of the power system running without damage from either inside or outside. It can be used in conjunction with other Remedial Action Schemes to protect from damage from both inside and outside the power system and to create a layered defense. Further differences from other Remedial Action Schemes are the abilities to:

- Incrementally expand the facilities protected, resources used, and threat protections;
- Readily utilize high penetrations of distributed energy resources and microgrids;
- Provide a platform for accommodating changes to the electric grid and electric sector; and
- Address potential constraints not part of the electric system, such as fuel supply.

[4] Also called "Special Protection Systems" or "Wide-Area Monitoring, Protection, Automation, and Control (WAMPAC)" systems.