Smart Grid Implementation Workshop

Breakout Group Report

Operating Resiliently Against Physical Disruptions, Cyber Attack, and Natural Disasters

June 20, 2008

Washington DC

Major Findings/Caveats

- Address all hazards
- Change “attacks” to “events” – inadvertent or deliberate
- Resiliency includes design, policies, procedures, etc.
- Appropriate levels of security (graded approach)
- Defense in-depth
  - Deter, prevent, detect, react, recover, risk assessment
  - End-to-end security
- Threat is beyond our control – look at vulnerability and consequences as part of risk assessment
- Consider systems development life cycle and lifetime of assets

Metrics for Measuring Progress

- Operating entities exhibit progressively mature characteristics of resilient behavior
  - Tailor existing resiliency scales (e.g., SEI, APQC MM), give companies ratings (benchmarking), track progress over time
  - Ensure consistency with NERC standards
- Tag standard metrics (e.g., SAIDI, SAIFI, CAIDI) and capture those contributed to by physical and cyber events
- A measure of the number of alternative, independent means to control and supply power to any load point on the distribution grid
  - Also alternative means within supply chain
- Increasing confidence and understanding of integrated operating margins and Smart Grid capabilities
  - Reduce estimation, increase measurement (info, not data)

Issues with Data, Methods, Analysis

- Complexity (amount and communication dependency of data)
  - Lack of complex systems engineering expertise
  - Need for additional applications that can analyze the data effectively
  - Information available in timely and prioritized manner to right place
  - Interdependence on other infrastructures (e.g., communication)
- Data scalability and accuracy (uncertainty)
- Crossing functional boundaries in supply chain (distribution, transmission, customer, etc.)
  - Regulatory and legal impediments (e.g., lack of information transparency from market concerns)
  - Culture issues – IT vs. operations, transmission vs. distribution, etc.
- Integrity, availability, and confidentiality of information
- Economics and personnel shortages (risk management)
- Lack of deployment of digital devices and need for integration of legacy systems
  - E.g., version control, patching, firmware, upgrading
- Defining and achieving consensus on scenarios to establish baselines

Path(s) Forward

- Establish metric development methodology and process
  - Take current baseline of metrics we already have
  - Identify goals
  - Lay out the roadmap
  - Identify the gaps in process or information
  - Caveat: Each metric will have separate implementation pathway
- Identify regulatory impediments to tracking these metrics (e.g., restrictions on information sharing)
  - Then determine what regulators need to reduce or eliminate impediment
- Identify who will fund the facilitation of the metrics
- Identify who will coordinate data sharing and where it is shared, as appropriate

Suggestions for DOE

- Continue to fund RD&D projects that address the issues identified
  - E.g., provide high-speed (e.g., distributed) computing to migrate planning tools to real-time operating models and visualization
  - Fund metrics development process
- Help share lessons learned, good and bad
  - Act as source of authoritative information
    - Establish registry of defined metrics and methodologies
  - Actively participate in standards process (with NIST, IEEE, IEC, etc.)
- Interagency coordination
  - Improve coordination with DHS for interdependency analysis
  - Establish liaison with NSF cyber/physical systems program
    - Can DOE incentive or subsidize education resources to get students to go into this area?
- Provide plan within 6 months for what DOE will do to act on workshop findings