Purpose and Deliverables

The purpose of the Task Force is to assess the reliability impacts of integrating Smart Grid technology on the bulk power system. The Task Force has prepared a report, titled Reliability Considerations from the Integration of Smart Grid, which reviewed Smart Grid characteristics, identifies reliability concerns including cyber-security vulnerability, and provides recommendations to NERC and the industry. The task force will now complete the work plan outlined in this report, including:

1. Integration of smart grid devices/systems requires development of new planning/operating tools, models and analysis techniques
2. Integration of smart grid devices/systems will change the character of the distribution system, potentially affecting bulk power system reliability
3. Engage Standard Development Organizations in the U.S. and Canada to increase coordination and harmonization in standard development
4. Develop risk metrics that measure current and future system physical and cyber vulnerabilities from smart grid integration

Approach and Milestones

Follow-on work for these tasks will focus on those smart grid devices/systems that are most likely to have an impact on planning and operations. These efforts address Item #K (Smart Grid Security) of the ESCC Critical Infrastructure Strategic Roadmap and the Technical Committee Critical Infrastructure Protection Coordinated Action Plan. 2

---

1. Integration of smart grid devices/systems onto the bulk power system requires development of new planning/operating tools, models and analysis techniques.

   The goal of this effort is to identify the tools and models needed by planners and operators to ensure the reliability of the bulk power system is maintained with the integration of smart grid devices/systems.

   **SGTF - Planning/Operations Subgroup**  Start Date: 1st Qtr. 2011  End Date: 2nd Qtr 2012

   Review modeling requirements for planning/operations to measure and understand system performance while accommodating smart grid integration:

   - Identify bulk power system modeling requirements for bulk power level smart grid devices/systems, communications, IT and control system interfaces.
   - Evaluate how to include cyber security and control system interfaces into planning/operations simulations to enhance control system security.
   - Assess the impact of bulk system smart grid devices/systems on system stability.
   - Review the Modeling, Data and Analysis (MOD) and Critical Infrastructure Protection (CIP) Standards for improvements.
   - Provide input into smart grid security and NERC’s Standards processes as applicable.

2. Integration of smart grid devices/systems will change the character of the distribution system, potentially affecting bulk power system reliability.

   The primary goal of this group is to assess if the changes promulgated by the smart grid devices/systems on the distribution system can affect bulk power system reliability.

   **SGTF - Planning/Operations Subgroup**  Start Date: 1st Qtr. 2011  End Date: 4th Qtr 2012

   Review existing and new distribution smart grid devices/systems and assess if there are any potential failure modes that might be introduced by their integration.

   - Identify bulk power system modeling requirements for distribution level smart grid devices/systems, communications, IT and control system interfaces.
   - Evaluate how to include the affects of distribution-level cyber security and control system interfaces in the modeling/simulation of bulk power systems.
   - Assess the impact of distribution smart grid system devices/systems on system stability.
   - Review the Modeling, Data and Analysis Standards (MOD) and Critical Infrastructure Protection (CIP) Standards for improvements.
   - Provide input into smart grid security and NERC’s Standards processes as applicable.
3. Engage Standard Development Organizations in the U.S. and Canada to increase Coordination and Harmonization in standard development

The primary goal of this effort is to form liaisons with U.S., Canadian standard setting groups to ensure they are coordinated and harmonized to support reliability.

SGTF - Cyber Security
Start Date: 1st Qtr. 2011
End Date: 4th Qtr 2013
Create pathways for harmonization and coordination.

- Monitor smart grid developments and remain engaged in its evolution (Federal/State/Provincial efforts, ISO/RTO, IEEE/IEC, etc.)
- Review existing and new standard developments
- Identify those standards that are vital to bulk power system reliability, including cyber and control system security
- Work with Canadian and US standards setting organizations to ensure coordination and harmonization of vital standards
- Report back on ongoing activities to the PC and CIPC

4. Develop risk metrics that measure current and future system physical and cyber vulnerabilities from smart grid integration

The primary goal of this effort is to further refine “Defense-in-Depth” and risk assessment approaches to manage cyber and physical security with smart grid integration

SGTF - Cyber Security
Start Date: 1st Qtr. 2011
End Date: 4th Qtr 2012
Refine and test “Defense-in-Depth” and risk assessment approaches

- Further refine technical methods
- Identify characteristics that should be measured to provide a current reference and future system measurement
- Form metrics of performance and risk
- Pilot the approach for bulk power system application
- Further refine as required
- Develop a report outlining the methods and documenting the results
- Report back on ongoing activities to the PC, OC and CIPC

Background
The integration of Smart Grid and associated technologies into many levels of the electric system may have bulk power system reliability considerations. While wise Smart Grid integration may present significant opportunities to improve monitoring, security, and power flow, a failure to adequately address the reliability considerations in the planning, design, and operation of the bulk power system could present reliability risks and challenges. While many of the technologies currently associated with Smart Grid have
been available for several years, others are yet unproven; and a rapid integration of all these devices with their associated control and data systems will present significant change in the electric industry that may potentially impact bulk power system reliability. Further, as interoperability has been proposed as the foundation for Smart Grid functions, cyber-security reliability considerations should be integrated to ensure bulk power system reliability is maintained.

Therefore, this NERC task force will review the implications of Smart Grid integration on power system planning, design, security, and operations as well as review NERC’s Reliability Standards to identify any enhancements and gaps.

**Membership**

NERC will seek task force membership from industry, security, and vendor subject matter experts, with final selection subject to the approval of the chair of the Planning Committee. Members must be willing to commit their time to participate in the task force discussions and contribute to writing the final report.

Each member may designate one alternate to ensure availability. Leadership positions (Chair and, if required, Vice Chair) will be approved by the chair of the Planning Committee.

Initially, the Task Force will be organized as outlined below:

- **Leadership Team**
  - Chair
  - Vice Chair (if required)
  - Team leaders
    - Planning/Operations Tools, models and analysis techniques
    - Distribution System Implications
    - Standard Development Organization Harmonization
    - Physical/Cyber risk metrics for use in smart grid deployment

- **Liaisons from Demand Response Data Task Force (DRDTF), Critical Infrastructure Protection Committee, Operating Committee, National Institute of Science and Technology (NIST), and the National Energy Board - Canada**

- **Members**
- **Observers**
- **NERC Staff**
Governance

The task force reports to the Planning Committee and its final work products will be subject to PC review and approval.

Meeting

Meeting and conference calls will be scheduled as needed.

Approved by the Planning Committee: December 8, 2010