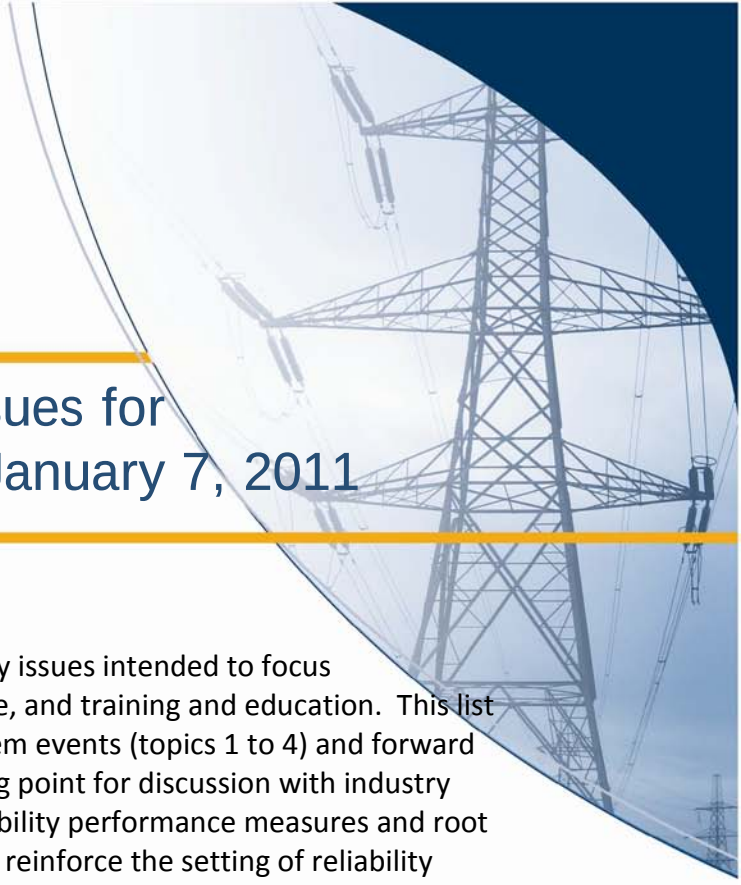
NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION



NERC President's Top Priority Issues for Bulk Power System Reliability – January 7, 2011

Background

Outlined below is a preliminary set of high priority reliability issues intended to focus ERO program areas, including standards setting, compliance, and training and education. This list is based partially on experience from reviewing actual system events (topics 1 to 4) and forward looking issues (topics 5 to 8). This list is offered as a starting point for discussion with industry experts. In the next few years, it is expected that new reliability performance measures and root cause analysis methods being initiated by NERC will further reinforce the setting of reliability priorities. The goal is to develop a list of priorities to focus work in the one to three year horizon on those areas most likely to have a positive impact on bulk power system reliability. This is a list of technical issues, and does not address a number of policy matters that could be addressed in an alternative forum such as a reliability summit. The list is in rank order.

1. **Misoperations of relay protection and control systems** – Nearly all major system failures, excluding perhaps those caused by severe weather, have misoperations of relays or automatic controls as a factor contributing to the propagation of the failure. Protection systems are designed to operate reliably when needed under the presence of a fault on the system, to quickly isolate a piece of equipment or a 'zone' of the bulk power system, without allowing the fault to transfer into adjoining facilities. The greater the number of facilities involved in an event, the more severe the impact to the rest of the bulk power system, with cascading failure such as resulted from the "Zone 3 Relay" issue in the August 2003 blackout being the extreme. Relays can misoperate, either operate when not needed or fail to operate when needed, for a number of reasons. First, the device could experience an internal failure – but this is rare. Most commonly, relays fail to operate correctly due to incorrect settings, improper coordination (of timing and set points) with other devices, ineffective maintenance and testing, or failure of communications channels or power supplies. Preventable errors can be introduced by field personnel and their supervisors or more programmatically by the organization. Adding to the risk is that system protection is an extremely complex engineering field –there are many practitioners but few masters.

2. **Human errors by field personnel** – Field personnel play an important role in the maintenance and operation of the bulk power system. They often are switching equipment in and out of service and aligning alternative configurations. Risks can be introduced when field personnel operate equipment in a manner that reduces the redundancy of the bulk power system,

sometimes even creating single points of failure that would not exist normally. Taking outages of equipment to conduct maintenance is a routine and necessary part of reliable bulk power system operation. However, any alterations to the configuration of the network must be carefully planned in advance to minimize loss of redundancy and avoid unintended single points of failure. It is also important that such changes and risks be communicated to system operators and reliability coordinators in advance, so that they can make adjustments in their operating plans and reliability assessments.

3. **Ambiguous or incomplete voice communications** – Out of longstanding tradition, system operators and reliability coordinators are comfortable with informal communications with field and power plant personnel and neighboring systems. Experience from analyzing various events indicates there is often a sense of awkwardness when personnel transition from conversational discussion to issuing reliability instructions. It is also human nature to be uncomfortable in applying formal communication procedures after personnel have developed informal styles over many years. Confusion in making the transition from normal conversation to formal communications can introduce misunderstandings and possibly even incorrect actions or assumptions. Further, once the need to transition to more formal structure is recognized, the transition is often not complete or effective. Results can include unclear instructions, confusion whether an instruction is a suggestion or a directive, whether specific action is required or a set of alternative actions are permissible, and confusion over what elements of the system are being addressed.

4. **Right-of-way maintenance** – The August 14, 2003 blackout highlighted effective vegetation management programs as a key recommendation for avoiding future cascading failures. More broadly, any encroachments in the right-of-way that reduce clearances to the point of lowering facility ratings or reducing the randomness of possible contacts can be a risk to reliability. Although these impacts may not always be readily apparent, under extreme wind and temperature conditions they may become more of a risk to bulk power system reliability. There are many challenges to effective right-of-way maintenance, especially maintaining proper clearances, including interventions by private landowners, local municipalities, and federal and state landowners.

5. **Changing resource mix** – Energy and environmental policies along with energy markets are driving proposals toward unprecedented changes in the resource mix of the bulk power system. Examples include integration of significant amounts of renewable (variable such as wind and solar), natural gas, storage and demand resources to provide energy and capacity. Industry's knowledge of the characteristics of the bulk power system comes from nearly a century of operational experience with the existing resource mix. However, integration of these new resources results in operating characteristics significantly different from conventional steam production facilities. An array of reliability services must be provided over a range of time horizons from seconds to minutes to hours and days, and annually such as load following, contingency reserves, frequency response, reactive supply, capacity and

voltage control, and power system stability. Continued reliable operation of the bulk power system will require an industry dialog with policymakers and regulators. Understanding the impacts on reliability will depend on accurate modeling of new resources, and development of new methods and tools for the provision of essential reliability services.

6. **Integration of new technologies** – Introduction of electric vehicles, demand-side management, variable generation, distributed resources and smart grid technologies presents tremendous opportunities but also introduces changes to the operating characteristics of the bulk power system. Integration of these new technologies requires changes in the way the bulk power system is planned and operated to maintain reliability. Further, additional tools/models are required to support their integration to meet policy and strategic goals. Without these changes, it will be challenging to maintain reliability with large-scale deployments. For example, some smart grid devices/systems increase exposure to cyber threats, while variable generation requires additional ancillary services. Integration of these new technologies must be achieved in a manner that does not undermine existing levels of stability, resilience and security of the bulk power system.

7. **Preparedness for high impact, low frequency events** – Although there is a wide range of threats labeled 'high impact, low frequency,' the greatest concern is being prepared for possible events that could debilitate the bulk power system for extended periods, such as widespread, coordinated physical/cyber attacks or geomagnetic storms. The industry must consider improving the design of the bulk power system to address these potential risks and prepare coordinated North American response plans for use during catastrophic events and be ready to deploy those plans to restore essential services in a timely manner.

8. **Non-traditional threats via cybersecurity vulnerabilities** – Establishment of enterprise risk-based programs, policies and processes to prepare for, react to, and recover from cybersecurity vulnerabilities is a high priority for the industry. The bulk power system has not yet experienced wide-spread cyber-attacks and a contributing factor has been the traditional physical separation between the industrial control system/SCADA environment and the business and administrative networks. This situation however is rapidly changing, predominantly due to the efficiencies that can be achieved by leveraging shared networks and resources so now even physically separated environments are susceptible. For example, the bulk power system could be as vulnerable to digital threats as IT systems, but with far more critical implications as the recent Stuxnet virus has shown. Disabling or turning systems off in a binary fashion is concerning enough but as illustrated by Stuxnet, industrial control system software can be changed and data can be stolen without intrusions even being detected. These injection vectors serve as a blueprint for future attackers who wish to access controllers, safety systems, and protection devices to insert malicious code targeting changes to set points and switches as well as alteration or suppression of measurements.