Written Testimony
Hearing of the U.S. Senate Energy and Natural Resources Committee
October 11, 2018

Thomas J. Galloway Sr.
NATF President and CEO

The purpose of the hearing is to examine black-start, which is the process for returning energy to the power grid after a system-wide blackout, and other system restoration plans in the electric utility industry.

I. Background

Chair Murkowski, Ranking Member Cantwell, and members of the committee – thank you for inviting me to testify on black-start and other restoration considerations in the electric utility industry. My name is Thomas (Tom) J. Galloway and I am the president and CEO of the North American Transmission Forum (NATF).

The NATF is a voluntary membership of transmission owners and operators, formed in response to the August 2003 blackout, with a mission to *promote excellence* in the reliable, secure, and resilient operation of North America's electric transmission system. The NATF was modelled after the Institute of Nuclear Power Operations (INPO), which has a analogous mission for the commerical nuclear power industry. The NATF's 89 members include investor-owned, municipal, cooperative, U.S. federal, and Canadian provincial utilities, as well as ISOs and RTOs, and together represent over 80% of the peak electrical load in the U.S. and Canada. The NATF is built on the principle that timely sharing of detailed information—best practices, operating experience, lessons learned, and areas for improvement—among its members is key to advancing transmission system performance beyond mandatory levels, especially during times of rapid industry change[1].

Bulk power system reliability and resiliency are closely related characteristics with some important distinctions. In the NATF's context, reliability expresses how seldom portions of the system "fail" or become undependable due to traditional impacts like equipment malfunctions and tree contacts. These impacts cause outages of varying frequency and duration that can disrupt end users. In the most extreme cases, such as the August 2003 blackout, the compounding of several "traditional" impacts can result in cascading outages that affect a large geographic area for days or even weeks. Resiliency involves severe, infrequent, and often non-traditional impacts. These high-impact, low-frequency (HILF) impacts—also called "gray sky" and "black sky" days—include threats such as extreme natural events or a postulated coordinated cyber-physical attack, respectively. In the most extreme cases, gray sky or black sky events are presumed to extend weeks or longer.

Mandatory reliability standards play a key role in reliability and resiliency, but other more-agile solutions are becoming ever more important given the pace of industry change and evolving threats. Accordingly, the NATF has placed increasing focus on resiliency in recent years. The NATF's resiliency approach considers that a severe impact, however unlikely, could occur; therefore, it necessitates advanced planning, hardening, processes to "operate through" the impact, and restoration strategies based on various considerations, including geographic scope, types of equipment involved/damaged, expected duration, cross-sector implications, and causes. Since severe-impact events could result in long-duration outages, alignment on restoration priorities, cross-sector collaboration, mutual aid, and robust communications are critical.

[1] For more information, please visit www.natf.net

In addition to confidential work, the NATF has shared select resiliency documents publicly, including ones focusing on the topic of supplement operating strategies (SOS) that deal with a broad loss of important operator tools during these types of events. Further, the NATF has engaged with the Department of Energy (DOE) and others on a standardized framework for response to a declared Grid Security Emergency (GSE).

II. Key Points

My testimony will cover five main points as listed below. In addition, I've included applicable attachments.

1. ***Restoration plans, priorities, and performance vary greatly based on the outage***
   Outage factors, such as geographic scope, duration, and involved elements and equipment; conditions, including the ability to move needed resources into affected areas; and specific cause(s) all greatly influence restoration. Black-start resources are rarely used but critical when portions of the system cannot be re-energized using an interconnection with adjacent, energized systems.

2. ***Natural events (severe weather) have caused the majority of recent significant outages***
   Weather influenced 9 of 10 of the most severe outages from 2008–2016. And that pattern has continued with hurricanes Irma, Maria, and (recently) Florence. While those impacts have been profound, lessons learned have been applied and system robustness has increased; over time, restoration performance has improved comparatively in many instances. Many of these enhancements support improved resilience for other, potentially more-severe non-weather-related events.

3. ***Bulk power system changes underway increase operational and restoration complexity***
   The scope and pace of industry change is unprecedented, including new dynamics in generation fuel mix, new technology, regulation, economics, and public-policy priorities. These changes provide various benefits but, in some cases, increase the complexity of both operating the bulk power system and restoring the system from outages.

4. ***Beneficial "no regrets" actions are being implemented***
   Significant efforts are underway to educate on threats, harden the bulk power system, ensure adequacy of key spares, augment mutual aid, enhance restoration plans, conduct comprehensive drills and exercises, and increase coordination—both cross-sector (e.g., gas, water) and with governmental partners (FERC, the DOE, etc.). The NATF is promoting an "all hazards" approach, with focus on actions that provide benefit under various scenarios.

5. ***Going-forward emphasis***
   Rather than create new or revised standards focused on individual resiliency hazards, FERC and the ERO should emphasize "no regrets" activities applicable to a range of resiliency hazards. The ERO should increase work with regulated entities and state regulators to align on system resiliency priorities and promote recovery for prudent investments (e.g., diverse and redundant black-start). The current grid command and control hierarchy is very effective and will be so in black sky events if communication capabilities are sufficient. Added focus on strengthening communications—technology, redundancy, diversity, and protocols—is essential.

III. Point 1: Restoration plans and priorities vary based on the outage

Outage factors, such as geographic scope, duration, and involved elements and equipment; conditions, including the ability to move needed resources into affected areas; and specific cause(s) all greatly influence restoration. Black-start resources are rarely used but critical when portions of the system cannot be re-energized using an interconnection with adjacent, energized systems.

Geographic scope

Generally, a broader geographic outage scope results in a more-difficult restoration and greater likelihood of reliance on black-start resources. In most outages, adjacent energized systems can be relied on to help restore power to the blacked-out sections. In addition, most electric utilities have a prioritized list of customers for restoration based on the local criticality of those loads, contractual obligations, etc. As the scope extends to multiple companies or regions, however, the likelihood increases that restoration priorities will not fully align. Reliability Coordinators and others with a wide-area view effectively assist in prioritizing restoration, but prioritization challenges further increase when scope exceeds available restoration resources (personnel and equipment) or other sectors (e.g., natural gas, communications, etc.) are involved. For example, electrical service to assets needed for generation fuel delivery may take on a higher priority in certain restoration scenarios.

Duration

Outage restoration from most traditional impacts is typically measured in minutes, hours, or occasionally days. As the expected outage duration extends to many days to perhaps weeks, restoration priorities must be re-evaluated and revised. Outages of very significant duration can be further complicated by evacuation of residents (rather than sheltering in place) and prohibiting access to affected areas by other than essential personnel (restoration crews, first responders, etc.).

Specific location – including the ability to move needed restoration resources into affected areas

Outage location and local conditions directly influence the restoration. Factors such as flooding or extreme cold and the ability to physically move restoration resources into the area influence restoration priorities and plans. As an example, during Hurricane Florence, significant flooding impeded restoration efforts. Similarly, restoration activities in Puerto Rico following Hurricane Maria were significantly complicated by the logistical challenges associated with moving resotration personnel and equipment to the island.

Criticality of Loads

Certain loads are by definition more critical, such as prompt restoration of offsite power to nuclear power plants. Further, if the outage impacts defense-critical installations, restoration priorities from a national security perspective may compete with local priorities, such as restoration to hospitals. Outages impacting those types of critical loads greatly influence restoration priorities.

Involved elements and equipment

Most outages from traditional impacts are distribution-centric. Distribution circuits are at lower voltage, provide power to a smaller subset of customer loads, and typically are not cost-effective to harden to the same extent as transmission level assets.

Some outages are generation-centric—such as the January 2014 "Polar Vortex" event (see NERC review – September 2014)—and require different restoration approaches.

Outages, even extremely large ones, can occur with limited equipment damage. For instance, the August 2003 Northeast blackout that interrupted power to about 40 million people was precipitated by vegetation contacts resulting in a cascading outage. Weaknesses in operator tools used to monitor the system delayed intervention to curtail the event. However, there was limited equipment damaged during the event. And while some customers were without power for extended periods, restoration to the majority of the system was accomplished in a few days.

Outage restoration is complicated in cases where unique, important, or significant amounts of equipment are damaged. To reduce that impact, the industry has placed considerable focus ensuring adequate spares and alternate approaches—such as pooled resources and sharing—for significant, long-lead-time equipment such as large power transformers.

Specific causes) impact restoration

In addition to those involving significant equipment damage, outages from malicious acts, such as a coordinated cyber-attack, could additionally impact restoration priorities and performance. In such cases, tools that operators use to monitor the system could also be impacted, limiting situational awareness and impeding decision-making. Further, outages involving a physical attack on electric system assets could impede restoration activities given the needed steps to ensure safety of restoration personnel.

IV. Point 2: Natural events caused the majority of recent significant outages

The top-ranked outage listed in NERC's "2017 State of Reliability Report," based on severity risk index, was the September 2011 "Southwest Blackout." This event was caused by weaknesses in two broad areas—operations planning and real-time situational awareness. However, weather influenced 9 of 10 of the most severe outages from 2008-2016. And that pattern has continued with hurricanes Harvey, Irma, Maria, and (most recently) Florence. While those impacts have at times been profound, lessons learned have been applied and, over time, restoration performance has improved comparatively in many instances.

For example, following hurricanes in 2004 and 2005, Florida Power & Light (FPL) implemented significant system upgrades, including strengthening over 800 lines that supply critical infrastructure, moving underground or otherwise hardening about half of its main power lines, upgrading over 200 substations in flood-prone areas with specific mitigations, installing over 80,000 intelligent devices (automatic feeders, etc.), implementing mobile command centers, and increasing drone use for damage assessment. As a result of these improvements, FPL performance during 2017's Hurricane Irma (a much more severe storm than those seen in 2004–2005) was demonstrably better, with average customer outage times essentially cut in half (2.3 days versus 5.4 days). What is particularly significant is that while these system upgrades improved performance for the targeted hazard (hurricanes), they were in many cases "no regrets" actions that also likely provided collateral resiliency benefits across a number of other credible hazards.

Similarly, Consolidated Edison implemented a number of lessons learned from benchmarking Hurricane Katrina in New Orleans and as a direct result of Hurricane Sandy. These include a defense-in-depth strategy

for important substations, including the use of more-conservative flood design bases, more moats, higher walls, dewatering capability, improved remote-station monitoring feeds aggregated to centralized locations, and added protection for specialized or high-importance equipment.

Hurricane Harvey, which impacted the Houston area was more a "water event" than a "wind event." This necessitated restoration and recovery techniques never used before in the that area. One key finding from these events was the importance of deploying drones as an effective way to identify field conditions and required restoration activities.

V. Point 3: Bulk power system changes underway increase complexity

The scope and pace of electric industry change is unprecedented, new dynamics in generation fuel mix, technology, regulation, economics, and public-policy priorities. These changes provide various benefits but, in some cases, increase the complexity of both operating the bulk power system and restoring from outages.

Generation fuel mix

Solar, wind, and natural gas generation are increasing while nuclear power and coal generation are decreasing. These changes are the result of factors including economics and public-policy priorities. From an electrical grid operation perspective, the changes introduce several new variables. For example, net loss of large base-load generation that employs a large rotating mass reduces system inertia; therefore, electrical frequency can change more rapidly during a transient and thus be more difficult to control. Solar power and wind are also "intermittent" generation resources, which creates challenges maintaining system balance and ensuring adequate reserves. Further, increased solar use has resulted in a corresponding increase in inverters. Several system events have resulted from inverter operating characteristics that were not fully understood.

From a system-restoration perspective, including during the use of black-start, reduced diversity in generation fuel source adds uncertainty. For instance, to the extent that natural gas generation dominates as the fuel source, the grid is potentially more susceptible to outages caused by interruption of that nearly "just-in-time" fuel supply. Grid operators are now performing exhaustive analyses to better understand electrical system sensitivity to the changing fuel mix along with appropriate compensatory actions.

New technology

Extensive use of new technology is revolutionizing how the grid operates. To name but a few, these include utility scale photo-voltaic (solar) generation resources, increased use of large-scale battery storage, prevalence of digital protection system devices (in favor of electro-mechanical relays), micro-grids, use of unmanned aerial systems (drones) for damage assessment, addition of smart meters for automatically reporting of power outages to control centers, and more-sophisticated grid modeling and situational awareness tools. These technology advances are allowing the grid to become even more tightly interconnected and offer a broad range of reliability, resiliency, and economic benefits.

However, the extensive use of advanced technology introduces challenges, including new requisite personnel skills (e.g., relay technicians need to be proficient in setting digital equipment and legacy electro-

mechanical equipment), potentially unrecognized operating characteristics or failure modes, and possible susceptibility to cyber-attack via supply chain and other vectors.

Regulatory changes/jurisdiction

The North American Electric Reliability Corporation (NERC) was certified by FERC as the Electric Reliability Organization (ERO). As the ERO, NERC is charged with enforcement of mandatory reliability standards for the bulk electric system. These standards became mandatory and enforceable on June 18, 2007. NERC is also responsible for conducting various assessments related to the bulk power system. Since certification as the ERO, NERC has matured significantly, with increasing focus on proactive risk identification.

While NERC, under oversight by FERC, is responsible for bulk electric system regulation, individual states have jurisdiction over the lower-voltage electrical distribution within their respective geographic areas. Additionally, under the FAST Act, the DOE was granted authority to issue orders to grid operators upon a presidential declaration of a Grid Security Emergency (GSE). GSEs are characterized as occurrence or imminent danger of one or more of four specific types: geomagnetic disturbance (GMD), electro-magnetic pulse (EMP), physical attack, or cyber-attack. Varying jurisdictions and authorities introduce increased complexity regarding alignment of priorities. And compliance obligations, without commensurate economic incentive, is a possible contributor to reduction in dedicated black-start resources.

Security (Physical and Cyber)

Physical Security

In April 2013, gunmen, using rifles, conducted a sophisticated attack on an important transmission substation. During this attack, 17 electrical transformers were severely damaged at a cost to repair of several million dollars. Prior to the attack, a series of fiber-optic telecommunications cables were cut in an apparent attempt to delay detection of, and response to, the attack. There were no injuries and the event had little direct impact on reliability of the electrical system. However, the electrical industry responded to this attack as a hallmark event, and accelerated efforts underway to bolster resiliency and security. These included fast-track development of a new NERC reliability standard (CIP-014) regarding determination and assessment of critical substations.

Cyber Security

Protecting the electrical grid from a variety of cyber threats is a top industry priority. Cyber security threats, as evidenced by the 2015 attack on the Ukrainian electrical grid, can be impactful. And the threats are becoming increasingly sophisticated. In an attempt to keep pace, NERC leadership has placed cyber security as a top priority and is currently on version 5 or greater for the associated Critical Infrastructure Protection (CIP) standards. In addition to evolving security threats, such as vendor supply chain vulnerabilities and increased use of cloud-based storage, other challenges include industry burden complying with changing mandatory standards, limited access to real-time threat information, and finite (and mobile) workforce cyber security skills. In my opinion, one of the most pressing concerns involves the nexus between increased connectivity of grid digital assets coincident with increasing cyber threats.

VI. Point 4: Beneficial (no-regrets) actions are being taken

Significant industry efforts have been taken and are underway to preserve high levels of grid reliability and resiliency and improve restoration from broad-scope outages. These actions include educating the industry and regulators on resiliency threats, hardening the bulk power system, ensuring adequacy of key spares, augmenting mutual aid, enhancing restoration planning, conducting comprehensive drills and exercises, and increasing coordination—both cross-sector (e.g. gas, water) and with governmental partners (FERC, the DOE, etc.).

Education

Following the April 2013 substation attack, the NATF and the Electric Power Research Institute (EPRI) began jointly conducting resiliency summits to help align industry efforts and advance performance. The NATF and EPRI are focused on an "all hazards" approach with an emphasis on implementation of "no regrets" actions. To date, over 10 summits have been completed with attendance typically consisting of greater than 100 industry experts, regulators, and representatives from government. The initial set of summits focused on highlighting the importance of resiliency, clarifying similarities and differences between reliability and resiliency, and identifying various threats. More recent summits have focused heavily on restoration and cross-sector coordination.

System Hardening

The industry has placed extensive effort on hardening transmission systems from known, relevant hazards such as hurricanes and floods. As awareness of and sensitivity to non-traditional resiliency threats has grown, the industry has moved forward with associated hardening on several fronts. These actions include amplifying guidance on how to determine "critical substations," workshops and best-practice documents specific to main control center and substation design and construction from a physical security perspective, EPRI analyses of the consequences of an EMP-event to the electric grid, and implementation by some companies of shielding protection of various key assets from the effects of an EMP. In addition to hardening assets, like main control centers and key substations, the industry has begun improving system models to identify and, where possible, reduce the risk of key assets by ensuring added redundancy and dispersing key functions. Hardening of electric grid systems and components in these ways does not preclude a resiliency impact but helps limit the scope and severity of the casualty, thereby allowing for more timely restoration.

Adequacy of key spare parts and innovative alternatives

The industry's Spare Transformer Equipment Program (STEP) program strengthens the ability to restore the transmission system more quickly in the event of a terrorist attack. STEP is a coordinated approach to increase the spare transformer inventory and streamline transferring those transformers to affected companies in the event of a transmission outage caused by a terrorist attack. Under STEP, each participating company is required to maintain and, if necessary, acquire a specific number of transformers. STEP requires each participating company to sell its spare transformers to any other participating company that suffers a "triggering event," defined as an act of terrorism that destroys or disables one or more substations and results in the declared state of emergency. Any investor-owned, government-owned, or rural electric cooperative electric company in the United States or Canada may participate.

In addition to STEP, the SpareConnect program provides an additional mechanism for bulk power system asset owners and operators to network with others concerning the possible sharing of other selected key equipment. SpareConnect establishes a confidential, unified platform for the entire electric industry to communicate equipment needs in the event of an emergency or other non-routine failure.

Large power transformers are expensive, take a long time to build, and are very difficult to transport. To augment STEP, SpareConnect, and other spare parts approaches, Con Edison and others have developed and deployed "recovery" or "resiliency" transformers. These smaller, modular, and lighter devices are relatively easy to transport and can be quickly placed in service at a variety of key system locations. In January 2017, Con Edison demonstrated a successful installation in less than three days in response to a mock incident. While they do not have the same design lifetime as standard transformers, these recovery transformers could serve as a critical bridge to restore the system while fully pedigreed devices are being obtained. Similar innovative approaches have been developed for other key equipment such as control houses.

Augmented mutual aid

Mutual aid is key to successful restoration from a broad system outage. The electric industry uses this approach extensively to surge added resources (lineman, equipment) into an affected area to help in outage restoration. Collaboration and reciprocity under these mutual aid approaches have been highly successful and have continue to evolve. In addition to lineman resources, the mutual aid now sometimes consists of associated management teams from the supplying company to help manage restoration in pre-determined areas under the general oversight of the host company. Based on lessons learned from Hurricane Sandy, the industry developed a new governance structure termed a "National Response Event" to help prioritize and assign larger sets of mutual aid resources from even-more-distant locations. A recent area of focus involves developing an equivalent mutual aid capability for specialized skill sets, such as cyber security personnel or protection system technicians that could prospectively be shared in the wake of a relevant event.

Enhanced restoration plans

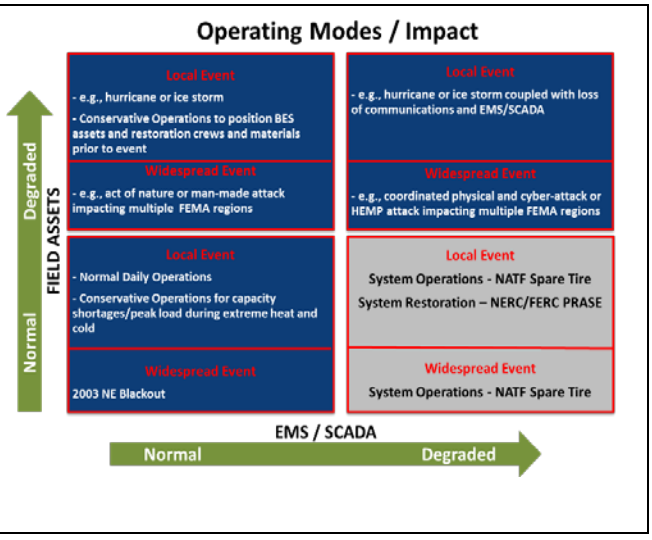
One specific area of "no regrets" action involves enhancements to restoration plans. Several NATF-EPRI resiliency summits have featured presentations and stressed emulation of National Incident Management System (NIMS) / Incident Command Structure (ICS), which encourages a whole community perspective to restoration and a common command and control hierarchy, respectively. Other summits have featured presenters from other industry sectors (water, gas, communications, etc.) to help clarify interdependencies that need to be factored into restoration priorities. Further, FERC and NERC have together conducted two different sets of inquiries to understand industry readiness to restore from system events as required by certain mandatory standards. Lastly, the NATF has commenced two separate restoration related projects—Supplemental Operating Strategies (SOS) and a report to the DOE on GSEs.

NATF Supplemental Operating Strategies

The Supplemental Operating Strategies (SOS) effort presumes a broad loss of some key operator tools (EMS/SCADA) used to monitor and control the electrical system due to cyber-attack or other impact. The SOS project identified a rank-order set (shown below) of key capabilities operators would need in order to manually operate or restore the system given an EMS/SCADA loss (shown below) with some proposed

compensatory actions. Future SOS project phases will consider coincident degradation of field assets, such as key substations.

Key Capabilities / *Priority Rank Order*
1. External Voice Communications
2. Internal Voice Communications
3. Area Control Error Calculation
4. Frequency Telemetry
5. Transmission System Monitoring and Control
6. Generation Dispatch and Automatic Generation Control
7. Personnel Deployment (Human Remote Terminal Unit)
8. State Estimation / Real-Time Contingency Analysis
9. Interchange Scheduling
10. Off-line Power Flow Analysis
11. Load and Wind Forecasting



NATF report to the DOE on GSEs

Section 215A of the Federal Power Act, added via amendment by section 61003 of Public Law 114-94 (the Fixing America's Surface Transportation Act or "FAST Act"), gives the Secretary of Energy certain authorities to issue an emergency order following the president's written declaration of a "grid security emergency" (GSE) as defined in the statute:

The term 'grid security emergency' means the occurrence or imminent danger of—(A). . . a malicious act using electronic communication or an electromagnetic pulse, or a geomagnetic storm event . . . and . . . disruption of the operation of such devices or networks, with significant adverse effects on the reliability of critical electric infrastructure or of defense critical electric infrastructure, as a result of such act or event; or (B) . . . a direct physical attack on critical electric infrastructure or on defense critical electric infrastructure; and . . . significant adverse effects on the reliability of critical electric infrastructure or of defense critical electric infrastructure as a result of such physical attack.

Because of the specialized knowledge and the wide range of designs and practices inherent in the companies that own and operate the bulk power system, the NATF has convened a GSE Team to offer recommendations on the following:

I. Communication between the U.S. Department of Energy (DOE) and the electricity subsector after the declaration of a GSE

II. Suggested criteria for declaring a GSE

III. Emergency operations and waivers associated with issuance of a GSE order

The current NATF document addresses prospective communication and waivers for all four types of threats associated with a GSE order—geomagnetic disturbance (GMD), electromagnetic pulse (EMP), cyber security,

and physical security. It also provides suggested criteria for declaring a GMD GSE. Suggested criteria for the other three emergencies (physical, cyber, and EMP) will be addressed in subsequent updates to this document.

Increasingly comprehensive drills and exercises

Electric companies routinely drill on and refine their restoration plans. Several NATF members have greatly increased the scope and complexity of these drills, including enhancements such as cross-sector coordination and assuming a loss of EMS/SCADA to test readiness for that situation.

SCE Resilient Grid V

One recent positive example is Southern California Edison's "Resilient Grid" exercise conducted on October 4, 2018. This was the fifth such exercise and considered a simulated combined cyber and physical attack that affected multiple assets within SCE and several other neighboring systems resulting in extensive residential customer outages and disabling of two major seaports, with the attendant economic impact. The drill emphasized needed cross-sector coordination as well as timely/measured updates to the public. To further complicate the drill and test restoration capabilities, SCE presumed a loss of EMS/SCADA (as presumed in NATF SOS documents) and interruptions in normal communications. The after-action roundtable discussed matters of critical interdependencies, cyber-attack liabilities, and the benefits and complexities of declaring such a situation—were it real—as a GSE.

Con Edison work with DARPA / RADICS

Con Edison is working with the Defense Advanced Research Projects Agency (DARPA) on testing of its Rapid Attack, Detection, Isolation, and Characterization Systems (RADICS) program. The objective of this program is to create a testbed and associated exercises to test feasibility of a black-start recovery in the midst of an ongoing cyber-attack. It involves coordination between operational and cyber experts and reviews how tools and technologies perform with limited power and ancillary services.

Another NATF member recently conducted a three-day long exercise that combined a cyber-attack with a natural disaster impacting a major city's critical infrastructure. Ninety exercise players participated overall, including major infrastructure owners from various sectors and local, state, and federal agencies. Exercise objectives were to build capabilities and coordination for enhanced incident response and recovery, and strengthen collaboration across sectors, jurisdictions, and disciplines.

VII. Point 5: Going-forward emphasis

Considering the industry changes and current work underway regarding resiliency, we believe the following would be beneficial:

- FERC, NERC, and the Regions should continue and increase work with regulated entities and state regulators to align on priorities for system hardening and to promote recovery for prudent investments.
- Rather than create new or revised reliability (or resiliency) standards that focus on individual hazards or threats, conduct a comprehensive review of existing relevant standards (such as TPL-001) to determine baseline performance that would improve resiliency regardless of the hazard.
- The current grid command and control hierarchy (Reliability Coordinators, Balancing Authorities, etc.) is very effective and will be so in black sky events if communication capabilities are sufficient. Much of NATF resiliency work has underscored the importance of reliability communications as a key tool to prepare for, operate through, and restore from severe events. Added focus on strengthening communications—technology, redundancy, diversity, protocols—is essential.
- Lastly, resiliency performance improvements can be measured after implementation through traditional metrics (such as FPL's reduction in average customer outage times); however, added measures are likely needed to proactively understand system resiliency and any important gaps. These measures could take the form of a maturity model.

Attachments

Documents related to NATF Supplemental Operating Strategies (SOS)

Bulk Electric System Monitoring and Control - An Overview of Backup Capabilities

Disclaimer

This document was created by the North American Transmission Forum (NATF) to facilitate understanding of Bulk Electric System Monitoring and Control Backup Capabilities. NATF reserves the right to make changes to the information contained herein without notice. No liability is assumed for any damages arising directly or indirectly by their use or application. The information provided in this document is provided on an "as is" basis. "North American Transmission Forum" and its associated logo are trademarks of NATF. Other product and brand names may be trademarks of their respective owners.

Open Distribution

Contents

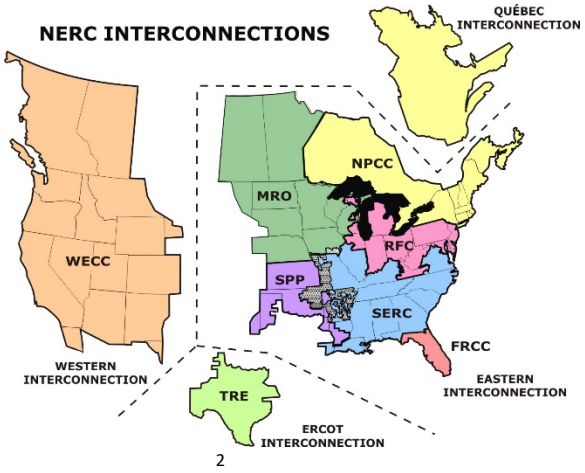
Introduction and Purpose

The Bulk Electric System (BES) is a complex network of electrical generation resources and transmission lines designed and operated to provide continuous and reliable electrical service. A key element in the reliable operation of the BES is the control centers that continuously monitor and control the generation and transmission power flows on the BES. Given the importance of these control centers, their infrastructures, and the tools utilized therein, there are a variety of methods employed to ensure these critical capabilities remain available and operational during both normal and emergency situations.

This document is intended to provide an overview of the key capabilities for the reliable operation of the BES, along with a description of the various approaches used within the industry to ensure redundancy for critical capabilities so that System Operators are able to continuously monitor and control the BES in the event of the loss of the primary control center capabilities.

Background of the Bulk Electric System (BES)

In North America, there are four Interconnections that operate independently of one another in order to provide economic and reliability benefits to all the interconnected entities.



2

- Eastern Interconnection
- Western Interconnection
- Texas Interconnection
- Quebec Interconnection

The nature of the AC interconnected system is such that continuous, diligent coordination within an Interconnect is essential to maintaining reliability. The BES is organized hierarchically, and within the Interconnections, there are one or more Reliability Coordinators (RCs) with authority to preserve reliability within their specific territories. Each RC has one or more Balancing Authorities (BAs), charged with maintaining proper load and generation balance (resulting in preserving system frequency within appropriate bounds), and one or more Transmission Operators (TOPs), charged with maintaining acceptable voltage and line flows. All of these entities work together both in real-time and for future time frames to ensure reliable operation of the BES.

[2] http://www.nerc.com/AboutNERC/keyplayers/Documents/NERC_Interconnections_Color_072512.jpg

Overview of Key Control System Functions

The reliable operation of the BES requires a high degree of coordination between multiple operating entities (RCs, TOPS, BAs, Generator Operators (GOPs), field personnel, etc.) and the assimilation of vast amounts of data. This provides System Operators with the information necessary to maintain situational awareness and to ensure the system remains in a reliable state as loads, transmission configuration, and generation output continuously change. The primary tool used by System Operators is the Energy Management System (EMS). The EMS provides the capability to assimilate and monitor system parameters in real-time, predict their future state and control equipment status and output to ensure system reliability. The EMS also implements Supervisory Control and Data Acquisition (SCADA) for the transmission system, which enables both monitoring and control of the grid.

Key Functions of an EMS/SCADA system can be characterized in five high level categories:

- Status and Control of the Transmission System
- Contingency Analysis of the Transmission System
- Status and Control of Generators
- Management of Generation Reserves
- Energy Accounting

Resiliency of Key Operating Infrastructure

Operations Control Centers

Control centers provide System Operators with the capability to reliably operate the electric grid while also ensuring continued operations should an event render a control center inoperable. In order to ensure functional obligations are maintained during adverse conditions impacting a primary control center, backup control center facilities are in place, with the same functional capabilities of the primary facility, allowing continued operation of the BES. NERC standard EOP-008-1 requires backup control center capabilities for the RC, TOP, and BA functions.

The primary/backup control center configuration design and System Operator functions within a control center vary based on the organization's functional responsibility, the structure of the organization, and the size or configuration of the service area. Similar to the variations of a control center's internal configuration, the procedures for operating a primary and backup control center also varies across the industry. The three typical configurations employed are often referred to as having a "hot/cold", "hot/warm", or "hot/hot" design.

Primary control centers are considered the "hot" facility while the backup control center is generally a "cold" standby facility that can be fully staffed and activated within two hours (per NERC standard EOP-008-1). Typically, the average time from primary to backup facilities is less than one hour away. The operation and maintenance of a tertiary operating facility is not typical within the industry. However, there are some examples of configurations that allow transfer of full or limited capabilities to an alternative facility.

Control Center Infrastructure

In addition to maintaining control center redundancy, many layers of protection for critical control center infrastructure are also employed. These include the following:

1. **Computing Capability and configuration:** Control Center tools are commonly provided via high-availability computing architectures. Energy Management Systems (EMS) and other control center systems are typically configured to provide a redundant pair for each system component for the primary control center plus an additional redundant pair for the Backup control center.
2. **Cyber Protection:** The computing systems for control systems are commonly embedded and logically separated within the larger corporate data networks. This separation enables these networks to benefit from the cyber protections deployed to protect the larger corporate networks, along with the ability to deploy more specific protection for the control network environments. Entities also employ physical security plans and measures to control access to Critical Cyber Assets as defined by the NERC CIP Standards.
3. **Power Supply, HVAC and other facility support infrastructure:** Control centers are designed for continued operation when off-site power from the local utility is unavailable. In many cases there are redundant off-site sources from the local utility along with redundant on-site generation capability. The typical configuration may also include an Uninterruptible Power Supply (UPS) with batteries to provide power to the control center during the transition from the local utility to the on-site generation. Many control centers utilize dedicated and redundant chillers, air handlers, and Computer Room Air Conditioning (CRAC) systems to ensure continued operations during equipment failure or maintenance.
4. **Data Communications:** There are a variety of data sources utilized by EMS and other System Operator tools. Data communication paths for applications are typically composed of a combination of commercial vendor data networks and proprietary private networks to create acceptably redundant communications networks. The private networks may consist of fiber, microwave, or other wireless technology.
5. **Voice Communications:** Voice communications between field personnel, TOPs, BAs, GOPs, and RCs are critical in managing BES reliability. Control centers employ layers of redundancy to minimize the probability of loss of voice communications systems. These various forms of communications include: corporate networks, direct commercial landline service, commercial cellular, and satellite phones. In some cases, entities also have access to proprietary radio, cellular, instant messaging or video link communication tools. All RCs and many TOP/TOs also have access to a NERC-managed messaging system (RCIS) for communication with neighboring control centers. In addition, all RCs have access to a NERC-managed dedicated phone line (NERC Hotline) for communication between RCs.
6. **Physical Security:** In addition to the Cyber Asset physical security measures mentioned above, the most critical control centers, as defined by NERC standard CIP-014-2 requirements, have undergone stringent threat and vulnerability assessments along with a review of their respective physical security plans. These plans are also required to be reviewed and endorsed by independent third parties. Control centers, at a minimum, generally employ on-site security and multiple check points with controlled access to control rooms and data rooms.

Defense in Depth for System Operations

As noted, significant effort is made to protect essential infrastructure and capabilities for the reliable operation of the BES. Regardless, there will ultimately be times for which extreme events may introduce brief moments of degraded operating capability for a particular set of tools or location. Fortunately, in addition to an entity's primary and backup systems, System Operators have coordination plans and

capabilities in place that allow them to coordinate operations within and across organizational boundaries. This "defense in depth" principle helps to maintain sufficient operating capability to ensure a reliable BES during even the most severe of operating conditions.

For instance, RC system capabilities will cover the entire host RC region along with modeling some (or all) of their neighboring RC systems (which may include portions of multiple TOP systems). This overlap of RC system visibility (host RC, host TOP, and neighboring RC and TOP areas) provides System Operators with multiple layers of redundancy necessary to maintain situational awareness and for coordinated system operations. Likewise, protocols for communication are included in critical operating procedures for both normal and abnormal system operations. Effective coordinated system operations requires robust and redundant internal and external communication capabilities, which are generally designed to include direct phone calls, blast (i.e., conference) calls, the NERC RCIS system, NERC Hot-Line, satellite phones, and other forms of telecommunication capabilities.

Business Continuity

In order to ensure business continuity for all potential system conditions, control center operators have an Operating Plan ("Plan") in place to address the loss of control center capability. This Plan will include requirements for items such as annual testing (in accordance with NERC standard EOP-008-1), periodic testing of infrastructure failover schemes (as needed), and applicable training. In addition, model changes, maintenance activities, and troubleshooting activities provide informal testing of failover schemes that will be used during control center evacuations. Many existing processes and procedures call for the failover of infrastructure to backup sites in order to alleviate issues on the primary system, providing opportunities for the testing of control center evacuation and transition of key infrastructure and operating capabilities. Many different subsets of evacuation processes can also be tested and validated during abnormal operating conditions.

Conclusion

The continued availability of control center infrastructure and operating capabilities is the primary element in maintaining reliable operation of the BES. Although a variety of methods exists across the industry, control centers and key infrastructure capabilities are commonly designed and implemented to provide multiple layers of defense. This includes primary systems, backup capabilities, and operating plans that facilitate coordinated interconnected operations. Due to the significance and complexity of these systems and their configurations, operating entities have documented plans to address loss of critical capabilities and to facilitate coordinated operations, even during extreme conditions. These plans are developed in accordance to NERC standards, often exceed minimum requirements, and are incorporated into System Operator training plans to promote the reliable operation of the BES.

It is imperative that these operating capabilities remain available under all operating scenarios. It is impossible to suggest all potential scenarios have been addressed with the variety of system designs and operating plans in place. However, the primary and backup capabilities in place today across the industry have integrated multiple layers of defense to help promote the continued reliable operation of the BES during most expected operating scenarios for an entity. This is coupled with the defense in depth that RCs provide by monitoring the same areas as TOPs and BAs to provide a high degree of resiliency to grid reliability.

Bulk Electric Systems Operations absent Energy Management System and Supervisory Control and Data Acquisition Capabilities—a Spare Tire Approach

Disclaimer

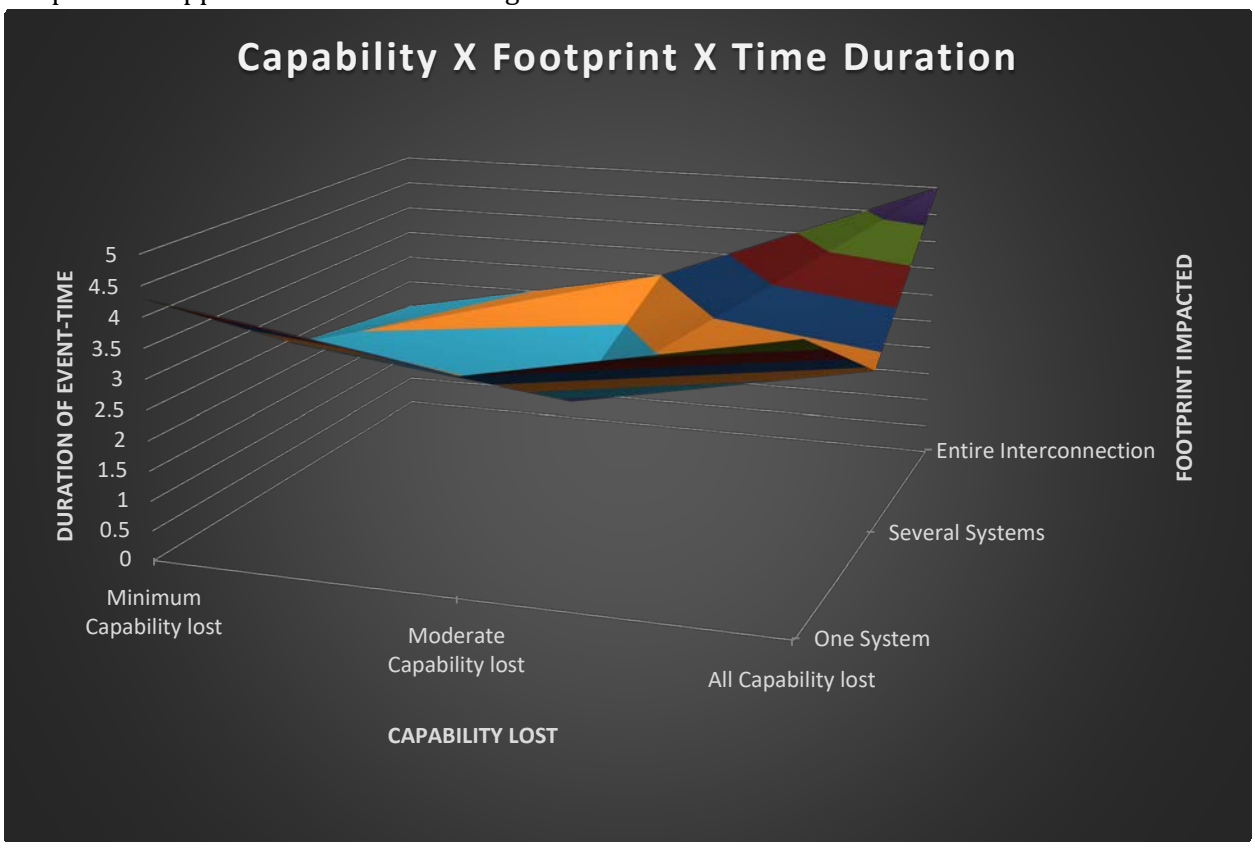
This document was created by the North American Transmission Forum (NATF) to facilitate understanding of bulk electric system monitoring and control backup capabilities. The NATF reserves the right to make changes to the information contained herein without notice. No liability is assumed for any damages arising directly or indirectly by their use or application. The information provided in this document is provided on an "as is" basis. "North American Transmission Forum" and its associated logo are trademarks of the NATF. Other product and brand names may be trademarks of their respective owners. This legend should not be removed from the document.

Open Distribution

This NATF Reference document, representing research performed by industry personnel who have in excess of 200 years of cumulative experience, is in response to a question originally raised by the Electric Subsector Coordinating Council (ESCC) regarding how electric utilities would continue to operate during an event causing loss of both primary and backup control systems (i.e., total loss of the Energy Management System (EMS)/Supervisory Control and Data Acquisition (SCADA)). This concept was subsequently characterized as a "Spare Tire" approach to ensure continued system operations following the loss of critical applications. As such, this document[3]:

- Captures the results of an assessment of what operating strategies and reliability tools are present today for Bulk Electric System (BES) operations during times when traditional tools for situational awareness, system control, balancing and communications are unavailable, both internally and coupled with external loss of capabilities
- Identifies future areas of industry work and research to better enable operations during scenarios where there is a total loss of all EMS/SCADA capability

The scope of the event assessed was a complete loss of EMS/SCADA where the extent of condition expanded across multiple regions for multiple days. This approach (Capability x Footprint x Timeframe) was necessary to evaluate the impacts on operations and industry readiness. The concept of this approach is shown in the figure below.



[3] A companion NATF Reference Document- *Bulk Electric System Monitoring and Control - An Overview of Backup Capabilities*, provides an overview of the key capabilities for the reliable operation of the BES, along with a description of the various approaches used within the industry to ensure redundancy for critical capabilities so that System Operators are able to continuously monitor and control the BES in the event of the loss of the primary control center capabilities.

In performing the assessment, the team identified 11 key capabilities needed for system operations in the event of loss of EMS/SCADA. These capabilities were included in a limited industry survey in order to (1) determine their rank in priority for "Spare Tire" operations and (2) understand the levels of redundancy generally associated with each. The results indicated the following:

Priority Rank Order
1. External Voice Communications
2. Internal Voice Communications
3. Area Control Error Calculation
4. Frequency Telemetry
5. Transmission System Monitoring and Control
6. Generation Dispatch and Automatic Generation Control
7. Personnel Deployment (Human Remote Terminal Unit)
8. State Estimation / Real-Time Contingency Analysis
9. Interchange Scheduling
10. Off-line Power Flow Analysis
11. Load and Wind Forecasting

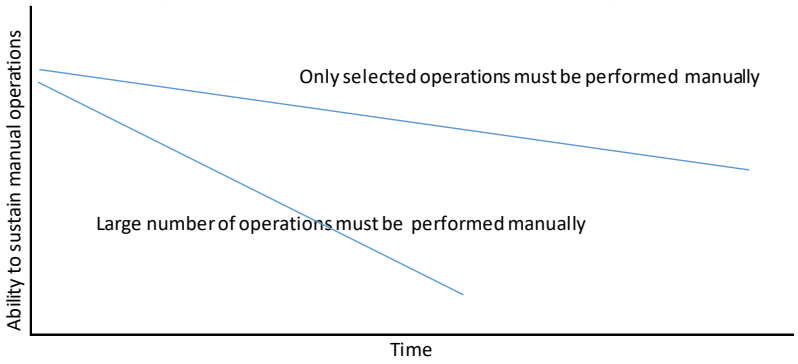
The ability to communicate was the highest ranked capability from the survey. This suggests the importance of having a robust communication network along with sufficient operating protocols available to enable effective communication with internal personnel, neighboring utilities, emergency responders, and other impacted stakeholders. The NATF survey also indicated that at least half of the respondents have implemented redundant capabilities beyond primary and secondary redundancy for the four highest ranked capabilities. At the same time, the results highlight other primary capabilities that remain critical for "Spare Tire" operations that may not generally employ redundancy beyond secondary levels.

Another key observation of the team is that any replacement of EMS/SCADA systems with alternate methods, such as involving humans, trucks, telephones, etc. would be:

- Limited in capability – the system will not function with comparable levels of efficiency and reliability
- Limited in time frame – given the personnel constraints and comparative inefficiency of this form of operation, it cannot be maintained indefinitely
- Resource-consuming – the same personnel who would be working to restore the system (along with ongoing forced outages) will be called upon for this type of operating environment
- Procedurally limited – it is possible that response and recovery procedures generally do not thoroughly define detailed responses to long-term events as described in the document.

It is of the utmost importance that utilities consider not only the availability for resource deployment but also the plans and protocol necessary across the entire enterprise to effectively execute this capability for prolonged periods. This includes the identification of critical skills

needed to operate the grid in this manner in addition to the training requirements for any personnel needed to perform tasks consistent with manual operation. This degradation of the ability to sustain manual operations is shown in the figure below.



Due to the various event scenarios possible, it was concluded that a single recovery method is not appropriate to address all events rendering an EMS/SCADA unavailable. However, as part of the review process for considering a "Spare Tire" strategy, consideration was given to principles that help prepare for and respond to multiple types of high-impact, low-frequency events. The following operating principles were found to be common across multiple entities based on shared experiences, similarities between procedures, and ranked responses for key capabilities.

- Understand impact and plan for personnel safety, training, and coordination
- Ensure availability of alternative communication capabilities
- Consider greater levels of redundancy for primary operating capabilities
- Ability to notify stakeholders and request (or lend) assistance
- Comprehensive and clear logistical plans for personnel and data distribution
- Understand and plan for resource implications (field, engineering, operations, etc.)
- Codify and practice concepts for "Spare Tire" operations
- Consider strategies that mitigate multiple high-impact, low-frequency threats

As for next steps to even better position the industry to address a "Spare Tire" scenario, the team identified the following areas for future work:

- Continue to address voice and data communications- Lead: DOE/National Labs/EPRI
- Develop additional Reliability Tools/Data Availability to aid situational awareness during a "Spare Tire" event- Lead: DOE/National Labs/EPRI
- Formalize strategies and plans for "Spare Tire" operations scenarios- Lead: Individual utility companies
- Formalize data sharing on "Spare Tire" operations strategies- Lead: NATF
- Harden EMS hardware components and develop streamlined EMS recovery process and capabilities- Lead: EMS vendors

It should be noted that individual company practices may vary from descriptions provided in this document. Also, this document does not create binding norms, establish mandatory reliability standards, or create parameters by which compliance with NERC Reliability Standards is monitored or enforced.

Bulk Electric Systems Operations absent Energy Management System and Supervisory Control and Data Acquisition Capabilities—a Spare Tire Approach (2017)