North American Transmission FORUM

Community Confidentiality Candor Commitment

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

Version 2023-1
Document ID: 1064
Approval Date: 11/3/2023

Contents

Version History

Date	Version	Notes
12/2016	2016-2	
11/3/2023	2023-1	Updated to new template and updated the image for Figure 1.

Review and Update Requirements

- Review: every 5 years
- Update: as necessary

1. 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.

2. Background of the Bulk Electric System

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.

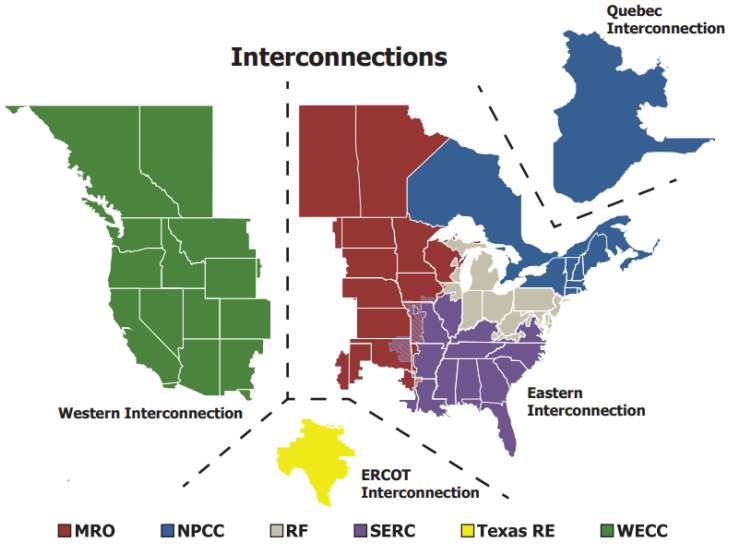

Figure 1: NERC Interconnections [1]

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 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.

[1] https://www.nerc.com/AboutNERC/keyplayers/PublishingImages/NERC%20Interconnections.pdf

3. 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

4. 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 vary 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 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. 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.

5. 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 require 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 Hotline, satellite phones, and other forms of telecommunication capabilities.

6. 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.

7. 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 with 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.