NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Lesson Learned

SCADA Failover Event

Primary Interest Groups
Transmission Operators (TOPs)
Balancing Authorities (BAs)
Reliability Coordinators (RCs)
Distribution Providers (DPs)
Generator Operators (GOPs)

Problem Statement
While initiating a failover process between the entity's primary and secondary data source, supervisory control and data acquisition (SCADA) caused the system to come up in a paused state. This paused state created a temporary loss of generating management system (GMS) functionality.

Details
The event began when the entity performed a planned failover to test configuration changes made within the GMS. After the test, the failover did not function as normal, causing the loss of visibility to GMS when GMS IT personnel attempted to fail back to the primary site. This loss of visibility included the loss of GMS alarming, the SCADA database, and all inter-control center communications protocol (ICCP) connections with six counterparties, including the TOPs and the Regional BA. The Regional BA placed the entity on state estimator values and all on-line generating stations were instructed to hold at current output.

The cause of this event was the timing of a SCADA_VALIDATE command (with reference to this specific vendor) during a failover. Initiating the failover process before the SCADA_VALIDATE was completed caused the system to come up in a paused state.

When operating from the primary site, all SCADA data is automatically updated to the secondary site every 5 minutes to keep the site data consistent. When a SCADA change is made by GMS IT staff, they run a SCADA_VALIDATE to allow SCADA to validate that the change did not interfere with SCADA functionality. Within the system, a SCADA_VALIDATE will pause SCADA so that it can validate a "snapshot" of that point in time.

During this event, GMS IT staff initiated a failover to the secondary site and verified that the failover was successful. Before failing back to the Primary Site, GMS IT ran a SCADA_VALIDATE.

The timing of the SCADA_VALIDATE and fail back process (which copies the SCADA database to the backup site) caused the SCADA database to be copied to the primary site "with the pause flag set to true." After the failover, the SCADA_VALIDATE did not complete the restart because it was initiated in the other domain. Working with the vendor, it was determined that it is appropriate to perform a SCADA_VALIDATE on the online server (in this case, secondary site) but it is recommended to wait 10 minutes to ensure SCADA has had time to pause, validate, and restart before failing over.

Once the SCADA_VALIDATE was implemented using the proper timing, GMS displays began to return to normal. Communication channels began functioning and all systems returned to normal. The Regional BA called to report seeing good ICCP values and took the entity's load and generation data off state estimator values. The entity contacted all on-line generating stations and instructed them to return to normal operations.

Corrective Actions

GMS IT personnel have identified and implemented two controls to prevent this type of event, and the vendor has added a third:

- GMS IT personnel have installed an alarm into the system that generates email alerts to all GMS IT personnel when a SCADA_VALIDATE has been initiated. This will alert GMS IT personnel to delay performing a failover process until the SCADA_VALIDATE process is complete.
- A new procedure will require that, prior to initiating a failover between sites, the system must run in a stable condition for 20 minutes after initiating a SCADA_VALIDATE.
- Based on information shared with the vendor by the entity, the vendor is modifying training related to failovers to include the above information.

Lesson Learned

An understanding of the SCADA_VALIDATE function by all users can significantly improve an entity's response to unexpected events.

When performing a failover between primary and alternate sites, it is recommended to wait 10 minutes after performing a SCADA_VALIDATE to ensure SCADA has had time to pause, validate, and restart prior to the failover.

NERC's goal with publishing lessons learned is to provide industry with technical and understandable information that assists them with maintaining the reliability of the bulk power system. NERC requests that you provide input on this lesson learned by taking the short survey provided in the link below.

Click here for: Lesson Learned Comment Form

For more Information please contact:

NERC – Lessons Learned (via email)	Bill Kunkel (via email) or (651) 855-1717
Source of Lesson Learned:	Midwest Reliability Organization
Lesson Learned #:	20160602
Date Published:	June 14, 2016
Category:	Communications

This document is designed to convey lessons learned from NERC's various activities. It is not intended to establish new requirements under NERC's Reliability Standards or to modify the requirements in any existing Reliability Standards. Compliance will continue to be determined based on language in the NERC Reliability Standards as they may be amended from time to time. Implementation of this lesson learned is not a substitute for compliance with requirements in NERC's Reliability Standards.