NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Lesson Learned

Failure of Energy Management System While Performing Database Update

Primary Interest Groups
Reliability Coordinators (RC)
Transmission Operators (TOP)
Transmission Owners (TO)

Problem Statement
There was a failure of Energy Management System (EMS) while performing a database update.

Details
While performing edits to the EMS database, the entity received alarms that indicated errors for the communications servers. A decision was made to restore the database to its original state. While performing the restore procedure, the standby communications server in the Primary Control Center (PCC) was manually restarted. This caused the reversal of the database edits to fail and create faulty data files that synchronized across the integrated system servers. Although alarms were received for all communication servers, only the standby communications server in the PCC failed; the EMS remained fully operational.

The faulty data files were manually removed from all servers, and a SCADA server failover was completed. An attempt to enable the standby communications server at the PCC failed. The EMS group executed a system warm restart, but since the EMS is an integrated system, the system warm restart resulted in the faulty data in the database being loaded into the remaining two communications servers, whereby all three communications servers failed. At this point, the EMS lost functionality and was operational on a sporadic basis. At no point was the EMS off-line for a period exceeding 30 minutes. With the failure of the three communications servers, incremental system scans were performed.

Subsequently, the substantive issues with the EMS were resolved and the EMS was restored with a minimum server requirement configuration with full functionality. Once the limited server system was verified as stable, all remaining servers were successfully brought back manually into synchronization with the EMS.

Corrective Actions

- Training documents will be developed to document revised steps for database updates and communication server restarts to eliminate the failure mode experienced during this incident as a result of the integrated system.
- Database update testing procedures and documentation will be reviewed to ensure that testing requirements are clear and concise. Although the database updates were implemented first on

both the Product Development System (PDS) and the Dispatcher Training System (DTS), error logs were only partially reviewed. Therefore, the testing procedures will be updated to include step-by-step instructions to ensure that the procedures are completely carried out, thus simulating the production environment that includes separate windows used for log viewing and update time log tracing. EMS analysts will receive training on the existing and new procedures.

- The EMS vendor agreed to upgrade the EMS to a new EMS server environment in which the PCC and the Auxiliary Control Center (ACC) databases will be separate. In the new system, database updates will be required to be performed independently on the PCC and ACC to reduce the risk of any anomalies at the PCC from being propagated to the ACC. This will provide increased reliability to the EMS system.

Lesson Learned

When the EMS was purchased, the vulnerability of an integrated system architecture was unknown. To eliminate this now-exposed vulnerability, it is recommended that functional separation of the PCC from the ACC be implemented.

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 your 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)	NPCC – Event Analysis
Source of Lesson Learned:	Northeast Power Coordinating Council
Lesson Learned #:	LL20131003
Date Published:	October 29, 2013
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.