Lesson Learned

Indistinguishable Screens during a Database Update Led to Loss of SCADA Monitoring and Control

Primary Interest Groups
Balancing Authorities (BAs)
Transmission Owners (TOs)
Transmission Operators (TOPs)
Reliability Coordinators (RCs)

Problem Statement
During a planned database update and failover, an Energy Management System (EMS) operations analyst inadvertently changed an on-line SCADA server database mode from "remote" (online) to "local" (local offline copy), which caused a loss of SCADA monitoring and control of Bulk Electric System (BES) facilities.

Details
An EMS operations analyst notified an on-duty system coordinator of a desired database update and failover. After concurrence with the on-duty system coordinator and notification of affected parties, the operations analyst proceeded to set up the maintenance workstation in preparation for the failover from the on-line SCADA server to the backup SCADA server. The maintenance workstation is connected to the real-time system, but has the ability to separate its EMS functionality from the real-time databases for validating and staging database updates. The operations analyst had two remote desktop sessions open, one for on-line SCADA server and other for backup SCADA server. In addition, the analyst had a third desktop window that was integral to the maintenance workstation. The operations analyst proceeded to change the maintenance workstation's database mode from remote (online) to local (offline) to complete final database modifications before the failover. Due to the identical screens, the mode change and database modifications were inadvertently performed on the on-line SCADA server database instead of the maintenance workstation's database. As a result, the front-end processor (FEP) processes stopped polling remote terminal units (RTUs) and failover functionality was disabled. This caused a loss of SCADA monitoring and control of BES facilities for 31 minutes and 44 seconds.

Corrective Actions
Database modifications were immediately suspended until the following mitigation actions were in place:

1. Implementation of unique background identifiers to distinguish each SCADA server from the local maintenance workstation to provide heightened awareness.

2. Development and implementation of a formal procedure and checklist for SCADA database staging and implementation. This procedure and checklist should include, but not be limited to:

   a. All steps required to implement a SCADA database update on the on-line system; and

   b. Notification protocols throughout the EMS on-line SCADA maintenance activities.

Lesson Learned

The root cause of the event was that the EMS operations analyst mistakenly switched the on-line SCADA server database to local (offline) mode from remote (online) mode, which caused the FEP processes to stop and disabled the failover functionality. The initial cause of this action was that the remote desktop screens to each SCADA server, which the operations analyst set up on the maintenance workstation, were identical in appearance. This made it difficult to differentiate between screens and contributed to the analyst mistakenly selecting the inappropriate screen.

Another cause was the lack of a formal written process or checklist for implementing database changes. Without a checklist or a procedure, the operations analyst was unable to follow proper protocol and failed to verify that he was working on the appropriate device prior to initiating the database modification.

Discussion with the EMS vendor indicated that switching between the local and remote database modes was not an intended feature for the SCADA servers. The vendor did not identify any situations in which it would recommend changing the database mode on a server and indicated that a future release of EMS software would eliminate the ability to switch database modes on a server.

NERC's goal in 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)   FRCC – Lessons Learned (via email)

Source of Lesson Learned: Florida Reliability Coordinating Council

Lesson Learned #:   20130802

Date Published: August 21, 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.