NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Lesson Learned

Inappropriate System Privileges Caused Loss of SCADA Monitoring

Primary Interest Groups

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

Problem Statement

An entity experienced a loss of SCADA telemetry—specifically a loss of the channel status indicators—for 76 percent of its transmission system. This problem occurred during the implementation of a scheduled SCADA database update that caused one of the front-end processors to be in an abnormal state. An incorrect command was used to remedy the situation, which resulted in the channel status indicators being set to a failed state. The RC and neighboring entities were promptly contacted and field personnel were dispatched to staff critical substations in order to verbally transmit data and maintain operating capability, per the entity's Critical Facilities Staffing Procedure. The SCADA support team resolved the problem, and full SCADA functionality was restored 42 minutes later.

Details

An entity's SCADA support staff was deploying a change to one of the SCADA system's front-end processors. The change was required in order to remove a field device from the front-end processor's scan list. During the implementation of the change, the SCADA support staff did not use the appropriate system privileges to stop and start the front-end processors' scanning processes. This resulted in two scanning processes operating simultaneously. The command used to stop the second set of processes was not appropriate for the situation, resulting in the scanning processes assuming that the field device channels were not active, thereby disabling a portion of the SCADA system.

Analysis by the SCADA support staff and the SCADA system vendor determined that the command used to stop the errant scanning processes was not correct since the scanning processes required an immediate termination, not a controlled shutdown. The scanning processes were designed to set the channel status to a failed state for a controlled shutdown.

As detailed above, the RC and neighboring entities were promptly contacted while field personnel were dispatched to staff critical substations in order to verbally transmit data and maintain operating capability, per the entity's Critical Facilities Staffing Procedure.

Corrective Actions

The incident, including the correct steps required to implement the front-end processor change, was communicated to the SCADA support team. Training on the proper steps to use when making any change to the production SCADA system was conducted.

The entity reviewed this incident with its vendor and is putting additional preventative measures in place, including error checking to prevent a user from stopping or starting the scanning program using an incorrect command.

Lesson Learned

Entities need to ensure that they fully understand and verify with their EMS vendors, the correct procedures and commands required in all situations. Specifically, entities need to better understand the behavior of the system to various commands. This was an unanticipated event, but could have been prevented if the entity had implemented better controls.

Entities should also consider:

- Reviewing the training with respect to change management to ensure that it includes a checklist of steps required; and
- Educating SCADA support staff on global impact of commands on the entire SCADA system.

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)	Jacquie Smith (via email) or (303) 247-3067
Source of Lesson Learned:	Reliability*First* Corporation
Lesson Learned #:	20130801
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.