NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Lesson Learned

EMS Recovery Strategy

Primary Interest Groups

Reliability Coordinator (RC)
Balancing Authority (BA)
Transmission Operator (TOP)
Transmission Owner (TO)

Problem Statement

An energy management system (EMS) auto-recovery process was configured such that all nodes (e.g., servers, workstations) in the EMS were prompted to reboot for a particular system condition. This complete system restart sequence took 47 minutes to complete. Consequently, there was a complete loss of control and monitoring functionality until each critical server and workstation reported its status as normal and fully functional.

Details

The SCADA System lost all functionality due to brief loss of communication to a critical system program. This critical system program stopped sending heartbeat signal on both LAN A and LAN B for a period of 57 seconds.

The brief loss of communication to this critical system program and the subsequent re-establishment of communications to that program (stalled for 57 seconds) led to a system-wide auto-recovery process to bring every node in the EMS (e.g., servers/workstation) to a consistent state. Due to the system size, this entire auto-recovery process took 47 minutes to complete. Consequently, there was a complete loss of control and monitoring functionality until each critical server and workstation reported its status as normal and recovered to full functionality.

The root cause was determined to be a core SCADA program stalling for 57 seconds on the primary SCADA node and server due to a disk fault.

Corrective Actions

The system has been reconfigured such that if this scenario were to occur again, only the problematic server would unload and reboot.

Lesson Learned

Careful analysis of EMS system configurations that initiate a complete system restart for various failure modes should be performed during the commissioning of the EMS to identify and minimize the duration of EMS unavailability.

EMS nodes (e.g., servers, workstations) should be prioritized during an auto-recovery process such that essential nodes are up and available first to give operators the ability to monitor and control the electrical system as quickly as possible. The recovery of nonessential servers, workstations, etc. could have a significant impact on the duration of a complete system restart.

Scenarios should be evaluated that could trigger an application or system recovery due to a system condition. Procedures should be developed and periodically reviewed to ensure minimal recovery time, and to familiarize staff on recovery processes.

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)	NPCC – Event Analysis
Source of Lesson Learned:	Northeast Power Coordinating Council
Lesson Learned #:	20150604
Date Published:	June 25, 2015
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.