NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Lesson Learned

Loss of SCADA Due to Memory Resources Being Fully Utilized

Primary Interest Groups
Transmission Operator (TOP)
Transmission Owner (TO)

Problem Statement
An Entity experienced a loss of Supervisory Control and Data Acquisition (SCADA) control and monitoring due to the memory resources on the primary SCADA communications server being overwhelmed by Secure Shell (SSH) sessions generated from another SCADA host.

Details
The SCADA administrator, along with the SCADA support vendor, identified that the memory resources on the primary SCADA communications server were overwhelmed, which prevented the control and monitoring of the electric system. The post-event investigation identified that an SSH session repeatedly initiated commands. A discrepancy in the EMS host-naming convention used on a LINUX host file caused the memory resources to exceed their maximum capacity.

After the event, and while trying to duplicate the incident, the SCADA vendor discovered that some of the proprietary protocols used in the communication front-end processors did not support the Network Address Translation (NAT) used in the failover process from the primary to the backup communications front-end servers. This could have prevented the failover process that allows the backup SCADA communications server to take over upon the primary server's failure.

Corrective Actions
The following actions were taken to correct the problem:

- The SCADA servers, workstations, and other crucial host resources are now subject to being monitored and alarming upon exceeding threshold parameters.
- The host names on the host file created and maintained by the SCADA vendor have been corrected and tested.
- The SCADA configuration settings were modified so that the front-end processor at the backup control center is used in the event the primary front-end processor fails.

Lessons Learned
The SCADA host resources should include monitoring and alarming of crucial events and server resources so that users are aware of any possible problems and can then prevent incidents such as loss of SCADA system functionality.

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)	David Penney (via email) or (512) 583-4958

Source of Lesson Learned:	Texas Reliability Entity
Lesson Learned #:	20140604
Date Published:	June 19, 2014
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.