NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Lesson Learned

SCADA Failure Resulting in Reduced Monitoring Functionality

Primary Interest Groups
Reliability Coordinators (RC)
Transmission Operators (TOP)
Balancing Authority (BA)

Problem Statement
An entity's primary control center SCADA Management Platform (SMP) servers became unresponsive, which resulted in a partial loss of monitoring and control functions for more than 30 minutes. Because this loss of functionality was a result of a conflict between security software configuration changes and core operating system functions, a cybersecurity event was quickly ruled out, and no loss of load occurred during this event.

Details
The primary control center SMP servers ceased network functionality and were unresponsive to login attempts from the local console. Physical reboots of the servers were only able to resolve the problem momentarily. Recovery plans were immediately activated, and predefined decisions and procedures were followed as designed.

The entity's primary control center Energy Management Platform (EMP) servers automatically began using the available SCADA signals provided by backup control center SMP servers and multisite IP routable SCADA. Manual actions quickly restored additional SCADA functionality for critical non-IP routable circuits by moving those circuits to the backup SMP servers. Key generation facilities and substations were staffed to ensure that any needed control operations could be performed. Once the primary SMP servers were stabilized, they were used to operate only noncritical SCADA circuits until root cause was established and full remediation was completed. This was possible due to the multisite redundancy design of the overall Energy Management System, which allowed the entity's primary control center EMP servers to operate in a mixed mode, combining available SMP capabilities at both primary and backup control centers. Having this multisite redundancy meant the operators did not need to physically travel to the backup control center during this incident, and it also lowered risk during root cause analysis.

The entity discovered that the root cause stemmed from a planned change to the security policy configuration of the host-based intrusion detection (HIDS) and intrusion prevention (HIPS) software. As an unintended result, the HIDS/HIPS security software on the SMP server hosts began to block certain core operating system processes when those processes executed in a specific order that coincided with the HIDS/HIPS policy change. The block did not occur until several days after the change was implemented, when the SMP servers performed the specific functions that triggered the conflict and caused the HIDS/HIPS security software to lock down the core operating system.

Once the root cause was identified, the entity created a new HIDS/HIPS security policy configuration that allowed the HIDS/HIPS security software to handle the core operating system functions on the SMP server hosts properly. The entity then conducted the necessary testing and implementation to restore functionality to the SMP systems.

Corrective Actions

The entity engaged the HIDS/HIPS security software vendor to review and implement policy changes to better manage the balance between custom configurations and secure threat detection and protection. Processes for implementing HIDS/HIPS security policy changes while also maintaining system integrity are being reviewed for enhanced functionality and reliability. Solutions from these reviews are being implemented.

Lesson Learned

This event brought forward several positive lessons learned that minimized the extent of the outage:

- Security software configurations need careful analysis, design, testing, and implementation, as they may impact reliability in unpredictable ways.
- Registered entities should consider a "multisite hosting" configuration. This configuration provides flexibility and convenience for rapid recovery capability of EMS and SCADA functions.
- Frequent exercise of and training on recovery plans ensures that actual event responses go according to plan and promptly mitigate operational impacts.

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)	Steve Ashbaker (via email) or (801) 883-6840
Source of Lesson Learned:	Western Electricity Coordinating Council
Lesson Learned #:	20131002
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.