NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Lesson Learned

EMS System Outage and Effects on System Operations

Primary Interest Groups

Reliability Coordinator (RC)	Transmission Operators (TOP)
Transmission Owners (TO)	Balancing Authorities (BA)
Interchange Authorities (IA)	Generator Operators (GOP)

Problem Statement

An entity's Energy Management System (EMS) began to lose data necessary for visibility of portions of its transmission network causing functionality and/or solution interruptions for some of its EMS operational tools. No loss of load occurred during this event and it was quickly determined to not be a cyber security event.

Details

Upon completion of scheduled transmission switching during a fall day with mild temperatures and clear weather conditions, a large utility with BA/TOP responsibilities experienced an abnormal condition on the data networks serving the EMS. Excessive data packets being sent on the data network resulted in heavy loading. The extreme loading created a performance degradation of the data flows between the Supervisory Control Data Acquisition (SCADA) system, EMS Supervisory Control and various supporting systems. At times during the event, the degraded data flows limited the visibility of the EMS SCADA data for the TOP/BA control center, several TO control centers and the generation operations group. The event was coincident with scheduled network maintenance activities, and software changes to the data historian test servers, which are used to capture data and record it to storage. This work had been started after all morning transmission switching had been completed per existing standard infrastructure maintenance review and authorization procedures. To compound the problem, as the event unfolded over an eleven hour period, EMS personnel were not able to determine the root cause of the excessive data network traffic, could not accurately predict when the problem(s) would be solved and when data would be restored to operations.

There was no loss of situational awareness or control functions due to the entity utilizing back-up systems and extreme condition procedures. Operations used a backup AGC system, which is completely independent of its EMS AGC system, to meet its BA requirements for balancing generation and load. Real Time Contingency Analysis (RTCA) continued to be performed by updating previous state estimation-power flow cases and system planning cases with current data for load, transmission status, generation status/output, interchange, etc. The updated information was provided by field and other control center personnel still having visibility. The RTCA studies included contingencies to ensure nuclear plant operating parameters and off-site power requirements would continue to be reliably met. The real-time interchange tagging system was not affected. Key facilities and substations were continuously monitored to ensure any needed switching could be performed. Increased communications were implemented with the

generators to inform them of the situation and update them on the progress to restore the EMS. Neighboring utilities were contacted to check tie line flows and to inform them of the issue.

Because of the loss of data visibility, the RC initiated a procedure called "Conservative Operations". This procedure is initiated when there is a potential risk to the reliability of the TOP or BA in the Eastern Interconnection. These potential risks include, but are not limited to, when an operator is unsure about the outcome of a next contingency condition as a result of unstudied conditions, loss of SCADA or EMS visibility or unexplained or unknown power system conditions. One step performed during "Conservative Operations", if needed, is for all maintenance and switching activities to cease so that the RC knows the exact state of the system and which elements are in or out of service. There was also another potential action, which was not implemented, calling for all transmission lines to be put back in service. It was determined after discussions with field personnel that the procedure had not been used in recent memory and some personnel reacted to it in a different way than intended. For example, some personnel put "out of service lines" back in service and notified the RC while some personnel left the system like it was at the time "Conservative Operations" was initiated (which is the actual intent).

Before the event, numerous network firewall and historian software changes were being implemented with proven change management processes in place. Although network firewall and historian changes were reversed to their previous "pre-change" state, isolation of network segments was still required to identify the source of excessive data traffic. The problem was found to be a historian test server issuing unidentified packets to the other historian servers. The network, not able to interpret the packets, sent them back creating a loop and ultimately resulted in network traffic congestion. This had been a latent code bug which had not previously been found by the vendor or others using the software. After incorporating preventative measures such as removing all of the historian servers from the data network and performing additional troubleshooting, the data network connectivity was restored and systems were monitored to ensure overall performance.

Corrective Actions

The EMS group engaged the historian vendor and implemented a variety of changes to better manage the data network performance between the distributed components of the system. Two reviews, a cross-functional internal and an external, were conducted to evaluate what occurred during the event, the performance of backup tools used, the procedures that are used to inform stakeholders internal and external to operations of an ongoing event's status, and the procedures to manage the system during a state of "Conservative Operations". Changes from this review are being implemented.

Lessons Learned

This event brought forward numerous lessons learned which are:

- All entities should have a procedure such as "Conservative Operations" which provides possible steps they may have to take to ensure reliability. This procedure will forewarn or instruct all parties involved in the use of the power system, including neighbors, of the possible steps that may have to be implemented to maintain situational awareness and reliability.

- Training should be conducted routinely on all procedures especially those related to low probability, high impact events regardless of how often the procedures are used.
- Major updates to new operations systems which are not yet in production should include a proactive involvement with the software vendor.
- "Data throttling" processes should be investigated and implemented for critical networks to ensure their maximum bandwidth limits are not approached and, if limits are approached, automatic steps would be implemented to ensure key critical data is still delivered to critical applications.
- A single "master" scheduling entity should be considered for coordinating changes to firewalls, software, networks, and test systems. The complexity and interdependence of the communications networks, application software, firewalls and test systems of today require this.
- Scheduled telecom and applications infrastructure maintenance activities should intentionally avoid periods of high risk periods of extreme weather, system conditions (e.g. large load ramps) and system activity (e.g. switching) to facilitate the survivability of system operations during these extreme type events.

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 on this lesson learned please contact:

NERC – Lessons Learned (via email)	SERC – SAEA@serc1.org
Source of Lesson Learned:	SERC Reliability Corporation
Lesson Learned #:	20130201
Date Published:	February 8, 2013
Category:	Communications