

Lesson Learned

Loss of EMS Monitoring and Control Functionality for More Than 30 Minutes

Primary Interest Groups

Reliability Coordinator (RC)
Transmission Operator (TOP)
Transmission Owner (TO)
Generator Operator (GOP)

Problem Statement

An Energy Management System (EMS) was lost due to a problem connecting to a relational database management system.

Details

The system failure was triggered by an insufficient amount of disc storage space for the Oracle recovery log area, but no Oracle services terminated as a result of this condition. As Oracle data tables are updated, Oracle saves all changes in “redo logs” to protect the database in the event of an instance failure, which is part of the Oracle online recovery strategy. Since there was no room to update the recovery log area, all attempts to insert or modify records in the data tables were being backed up on the Application server.

The EMS application server will attempt to send data to Oracle in Oracle’s quasi-suspended state as long as an error-free connection is established. Part of the connection recovery involves initializing a number of related processes within a predetermined time frame. During this initialization phase, the EMS Oracle failover subsystem detected that the connection to Oracle was lost again. In addition, the backup and alternate EMS application servers were notified that a failover was initiated by the application server while running as the functional primary and waiting for subsequent messages from the initiating server. The failover process timed out on the initiating functional primary application server, causing the server to be brought down as part of the failure-detection strategy. Since the failover process timed out on the initiating functional primary application server and the other Application servers did not get a complete set of instructions, the remaining servers acted as they were at fault and also failed.

The Oracle recovery area ran out of disc space because of an increased amount of historical data being collected. The system is designed to operate without Oracle for a period of time; therefore, the system can handle Oracle being shut down manually or abruptly and remaining down. The intermittent connection condition as experienced created problems for the software that led to the system failure.

Corrective Actions

The archive area disc space was recovered by deleting accumulated archive log files. Once sufficient disc space was recovered, the Relational Database Management System (RDBMS) was restored to service. The

EMS vendor states that they resolved the issue of the Application servers failing as part of a subsequent software release. The new software release is in the process of being tested.

Lessons Learned

The EMS was generating event messages related to the RDBMS going online and offline well in advance of the system failing. Now that it is known that this condition has the potential to cause a total system failure, maintenance staff has increased the alarm priority to the highest level and can implement automated controls that shut down Oracle in an attempt to prevent this intermittent connection condition. Existing operator training classes will be enhanced to include increased awareness for the meaning and consequences of this and other non-typical system messages.

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 #:

20140802

Date Published:

August 5, 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.