NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Lesson Learned

Control System Network Switch Failure

Primary Interest Groups

Generator Owners (GOs)
Generator Operators (GOPs)

Problem Statement

A partial failure of one of the redundant core switches on a control system mesh network caused a data communication failure. This resulted in two generating units tripping simultaneously, losing a total net output of 1130 MW. There were no alarms or warnings prior to the unit trips.

Details

A data communication failure at a generating plant resulted in both generating units tripping off-line, and the cause of the event was a partial failure of one of the redundant core switches on a control system mesh network. The core switches served as a communications hub for both units. The partial failure of the primary core switch allowed the system to keep its ports open for traffic. The secondary switch detected the problem that the primary switch had and opened its ports for communication, and this simultaneous operation of both switches caused the network to loop, generating a data storm.

The data storm blocked the communication between the boiler controls and the burner management control processors on both units. When communication between these two processors was interrupted, a unit trip occurred. The “loss of fault tolerant burner control system communications processor (BCS CP)” was the immediate cause of the unit trips. Consequently, the turbine control system on each unit listed its associated BMS as its trip signal source.

The switch alarming is monitored in the network internally and is intended to notify the operator in the event of a switch fail-over or a switch port failure. However, due to the data storm, the operator did not receive any alarms prior to the event. The first indication of a problem to the operator was all operator screens experienced a loss of communications with the rest of the control system, which resulted in loss of visibility into the controls on both units.

Corrective Actions

The failed switch and its redundant twin were replaced**.**

Lessons Learned

- Although redundant devices are implemented to increase reliability, implementation of such devices may introduce unanticipated failure scenarios if not fully tested.
- Whenever practical, consider a reliable external monitor that can provide diagnostics and alarming to reduce the risk of an undetected failure.
- Consideration should be given to testing and verification of the network topology and fail-over function.

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 #:	LL20141201
Date Published:	December 9, 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.