NERC Lessons Learned
Loss of Monitoring due to a “Half Failed” High Availability Switch Pair

Kevin Hatch, Manager Reliability Engineering

System Operations Subcommittee

September 1, 2023

Problem Statement

- Due to an incomplete failover between firewalls, an entity experienced intermittent inter-control center communications protocol (ICCP) data failures and data quality issues in the energy management system (EMS) and plant information (PI) applications. As a result, the entity lost monitoring capability for more than 30 minutes until the system was switched to a Backup Control Center

Details

- System operators noticed they had no updates on the data and had frozen screens on EMS and PI displays
- Under normal circumstances, the failover occurs seamlessly between network switches
- The active firewalls connected to the “half failed” switch remained active until they were manually failed over to the second firewall in each firewall pair

Corrective Actions

- The ICCP connections were re-routed to a Backup Control Center, and the EMS network was switched to the Backup Control Center. System operators were already at the backup; both centers are continuously staffed

Lessons Learned

- Entities should work with their switch vendors to configure a firewall health check that continuously confirms the ability to reach devices beyond the directly connected switch.
- In addition to commonly performed failover testing, all aspects of critical system operation must be tested on redundant systems, especially when the system is not fully healthy
- Keeping a small inventory of critical components for quick replacement can help in rapid recovery after a failure and reduce supply chain issues.

NERC Lessons Learned

- LL20230801_Loss_of_Monitoring_Half_Failed_High_Availability_Switch_Pair.pdf (nerc.com)

Contact

Presenter:
Kevin Hatch,
Kevin.Hatch@pjm.com

Member Hotline

(610) 666 – 8980

(866) 400 – 8980

custsvc@pjm.com

PROTECT THE POWER GRID

THINK BEFORE YOU CLICK!

pjm

Be alert to malicious phishing emails.

Report suspicious email activity to PJM.

(610) 666-2244 / it_ops_ctr_shift@pjm.com