

# NERC Lessons Learned

# Loss of Monitoring and Control Due to a Communication Failure Between Control Centers

- **Communication Failure Across Control Centers**
  - Multiple incidents of EMS/SCADA data visibility loss
  - Disruption stemmed from VPN, firewall, and EVPL failures
  - Impacted monitoring and control of grid operations

- **Case 1**

- UPS maintenance at Control Center B caused firewall outage
- ARP issues blocked data despite VPN tunnel being active

- **Case 2**

- Unknown VPN failure led to split-brain between COM servers
- Dual primaries and unsynced databases caused EMS cold start

- **Case 3**

- EVPL degradation limited traffic to one direction
- Servers appeared healthy but weren't transmitting data

- **Immediate Measures**

- Transitioned personnel to alternate centers
- Technical bridges established and vendors engaged
- EMS patch issued and new operational processes implemented

- **Long-Term Fixes**

- Refined COM restart logic
- Improved EMS visibility and field control strategies
- Strengthened vendor coordination for root cause analysis

- **System Design & Operations**

- Co-locate EMS servers with on-site operations staff
- Ensure stable, redundant power and data paths
- Deploy multi-node redundancy to avoid split-brain logic

- **Process Improvements**

- Assign ops staff at BUCC during routine operations
- Use direct connections vs. VPN during maintenance
- Enforce robust heartbeat protocols and contingency plans

- The Lesson Learned document published by NERC can be found at the link below

[Loss of Monitoring and Control Due to a Communication Failure Between Control Centers](#)