

## Lesson Learned

### Implementation of Critical Control Applications

#### Primary Interest Groups

Balancing Authorities  
Distribution Providers  
Generator Operators  
Load Serving Entities  
Reliability Coordinators  
Transmission Operators

#### Problem Statement

An ancillary automatic load-shedding program initiated unintentional load shedding when an Intercontrol Center Communications Protocol data link was interrupted.

#### Details

The entity had recently installed a new EMS system which had an automatic distribution load-shedding function. The automatic load-shedding program was designed to detect a gross imbalance between generation and load and if the triggering criterion was met, it would select distribution feeders and automatically open the breakers to shed load. The load-shedding program configuration defaulted to a 9,999 MW offset when the ICCP data link was interrupted and the telemetry value became invalid. This offset was added to the actual load value, causing the calculated load value to exceed the load-shedding program's trigger threshold.

#### Corrective Actions

- The new load shed program was immediately removed from the EMS production system.
- The system load "offset" was immediately removed from the automatic generation control EMS system.
- The original load-shedding program was returned to service

#### Lesson Learned

- Proper handling of data by EMS or SCADA systems, state estimators, and ancillary programs when the data quality becomes invalid or missing is imperative.
- Entities should understand how data is processed by EMS/SCADA systems and ancillary programs that take independent and automatic system control actions.

- When new critical control applications such as automatic load shedding are implemented, complete functional testing programs should be developed and verified for accuracy.
- Functional testing should be conducted to determine the response of the system based on all possible changes in parameters.
- Where possible, automatic control applications should check against other applications before activating.
- For a period of time after online implementation, critical control applications should always have a notification process and ability for human manual intervention if necessary.

For more information please contact:

Earl Shockley  
Director of Events Analysis and Investigation  
[earl.shockley@nerc.net](mailto:earl.shockley@nerc.net)  
404-446-2560 ext 270

*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.*