NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Lesson Learned

Loss of Communication to Multiple SCADA RTUs at a Switching Center

Primary Interest Groups
Transmission Operators (TOPs)
Reliability Coordinators (RCs)

Problem Statement
Grid operations lost communication with multiple substation remote terminal units (RTUs) when conditions allowed a pre-existing configuration error to express itself. The event that transpired had wide reaching impacts to both control center operations and field personnel.

Details
Communication with a total of 87 RTUs was lost, including 34 Bulk Electric System (BES) RTUs. The various substations affected had operating voltages ranging from four kV to 500 kV. This resulted in the loss of substation control and data acquisition (SCADA) functionality. The total event duration was 78 minutes.

Context Behind the Event:
A Regional switching center that contained the energy management system (EMS) platform for the area's RTU communication was relocated to a newly constructed control room approximately two months prior to this event. The power for this EMS platform was routed through an uninterruptible power supply (UPS) that was a new and different model compared to other Regional switching center facilities.

A transformer that supplied the primary station service power source was taken out of service for maintenance. This created a UPS general alarm that was acknowledged by both the switching center system operator and the transmission dispatcher. The switching center system operator determined that a substation operator needed to be called out to investigate the cause of the alarm. Due to distractions with other scheduled switching that was also taking place, the dispatch request was never issued and the cause of the UPS general alarm was not investigated.

Approximately 5.5 hours later, and as a result of the UPS general alarm not being investigated, communication with the 87 RTUs was lost as the UPS system was operating in battery mode and was unable to maintain proper voltage to operate the communications equipment. A technician was sent to determine the cause of the power failure and found the main circuit breaker to the UPS tripped.

This main circuit breaker was reset and closed by the technician, restoring power to the RTU communications equipment.

Upon Further Review
An inspection determined that the UPS auto/manual restart switch was selected to the manual position, a factory default setting the vendor was unaware of and did not correct during in-servicing of the new

system. In the manual configuration, the UPS system is designed to trip the main circuit breaker for a momentary loss of ac power, and go on battery power as experienced during the event.

The vendor has since set the switch to the "auto" position, which will ensure that the main circuit breaker remains closed and the UPS transfers to the alternate ac power supply. Subsequent local testing has verified the UPS system automatic transfer switch to be functional and now appropriately set.

A latent error had created a system condition that lay undetected until specific circumstances were achieved.

Latent Error:
An error is considered a "Latent Error" when the error has no immediate impact and is not detected until certain conditions trigger or allow its consequences to be revealed. In this case, it was a switch left in the wrong position for the equipment's application.
Some other examples:

- Miswiring that defeats a protection system while not causing an alarm and is not caught in post-modification testing.
- A typo in a database that changes a maintenance schedule from six months to six years, resulting in equipment failure due to lack of maintenance.

Human Performance Perspective

Testing and Energization of New Equipment

The time when new equipment is being installed is the best opportunity for local technicians and substation operators to work with vendors and receive training on new equipment.

The "As Left" condition of newly installed equipment needs to be understood and verified so that proper operation will occur when called upon to perform its required function.

Equipment Has Become More Advanced And Complicated

Many times, physical control switches have been replaced with logic buried in menus on a display screen. This can result in unwanted factory default settings remaining "as delivered" and resulting in equipment not operating as expected.

Control/selector switches may be located in areas that are not normally inspected on a routine basis. This can lead to a condition that is not readily visible to the technician or substation operator.

Understanding the Meaning and Significance of Alarms

There are several circumstances where alarms are grouped together to produce one alarm point and then require in-depth local troubleshooting to determine the actual problem.

Alarm nomenclature can be misleading as to the actual problem or severity of the condition. In this case, a UPS general alarm came in after the loss of primary ac power to the UPS; however, the urgency was not understood as there was no apparent power system trouble.

It was not clear that the communication equipment was running on battery power until the RTU communication failed.

Is the Training Provided Adequate?
Even though new equipment may perform the same function as existing equipment at other locations on the system, new equipment may have features, operating modes, or alarm conditions that exceed similar existing equipment and are either not needed or affect the expected operation of the new equipment.

Lack of familiarity with the operation of this new equipment can lead people to expect it to respond similarly to those existing on the system.

In this case, the UPS system in question was a different make and model than that at other locations on the system and had only been operational for about 2 months.

Work Planning
When planning work that removes a power supply, the planner should know what loads are on that supply, which ones are critical loads, and how those critical loads would be supplied during a configuration change. Without knowledge of these aspects and/or the development of specific written work instructions or a checklist to coordinate the configuration change, much can be left to chance or dependent on individual human performance.

Corrective Actions

- The UPS system auto/manual restart switch at this facility was placed in the auto position.
- Future installations of similar UPS systems have been flagged to ensure correct auto/manual restart switch position selection prior to releasing equipment for regular service.
- Operating personnel have been counselled regarding deficiencies in the response to the UPS general alarm received on the day of the event.
- Mandatory operator response to alarms of this nature have been reinforced, including communication requirements.
- Training was conducted with operations personnel about the importance of the on-site UPS facilities and their impact on area RTUs.
- Training was provided about the locations of all on-site UPS facilities and their local alarm panels.
- Contacts for when UPS facility issues are encountered have been specifically identified and posted.

Lessons Learned

Commissioning

- When new equipment is commissioned and testing is performed by a contractor, the entity should ensure that the contractor's startup checklist includes all necessary settings, including switch positions. Otherwise, a latent error may set up part of the conditions necessary for a later failure.

Alarm False Sense of Security

- Assure that each alarm adequately describes the equipment or system operating status.
  - Sometimes alarm conditions have no immediate undesired consequence. This may lead to a false sense of security if the alarm does not adequately describe the equipment or system operating status.
  - As seen in this case, the RTU equipment continued to operate normally until the UPS battery ran out of power. It is likely that if the alarm actually stated that the UPS was operating on battery power that different actions would have been taken.
  - Properly categorize all alarms so that prioritized and proper action can be taken based on the significance of their cause.

When an Operating Event Is Assessed and Corrected

- Keep looking at the extent of the condition–look beyond the particular adverse event and inspect other areas of your system for similar issues.
  - Are there other pieces of equipment or systems that are new and may have a similar condition/trap in place?
- Periodically review your process for integrating new equipment onto the system. Work to remove any ambiguous meanings of alarming conditions for new equipment between both field and dispatch personnel about its operation.

When Planning Work that Removes an Important Power Supply

- The work planner should know what loads are on that supply (what could be lost?), which ones are critical loads (what absolutely needs to be kept powered?), and how those critical loads would be supplied during the configuration change.
- If there is a critical load or UPS that should automatically switchover to another source, include steps in the work instructions to verify that before turning off the normal source, that the alternate source is available. Then when the normal power is removed, check to ensure that the critical load or UPS does transfer over. If it does not do so automatically, then do it manually and then check that the alternate source is indeed powering it.

- If there is a "maintain positive control" policy to not trust auto transfers, then transfer to the other source manually before removing normal power.

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)	WECC Event Analysis
Source of Lesson Learned:	Western Electric Coordinating Council
Lesson Learned #:	20180601
Date Published:	June 5, 2018
Category:	Transmission Facilities

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.