NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Lesson Learned

Loss of Monitoring or Control Capability due to Power Supply Failure

Primary Interest Groups
Transmission Owners (TOPs)
Reliability Coordinators (RCs)
Balancing Authorities (BAs)

Problem Statement
Several entities have experienced energy management system (EMS) outages due to power supply failure.

Details
Stable and secure power supplies are critical to control rooms, data centers, and substations. Power supplies typically include normal power supply (e.g., utility feeders), standby power supply (e.g., diesel generators), and uninterruptible power supply (UPS).

During the seven EMS outages that are reviewed in this Lessons Learned document, system operator's situational awareness was degraded due to power supply failure.

Case 1:
Maintenance was scheduled at a switching center. According to the procedure, normal power supply was disconnected. However, the automatic transfer switch (ATS) failed to transfer to the standby power supply, an emergency diesel generator. All load was carried on the building UPS battery system. An EMS alarm was generated and sent to both the system operator and the transmission dispatcher.

Maintenance personnel were dispatched to investigate the status of both the main ATS and the emergency generator. The personnel informed the dispatcher that load would remain available for up to eight hours on the UPS battery system. The center experienced a total loss of facility power two hours later, including all EMS workstations. It was later discovered that the UPS battery system actually had only two hours of capacity, not eight hours. The emergency generator failed to start due to a 240v regulator failure.

Case 2:
Maintenance was scheduled to perform a planned building power supply switchgear outage as part of a switchgear upgrade project. The switchgear outage involved an interruption of the UPS power input while maintaining the UPS loads with the battery system. Before removing the UPS power input, facility maintenance personnel verified the UPS system was fully charged and had a 24-minute run time at full load.

Charging power was restored to the UPS nine minutes later. At that time, the FM personnel noticed that the UPS control panel was indicating zero charge on the batteries and recognized that the UPS loads had been de-energized.

Meanwhile, the EMS recorded remote terminal unit (RTU) failure and hardware failure and the EMS servers went offline. The RTU failures were due to loss of power to the "RAD" multiplexers that are normally fed off UPS A/C. The RTUs in the field require the availability of the redundant RAD Multiplexers at both the primary control center (PCC) and backup control center. The loss of the multiplexers at the PCC caused the RTUs in the field to suspend communications.

The entity had just had the UPS maintained and tested satisfactorily by the vendor two months prior. The UPS tests were performed under a normal UPS configuration while connected to float charge, and the batteries were not removed from the float to observe voltage drop at a resting state. The faster discharge rate was determined to be due to a lower battery capacity and not a faster discharge rate.

Case 3:

A communication path between a substation and the control center was lost due to a power supply failure that was caused by loss of a fuse at the substation. The system operator received a pop-up text message about the loss of communication path but failed to notice as it was not an audible alarm. This resulted in a loss of ability to control BES elements at the substation for three hours.

Case 4:

An entity lost multiple RTUs, resulting in stale data being used for the results of EMS analysis for 90 minutes. It was discovered later that the 480 V main breaker was tripped two hours before the event occurred by an unknown reason. After the 480 V main breaker tripped, the load was carried on the UPS system. The UPS system depleted within two hours, triggering a switchover to an alternate source.

When the alternate source was activated, the servers lost power due to the redundant power supplies in the racks not being connected to the alternate power source, causing the RTU failures. An alarm was sent to the building facilities regarding the power supply failure; however, the facilities thought it was a false alarm as they thought it was due to the UPS card, and hence did not notify the control center.

Case 5:

An entity's network traffic was interrupted between the primary control center and the rest of the network. The entity has redundant systems and network equipment; however, the primary and redundant firewall switches that link the primary control center to the rest to the network were connected to the same ATS in the same rack. An overcurrent event caused circuit breakers to open on power distribution units (PDUs) that feed electricity from a UPS to the single ATS. As a result, both firewall switches were de-energized.

Case 6:

There was scheduled maintenance on the UPS system to increase the electrical capacity of the control room. When the load was switched from the "B" side PDU to the "A" side PDU, it caused a breaker to trip

within one of the EMS racks that contained a set of core EMS servers. It was discovered that the PDU overloaded the breaker when all the load was moved to the "A" side to allow working on the "B" side.

Case 7:
The entity experienced loss of Inter-Control Center Communications Protocol (ICCP) connections. The cause of the failure was a loss of power to the control room that was caused by a broken pole that dropped the first circuit into the control center and subsequent line switching issues that dropped the second circuit. The backup generator came on-line, but several systems, including the ICCP connections, were lost due to inrush current upon repowering the devices simultaneously, overloading the breakers for the racks. Power inputs for several devices were connected to the same breaker that had capacity slightly above steady-state requirements. If that breaker gets tripped, those devices lose all power.

Corrective Actions
In each of these cases, upon noticing the degradation of the situational awareness, the entity contacted the appropriate personnel (e.g., RC and operations support staff) to assist with monitoring and help repair the situation.

Case 1:
Facility power was restored when station maintenance personnel initiated a manual override of the ATS, successfully restoring off-site power via the alternate source. The failed 240v regulator was replaced. The standard substation instructions are to be updated to include the expected capacity of the facility UPS battery system with all affected system operating personnel made aware of the revision.

Case 2:
Facilities maintenance manually re-energized individual UPS load centers by physically bypassing the UPS. A separate battery backup was added to the RAD multiplexer power supply in the communications room at the PCC. Substation RTUs are currently connected through multiplexers (MUXs) via serial communications to both RAD multiplexers, one located at the PCC and one at the BCC. The settings for the substation RTUs were modified to allow for continued communication upon the loss of communications path to one of the MUX units. Specifically, the "Automatic Subchannel Disable" function was enabled with a 13.5 second delay on the RADs at the remote RTUs so that communications will restart to the remaining control center RAD Multiplexer upon loss of one channel.

Case 3:
The fuse was replaced. The messages were modified to be audible alarms that require operator acknowledgment.

Case 4:
The building personnel manually switched the servers to the alternate source. The configuration error (the power supplies of the switches were accidentally connected into the same UPS circuit) was corrected.

Case 5:
The circuit breakers were manually closed. The affected ATS was replaced. In addition, an alternate route

will be added to another ATS that will be used for the redundant firewall switches, providing separate power sources between the primary and redundant firewall switches.

Case 6:
The decision was made to fail over to the backup EMS located at the backup control center. The electrical load on the PDUs were distributed to separate breakers within the same PDU.

Case 7:
The following corrective actions have been made:

- Increasing the amp loading capacity of the breaker(s) for the racks that are needed
- Adding additional breakers to the PDU to the racks as needed
- Separating the inputs of the device that were connected to the same breaker
- Redistribute devices to prevent overloading

Lessons Learned

While each of these EMS-related events were slightly different, there were some common themes and lessons learned that can be applied.

- Routines should be created for monthly testing and maintenance running of the backup generator. Test and maintenance operation of a generator should be performed at full load based on the supplier's recommended maintenance routines.
- The necessary UPS battery life, charge cycle, and size should be assessed as part of a risk analysis. The document about the expected capacity of the facility UPS should be up to date.
- Periodic maintenance and monitoring of any UPS system are beneficial. While some UPS systems perform battery maintenance/cycling internally, additional checks and testing may be needed to verify existing bypass capabilities, current loading, and other desired functionality.
- The devices should be balanced between PDUs to prevent overloading. Additional breakers to the PDU are needed when multiple devices are connected to the same breaker.
- It is essential to ensure that the input ratings of the PDU are in harmony with the outlet ratings and that they have the required functions. Intelligent PDUs are recommended because they can monitor the power supply to equipment, unbalanced loading of circuits, power consumption, switching in and out, etc.
- The power supplies of the switches should be connected into the different UPS circuits. The separate routes are needed for the redundant ATS to provide independent power sources between the primary and redundant firewall switches.
- A redundant sealed valve regulated lead acid battery string on each parallel UPS is recommended. In addition to higher reliability, this will allow for more comprehensive testing of each module. The redundant battery string will allow for annual performance testing to include load bank testing and

float voltage testing of a string while it is not in service. The battery strings will also be rotated on a two- to three-month cycle.

- Communication between work groups or departments is vital to maintaining situational awareness of the bulk power system. A procedure should be created and enforced to ensure all work groups/departments (e.g., facility, control room, etc.) are notified of what occurred.
- Mandatory operator response to alarms should be reinforced, including communication requirements. Audible alarms are necessary for operator acknowledgement.

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 is asking entities who have taken action on this lesson learned to respond to 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)	NERC – Event Analysis (via email)
Source of Lesson Learned:	NERC
Lesson Learned #:	20190801
Date Published:	August 1, 2019
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.