NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

NERC Lessons Learned

Mark Vastano, Senior Reliability Analyst
April 23, 2015

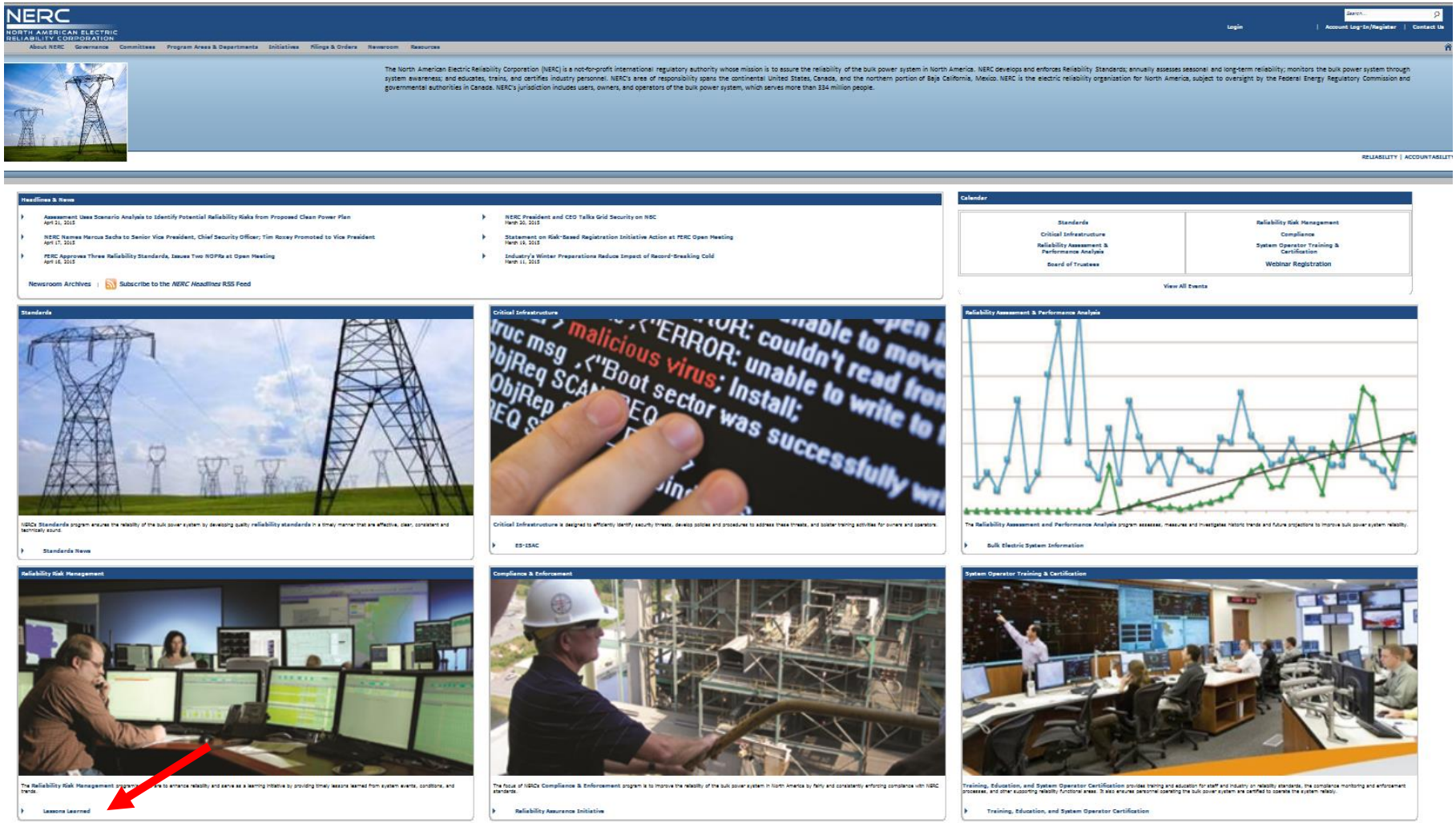
RELIABILITY | ACCOUNTABILITY




Webinar Objectives

- Review the NERC Lessons Learned published since the November 2014 webinar.
- Review the NERC Lessons Learned feedback received to date.

Link to Lessons Learned on NERC Website



Lessons Learned Process

Regional Entity staff are the critical link between the registered entity and NERC staff in the lessons learned (LL) process. Regional Entity staff provide the means of facilitation and feedback between the entity and NERC throughout the process. Regional Entity staff has ownership of the potential LLs emanating from their Region and shepherd those LLs through the process.

NERC Lessons Learned Published since the November 2014 Webinar

Three NERC LLs were published in December 2014

- LL20141201 – Control System Network Switch Failure
- LL20141202 – Bus Differential Power Supply Failure
- LL20141203 – Generation Facilities Loss of Multiple Generators Due to Control Air Problems

Six NERC LLs have been published to date in 2015

- LL20150201 – Digital Inputs to Protection Systems May Need to be Desensitized to Prevent False Tripping Due to Transient Signals
- LL20150202 – Consideration of the Effects of Mutual Coupling when Setting Ground Instantaneous Overcurrent Elements
- LL20150301 – Importance of Backup Energy Management System Failover Testing after Network Device Reconfiguration

NERC Lessons Learned Published since the November 2014 Webinar

2015 Lessons Learned cont.

- LL20150302 – Importance of State Estimator save Cases and Troubleshooting Guide
- LL20150401 – Detailed Installation and Commissioning Testing to Identify Wiring or Design Errors
- LL20150402 – Severe Flooding Damages Transformer Substations

LL20141201 Control System Network Switch Failure

A data communication failure caused by a partial failure of one of the redundant core switches on a Control System mesh network. This resulted in two generating units tripping simultaneously losing total net output of 1130 MW. There were no alarms or warnings prior to the unit trips.

A Data communication failure at a generating plant resulted in both generating units tripping off line. The cause of the event was a partial failure of one of the redundant core switches on a Control System mesh network. The core switches serve as a communications hub for both units. The partial failure of the primary core switch allowed it to keep its ports open for traffic. The secondary switch detected the problem that the primary switch had and opened its ports for communication.

LL20141201 Control System Network Switch Failure

This simultaneous operation of both switches caused the network to loop and generate a data storm

Lesson Learned

Although Redundant devices are implemented to increase reliability, implementation of such devices may introduce unanticipated failure scenarios if not fully tested.

Whenever practical, consider a reliable external monitor that can provide diagnostics and alarming to reduce the risk of failure. Consideration should be given to testing and verification of the network topology and fail-over function.

LL20141202 Bus Differential Power Supply Failure

A microprocessor Bus Differential relay scheme hardware failure initiated a double bus trip on the BES resulting in a loss of 58,000 customers.

The substation has a 115kV Single Breaker Double Bus configuration with 10 elements and is protected by a B90 Bus differential scheme. The scheme consists of 7 IED (intelligent electronic devices) 3 differential relays (one per phase), a tripping IED, Control IED and Bus Selector SW IED. The scheme uses multiple zones of protection to identify and trip only the faulted bus. The zones are identified by “bus selector switch” inputs which are used to place the breaker on Bus -1 or Bus-2. Internal logic places the breaker CT contribution in the bus-1 or Bus-2 differential zone. Using this type of scheme, one bus differential scheme can protect two busses.

LL20141202 Bus Differential Power Supply Failure

- The “A” phase differential relay power supply capacitor started degrading, this caused the reference voltage used in the A/D converter to provide erroneous current and voltage values used in the protection element calculations. This resulted in an A phase differential trip for Bus-1 and Bus-2, the voltage supervision was not effective since the degraded capacitor also resulted in erroneous voltage values used in the differential element supervision. This version of the relay does not monitor the power supply internal logic voltages and therefore the relay did not take itself out of service. The double bus trip resulted in a sustained loss of over 58,000 customers.

Lessons Learned

- The importance of independent device supervision - For important and high impact schemes such as, bus differential schemes using multiple zones in one relay, the supervision should be independent of the tripping device. In this case the mode of failure affected the supervising element along with the tripping element (current) being measured.

LL20141202 Bus Differential Power Supply Failure

Lessons Learned cont.

- The inherent design of this scheme, in which one scheme protects Bus-1 and Bus-2 thereby putting both busses at risk during a device failure or misoperation, must consider increased security of the scheme when applied.
- Relay manufacturers should ensure there is sufficient device self-monitoring to allow the device to be disabled prior to causing an unwanted trip. The manufacture must communicate the risks clearly to the owners and immediately when the problem is discovered.

LL20141203 Loss of Multiple Generators due to Control Air Problems

On more than one occasion, system disturbances have been reported due to the loss of a single air system component causing multiple generating units to trip. The NERC EA staff has observed other occasions of multiple unit trips at generating plants due to degradation of station air supplies.

- In one example, a power plant was equipped with two air headers, which are normally separated. The plant experienced a problem with an air compressor that was serving one of the headers and took that compressor out of service for repair . While this compressor was out of service, the air headers were tied together per plant operating procedure. During the time that the air headers were tied together, a valve on one of the headers failed, which degraded the station air supply for the plant and resulted in multiple generating units tripping.

LL20141203 Loss of Multiple Generators due to Control Air Problems

- In another example, a power plant with a common air header to both of its units experienced an overheating condition in the compressor room, causing two station air compressors to trip. The resulting drop in air pressure supply required the plant operators to manually trip both units due to load swings.
- In a third example, a loss of auxiliary cooling water caused all instrument air compressors at a generating station to trip. The resulting loss of instrument air supply caused the run back and trip of both of the stations generators .

LL20141203 Loss of Multiple Generators due to Control Air Problems

Lessons Learned

- It is recognized that plant design or other circumstances require generating plant personnel to operate with a single air header or multiple air headers tied together. While in that configuration, a problem with any part of the air system supply or the headers may result in a drop in control air and causing multiple units to trip. The amount of time that power plants are in this configuration should be kept to a minimum to reduce the chances of this type of failure occurring. When possible, individual air compressors should be fed from separate power supplies. The installation of additional air compressors may be required to handle a significant loss of station air.

LL20150201 Digital Inputs to Protection Systems May Need to be Desensitized

A converter station was lost due to erroneous initiation of a top-oil temperature trip signal from transformer protection system. The operating entity investigated the connections in the transformer cabinet at the time and visually inspected the transformer and temperature gauges.

- Both the transformer's current temperature and the drag hand for the high-temperature indication were below alarm/trip levels
- No evidence of loose or corroded connections in cabinet
- Multiple events initiated by this type of erroneous input signal have been observed in the event analysis process.
- Protection digital inputs were too sensitive to transient signals, signal noise, or high-resistance contact bridging from outdoor mounted devices
- Determined (with vendor) that loading resistors should be installed on the digital inputs to desensitize them to transient signals

LL20150201 Digital Inputs to Protection Systems May Need to be Desensitized

- The entity identified transient signals were mistaken as a full-contact closure due to arcing or high-resistive bridging of the trip contact. The protection digital inputs were too sensitive to transient signals, signal noise, or high-resistance contact bridging from outdoor mounted devices

Lessons Learned

- Outdoor mounted devices that have inputs to protective relays have the potential to be exposed to shocks and vibrations or may be negatively impacted by dampness and corrosion. These events could cause transients to be detected as contact closure by the protection digital inputs. The protection digital inputs should be designed or modified as necessary to reduce their sensitivity to a possible transient or high resistance contact bridging being incorrectly detected as a full contact closure.

LL20150202 Mutual Coupling when Setting Ground Instantaneous Overcurrent Elements

An event caused the unintended trip of multiple transmission lines and a large generation facility. The trips were due to an incorrect setting on a numerical relay directional ground instantaneous overcurrent (IOC) element. This setting caused it to mis operate in response to a fault on a mutually coupled adjacent line. Failure to consider the effects of mutual coupling between adjacent lines led to the improper derivation of the ground IOC element settings, and this resulted in a protection system mis operation.

- When developing the ground IOC element setting, the entity did not consider nor simulate a line-end fault (with end open) on the adjacent line that was mutually coupled to the protected line
- The adjacent line ran in the same right of way as the protected line for a significant portion of the protected line's length
- Line relays were placed in service with ground IOC settings that had the potential to misoperate

LL20150202 Mutual Coupling when Setting Ground Instantaneous Overcurrent Elements

- Entity disabled ground IOC and relied on directional ground distance elements since both elements were set to instantaneous trip for 80% of line
- For applications where a zone 1 directional ground distance element is not available, the entity has concluded that it is prudent to increase the ground IOC setting design margin applied to the worst-case out-of-zone fault to better account for protection system component tolerances and fault simulation modeling tolerances.

Lessons Learned

It is important that the mutual impedances between all line pairs be calculated and included when developing the system model.

The ground IOC element has no time delay and is therefore considered a zone 1 protection element. When this element is used as part of a protection system, it is critical that it be set so that it will not operate for any credible system event beyond the protected line (out-of-zone), while still providing adequate coverage for ground faults on the protected line. Determining the worst case out-of-zone fault is typically accomplished through the use of a fault simulation software tool to model the transmission system.

LL20150202 Mutual Coupling when Setting Ground Instantaneous Overcurrent Elements

Lessons Learned Cont.

The out-of-zone fault simulations to consider should include:

- A simulation of a fault on each line connected to each remote terminal that is close to the remote terminal with the remote line end open and closed.
- Perform the same simulation described in consideration one with the contingency of having the largest remaining remote terminal ground source out of service.
- Simulate a line-end fault (with end open) on all lines that are mutually coupled with the protected line for more than 10% of the protected lines length.
- Perform the same simulation described in consideration three with the contingency of having the largest remaining remote terminal ground source out of service.

LL20150202 Mutual Coupling when Setting Ground Instantaneous Overcurrent Elements

Lessons Learned Cont.

- It may also be possible to eliminate the use of ground IOC elements if zone 1 ground distance elements can provide adequate ground fault protection and if appropriate consideration is given to providing reliable ground fault protection when a loss of potential condition occurs.

LL20150301 Importance of Backup EMS Failover Testing after Network Device Reconfiguration

There was a loss of energy management system (EMS) supervisory control and data acquisition (SCADA) functionality for 49 minutes during a scheduled transfer of the EMS from the alternate control center (ACC) to the primary control center (PCC). Prior to performing maintenance on the PCC's uninterruptable power supply (UPS), all functionality of the EMS system, including the communication circuits, was successfully transferred from the PCC to the ACC. Upon completion of this maintenance work, the EMS communication circuit vendor was contacted and notified of the organization's intent to request a transfer of the communication circuits from the ACC to the PCC as soon as the PCC was made functional. The vendor provided the name and phone number of the technician who would be available to perform the switching.

LL20150301 Importance of Backup EMS Failover Testing after Network Device Reconfiguration

The EMS analysts attempted to bring system functionality back to the PCC but the attempt was unsuccessful. A full system restart was then performed to establish system functionality at the PCC. The PCC came on-line, but the ACC failed, and EMS analysts were unable to restore ACC functionality. At this moment, the EMS loss-of-functionality event commenced due to the EMS. Communication circuits still being connected to the failed ACC. It should be noted that an EMS loss-of-functionality event will occur every time a full system restart is performed, and the duration of a typical event is five to eight minutes.

LL20150301 Importance of Backup EMS Failover Testing after Network Device Reconfiguration

Following the unsuccessful full system restart, the communication vendor was again contacted and was requested to transfer the communication circuits from the ACC to the PCC. The vendor reported that they were unable to proceed with the EMS communication circuit transfer because they were in the process of performing system maintenance. After the vendor completed this maintenance, the communication circuit transfer was successfully completed and EMS functionality was restored at the PCC. The duration of the EMS loss-of-functionality event was 49 minutes. At the event's conclusion, the ACC remained in a failed state.

LL20150301 Importance of Backup EMS Failover Testing after Network Device Reconfiguration

Upon subsequent investigation, it was discovered that due to a recent and extensive network device reconfiguration, one of the parameters was in error, and this resulted in the inability to restore ACC functionality via a full system restart. Device configuration modifications were then performed, and the ACC was successfully restarted with functionality restored.

Lessons Learned

- EMS maintenance and reconfiguration operations should be closely coordinated with vendors that are needed to support the changes to ensure that there are no overlaps in planned maintenance schedules. Succinct and accurate communication between registered entities and vendors is essential to ensure that both parties fully understand their roles and obligations during planned maintenance operations.

LL20150301 Importance of Backup EMS Failover Testing after Network Device Reconfiguration

Lessons Learned cont.

- Procedures for EMS system restart operations should be rigorously documented to ensure that the EMS can be restarted in the most rapid and secure manner. A step-by-step checklist for the procedure is desirable to ensure that no steps are overlooked. Steps should be included in the procedure to address conditions where restarts do not perform as expected.
- Entities should periodically review EMS redundancy to ensure ongoing independence between sites, including full functional failover testing.
- Entities should review and identify the extent of testing to be performed following significant EMS infrastructure reconfiguration.

LL20150302 Importance of State Estimator Save Cases and Troubleshooting Guide

A state estimator failed to solve for 37 minutes, resulting in real-time contingency analysis also being unavailable. During this event, operators had system visibility via supervisory control and data acquisition (SCADA) and could still take control actions, including the ability to shed load.

The Inter-Control Center Communications Protocol (ICCP) continued to function, providing real-time data to the RC and the other local entities in the RC's footprint. The entity confirmed with its RC that the RC's state estimator and. The entity confirmed with its RC that the RC's state estimator continued to solve and provide real-time contingency analysis. The root cause was never specifically determined. At the time of the event, the state estimator was not archiving save cases on a periodic basis. Because there was no saved data to review, support staff were unable to perform a detailed post-event analysis.

LL20150302 Importance of State Estimator Save Cases and Troubleshooting

Lessons Learned

- A state estimator should be able to automatically and frequently save cases to assist in post-event analysis. It should also automatically save non convergent cases.
- Operators and support staff should have clear guidance and training on troubleshooting state estimator failures. An online state estimator guide for systems operators should be available to ensure consistent troubleshooting. Periodic refresher training should also be employed, including reviews of recent aborted cases.
- A joint review of state estimator issues with other entities should be periodically conducted to ensure applicable common solutions are implemented.

LL20150401 Detailed Installation and Commissioning Testing to Identify Wiring or Design Errors

During a recent event, problems were encountered regarding redundant relays associated with a RAS, where two redundant RAS input/output (I/O) devices failed due to a firmware RAM/ROM processor error. The device failure alarms went undetected because of an error on the wiring diagram that prevented the positive dc from being connected properly, thus disabling the signaling of the I/O device's alarm status. While the schematic (or elementary diagram) correctly showed the proper I/O device alarm circuit design and connections, the wiring diagram of the RAS panel did not match the schematic.

LL20150401 Detailed Installation and Commissioning Testing to Identify Wiring or Design Errors

Lessons Learned

- Detailed checkout and commissioning processes must be in place to catch wiring errors or print discrepancies. These processes must be periodically reinforced in technical meetings or retraining sessions.
- Alarm simulation should include all terminal connections and interconnected wiring.
- Status indications and alarms should be verified by actuating device outputs (preferably by creating the initiating condition) while monitoring for expected status indication and alarms both at the local station and the remote operation center. If unable to fully simulate the alarm condition, initiating the device output is necessary to ensure there are no output wiring polarity issues.

LL20150401 Detailed Installation and Commissioning Testing to Identify Wiring or Design Errors

Lessons Learned Cont.

- Design processes should include peer review.
- Expansion, modification, or both of good utility practices must be continually undertaken with a strong emphasis on human performance.
- Installation and commissioning processes need to be constantly reviewed and reinforced, and checks and tests continually identified and addressed.
- Standardized RAS checkout procedures are a must. Specific requirements should be included in RAS checkout procedures to ensure consistent alarm checkout, utilizing formal individual alarm signoffs at both the local station and the remote operation center via SCADA.
- This is an excellent example of why relay health status alarms should be properly connected to provide remote alarm indications.

LL20150402 Severe Flooding Damages Transformer Substations

A storm resulted in record rainfall of nearly five inches in a short period of time. During the height of the storm, three and a half inches fell within the span of two hours. The downpour resulted in severe localized flooding of two transformer stations, quickly rendering the stations and all terminating circuits unavailable.

The monitoring, protection, and control equipment housed at the transformer stations is located below grade in basements. Flood water damaged this equipment and caused a misoperation of protection and control systems that removed 26,230 kV and eight 115 kV connected circuits from operation.

LL20150402 Severe Flooding Damages Transformer Substations

Lessons Learned

Entities should identify all transmission station buildings with critical power system equipment located below grade and which of these buildings are equipped with:

- Floor drain check valves;
- Sump pits or pumps; and
- Diesel generator capability to power sump pumps.
- Flood protection equipment should be verified to be properly operating during station inspections.
- A mitigation plan should be developed for all buildings identified at key stations, and this plan should be included in future modification plans.

LL20150402 Severe Flooding Damages Transformer Substations

Lessons Learned cont.

- Entities should consider relocating all replacement or new critical power system equipment in above-grade locations.
- Proper roof drains and grading for drainage at the building will help minimize the risk of flooded basements.
- Existing standards for cable conduit design should be revised to ensure that new and replacement cables supplying critical power system equipment enter the building via above-grade entrances. Where cable penetrations are below grade, ensure that they are routinely inspected and properly sealed.

Lessons Learned Feedback

NERC's goal with publishing LLs is to provide industry with technical and understandable information that assists them with maintaining the reliability of the bulk power system. NERC requests that industry provide input on LLs by taking a short survey. A link to the survey is provided on each LL.

Lessons Learned Feedback

LinkedIn™

Sam, see how your posts are doing

as of Sunday, February 22, 2015 11:59 PM PST

Write a new post

Recent posts	Page views	Likes	Comments
NERC's first two 2015 Lessons Learned posted Feb 20, 2015	77	12	--
Three more NERC Lessons Learned posted this week Dec 12, 2014	165	18	--
Three new NERC Lessons Learned posted Sep 16, 2014	67	9	--

Lessons Learned Survey Feedback

109 LL surveys have been received to date, most with positive feedback.

- Question 1 – Was the Lesson Learned understandable and easy to read?
  - 96% answered yes
- Question 2 – Did the Lesson Learned contain enough technical detail?
  - 76% answered yes
- Question 3 – Did the Lesson Learned result in any actions or changes by your company?
  - 24% answered yes
- Question 4 - How will you use this LL in your organization?
  - 76 people provided a text response.

Lessons Learned Survey Feedback

- Question 5 - What additional information would make this Lessons Learned more useful?
  - 56 people provided a text response.
- Question 6 - If NERC publishes another Lessons Learned containing a survey like this would you be willing to take the survey again?
  - 97% answered yes

Webinar Feedback

NERC is interested in your feedback to continually improve our process. In order to help us do so, please take a few minutes to complete the short webinar feedback survey:

https://www.research.net/r/SCPD2GT

Presenter contact information

- Mark Vastano – Mark.Vastano@nerc.net
- Jule Tate – Jule.Tate@nerc.net

Questions and Answers