NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Industry Advisory

Reducing Human Performance Errors by the Use of Configuration Control Practices

Initial Distribution: November 08, 2011

NERC and the Regional Entities have observed inadequate configuration control procedures being employed during Protection System construction or maintenance activities. Entities can further reduce the bulk power system's (BPS) exposure to these reliability risks by considering these examples and suggested barriers and if warranted, augmenting their existing configuration control practices during construction and maintenance activities.

This alert applies only to non-cyber assets.

Why am I receiving this? >>
About NERC Alerts >>

Status:	No Reporting is Required – For Information Only
	PUBLIC: No Restrictions More on handling >>
Instructions:	NERC Advisories are designed to improve reliability by disseminating critical reliability information and are made available pursuant to Rule 810 of NERC's Rules of Procedure, for such use as your organization deems appropriate. **No particular response is necessary.** This NERC Advisory is not the same as a reliability standard, and your organization will not be subject to penalties for failure to implement this Advisory. Additionally, issuance of this Advisory does not lower or otherwise alter the requirements of any approved reliability standard, or excuse the prior failure to follow the practices discussed in the Advisory if such failure constitutes a violation of a reliability standard.
Distribution:	**Initial Distribution:** Distribution Provider, Generator Owner, Generator Operator, Reliability Coordinator, Transmission Owner, Transmission Operator Who else will get this alert? >>

[What are my responsibilities? >>]

Primary Interest Groups:	System Operators, System Operators - System Protection, System Operations - Transmission Engineering, Generation Engineering, Transmission Planning
Advisory:	While the vast majority of Protection System construction and maintenance activities take place without negatively impacting the BPS, NERC and the Regional Entities are aware of situations where entities inadequately employed configuration control practices, resulting in unnecessary BPS equipment outages. The impact of these situations highlights the need for improvement in configuration control procedures during Protection System construction and maintenance. Effective configuration control procedures include the evaluation, approval, and management of changes to an established equipment configuration. By developing and implementing proper configuration control, entities can reduce exposure to the inherent risk of human performance errors that occur during the maintenance and testing of Protection Systems. This document does not intend to prescribe or define all aspects of a configuration control program. Instead, it is intended to highlight a few key elements of a configuration control program that, if properly implemented, could have prevented these incidents. The goal is to improve awareness of common industry practices that, if employed, can help reduce the risks associated with the construction and maintenance of Protection Systems. Below are a few real-world examples of incidents that emphasize the need for better configuration control procedures during Protection System construction and maintenance. Each of these examples demonstrates the risk to BPS reliability when adequate configuration control procedures are not observed. ***Example 1*** A relay technician performing scheduled maintenance on a protective relay system established the proper clearance and isolation procedures to perform the work. These procedures included opening several test switches that would provide an electrical barrier between the isolated equipment and any in-service equipment. After completion of the work, the technician began restoring the test switches to the closed position; however, he overlooked one of the switches in the process, leaving that test switch open. The open switch happened to block the only trip signal to one of the circuit

breakers. The technician released his clearance on the equipment and exited the substation. Sometime later, a fault occurred on the BPS and the open test switch prevented a trip signal from tripping the circuit breaker and from initiating the breaker failure scheme. Because the circuit breaker did not trip, the fault continued to be fed through the closed breaker until it was cleared by remote, time-delayed backup relaying. The result was an undesirable increase in the scope of the BPS equipment outage.

Example 2

During a substation project, the construction team failed to use the latest version of a construction document to complete the installation of a protective relay system. The most recent version of the document had incorporated a configuration change to the CT ratio for the protective relays. Because the team used outdated documentation, the incorrect CT ratio was configured for the relaying. During commissioning, the team failed to detect the error, since their testing reference was to the outdated documents. The Protection System equipment was placed into service with the wrong CT ratio and then sometime later tripped improperly during a system disturbance.

Example 3

A relay technician is performing a preventive maintenance activity on a transmission line protective relay and makes a temporary setting change in order to perform a calibration check. Upon completion of the work, the technician fails to restore the temporary setting to its original value. The equipment was inadvertently placed back in service with the temporary setting installed. The incorrect setting did not immediately produce an improper response; however, weeks later, the relay operated incorrectly for a fault on an adjacent transmission line. The improper line trip resulted in the outage of more BPS equipment than was necessary to clear the fault.

Example 4

A relay technician is working inside a transmission line relay panel, with the necessary work clearance and equipment isolation already established. The technician discovers a need for some additional documentation and steps out of the relay panel and walks over to a nearby file cabinet. Upon his return to the relay panel, the technician is distracted and inadvertently enters a different but identical panel with relaying protecting a BPS element that is in service. Unaware that he has entered the wrong panel, the technician resumes working and eventually crosses two wires that sends a transfer trip signal to a remote substation, tripping an in-service 345Kv transmission line.

Example 5

A technician accidentally opens the wrong current shorting switch for one contribution to a differential relay protecting an in-service transformer, causing the transformer to trip.

The above cases are examples of human performance errors that may have been prevented had adequate barriers and configuration control been applied.

Below are examples of some configuration control practices that are being applied in the maintenance and testing of protection systems. Employing these or similar practices can help entities reduce the risks of human performance errors.

- ***Maintenance Alteration Log (MAL)*** - A record of all manipulations of equipment during a construction or maintenance activity. This document requires the owner to initial each manipulation once when it is performed, and again when the item is restored to its normal state. Proper use of a MAL could have prevented the human error incidents in Examples 1 and 3 above.
- ***Isolation Card*** - A laminated plastic card placed by technicians on the physical equipment at points of isolation during maintenance or testing activities. Each technician has a personalized set of numbered isolation cards. Individual cards are placed on the physical equipment at points of isolation (*e.g.* test switch, control switch, or control panel) and often in a one-to-one association with entries on the MAL. After the technician has completed the work, and all items on the MAL have been restored to normal, the full set of isolation cards should have been collected. If cards are missing, the technician works to resolve the discrepancy before releasing his clearance on the equipment. By employing practices that include proper use of a MAL and Isolation Cards, entities can reduce the risk of the human performance incidents such as in Examples 1 and 3.
- ***Barriers*** - Colored electrical tape or rubber blankets are examples of soft barriers used to cover or protect exposed, energized components to prevent undesired electrical connections during maintenance. A device used to deter the operation of a control switch during a maintenance activity is an example of a rigid barrier. Soft barriers, such as safety tape, can be used as a visual barrier and placed across the openings of in-service equipment panels during maintenance to help prevent personnel from inadvertently entering these panels during a maintenance activity. Use of visual barriers could have been used to help prevent the technician from inadvertently entering an in-service relay panel as in Example 4.

- ***Flagging*** – Signage, safety tape, or any device used to attract the attention of personnel. Flagging can be used to identify equipment that is within the technician's zone of protection or to identify equipment that is outside the zone of protection. Flagging could have been used to help attract the attention of the technician prior to his entering the wrong relay panel, as in Example 4.
- ***Controls for distributing project documentation*** - Revised documentation should be distributed to personnel responsible for the construction, installation and testing, as well as those affected by the change. Old documents should be removed and filed or discarded, as appropriate. After documents have been approved, they should be available at all locations for which they are designated, used, or otherwise necessary, and all obsolete documents should be promptly removed from all points of use to prevent unintended use. Some entities apply such controls by establishing a single source of record for protection information. Proper document distribution controls, including timely distribution of updated documentation and destruction of outdated documentation, could have prevented the incident in Example 2.
- ***Equipment Isolation List*** - A detailed list of equipment isolation points used to electrically isolate the equipment under test during a maintenance or construction activity. Examples of items that would appear on an equipment isolation list are individual test switch poles, control switch positions, circuit breakers, etc. A technician should develop an equipment isolation list and have a peer check it prior to starting the job.
- ***Peer Review/Peer Check*** - The peer check is an independent review, by qualified personnel, to validate the technicians' equipment isolation list. The peer check should be provided by someone other than the technician performing the work or by members of a team that peer check each other's work. Peer review may be effectively used in conjunction with other practices, such as when relay settings have been modified in the field for testing or installation purposes by downloading or documenting the setting left on the relay and having an independent reviewer compare the setting with the office record.
- ***Self Check–*** Self checking is the process of pausing to review one's own actions prior to executing error-likely tasks. It is a four-step mental process to prevent errors, particularly on critical tasks or an irreversible procedure or step. Using the acronym **STAR**: **S**top and take the time to eliminate external distractions, focus on the task at hand with 100% undivided and focused attention. **T**hink, verify that no critical conditions have changed, consider the impact of your immediate action and

question anything that you are have uneasy feelings about or are uncertain. **A**ct, without losing physical or visual contact with the device, remain poised and attentive to your actions. Lastly, **R**eview, verify that you got only the specific results that you expected and wanted. By implementing self-checking skills, the technician could have avoided opening the incorrect test switch in Example 5.

- ***Place-keeping*** **–** A physical marker, either temporary or permanent, that helps one keep his/her place when reviewing sequential lines or columns. Using a straight edge or consistent marking methods, one can mark sequential progress when executing long and detailed procedures. These methods are essential when interruptions or delays prevent fluid movement through a process. Consistent procedures in place-keeping allow smooth transitions and handoffs for events that involve multiple persons to interact on the same or related procedures. Detailed place-keeping also provides a historical record for procedures that occur over extended time periods.
- ***Pre-job briefing*** –A pre-job briefing, also referred to as a tailgate or tailboard meeting, is helpful for providing clarity prior to a job start. These are usually carried out by the supervisor or more experienced personnel who understand details of the work and can point out the potential perils personnel may encounter during construction or maintenance. Some entities document the pre-job briefing in writing and have the document signed by each employee or contractor present on the job site. Pre-job briefings may be appropriate on a daily basis or multiple times during the day depending on the complexity of the work being performed.

The ES-ISAC estimates that the risk to BPS reliability from this vulnerability is **HIGH**, due to the daily exposure of the BPS to the adverse consequences of human performance errors during protection system maintenance and testing.

Background:	The analysis of BPS events frequently identifies human performance errors during protection system maintenance as a root cause or contributing cause of the event.

Contact: Earl Shockley
Director of Reliability Risk Management
Office: (404) 446-2570
earl.shockley@nerc.net

To report any incidents related to this alert, contact:
ES-ISAC 24-hour hotline
(609) 452-1422
esisac@nerc.com

Alert ID: A-2011-11-08-01

You have received this message because you are listed as a primary compliance contact for your organization on the North American Electric Reliability Corporation's compliance registry. If you believe that you have received this message in error, please notify the sender immediately and delete or otherwise dispose of all occurrences or references to this email. If you have questions about your membership in this list, please contact Trion King at NERC by calling (404) 446-9654 or emailing Trion directly at: trion.king@nerc.net.

North American Electric Reliability Corporation
3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
(404) 446-2560 www.nerc.com