Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Development Steps Completed

1. ~~The SAR posted for informal comment June 10, 2011 through July 11, 2011.~~
2. ~~2.~~1. SC authorized moving the SAR forward to standard development at the June 9, 2011 meeting.
3. 2. ~~First posting of Draft Version 1 on~~ The SAR posted for informal comment June 10 – July 11, 2011~~ with~~.
4. 3. Draft 1 of PRC-004-3 was posted for a 30-day comment period ~~closed on~~from June 10 – July 11, 2011.
5. 4. Draft 2 of PRC-004-3 was posted for a 45-day concurrent comment and initial ballot period from July 25 – September 7, 2012.

Description of Current Draft

~~This is~~Draft 3 of PRC-004-3 posted for a ~~45~~ 30-day formal comment period with parallel ~~initial~~successive ballot.

Anticipated Actions	Anticipated Date
~~45~~30-day Formal Comment Period with ~~Parallel Initial~~Successive Ballot	~~July, 2012~~January, 2013
Recirculation ballot	~~October, 2012~~February, 2013
BOT Approval	~~November, 2012~~May, 2013

Effective Dates: First day of the first calendar quarter that is ~~six~~twelve months beyond the date that this standard is approved by applicable regulatory authorities, or in those jurisdictions where regulatory approval is not required, the standard becomes effective on the first day of the first calendar quarter that is ~~six~~twelve months beyond the date this standard is approved by the NERC Board of Trustees, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

Version History

Version	Date	Action	Change Tracking

Definitions of Terms Used in Standard

This section includes all newly defined or revised terms used in the proposed standard. Terms already defined in the Reliability Standards Glossary of Terms are not repeated here. New or revised definitions listed below become approved when the proposed standard is approved. When the standard becomes effective, these defined terms will be removed from the individual standard and added to the Glossary.

Misoperation:

~~Failure of a~~The failure of an Element's composite Protection System to operate as intended.

Any of the following is considered a Misoperation:

1. **Failure to Trip - During Fault** - A failure of a Protection System to operate for a Fault within the zone it is designed to protect. ~~(~~The failure of a Protection System component is not a Misoperation as long as the overall performance of the Protection System for ~~an~~the Element it is designed to protect is correct~~.)~~.

2. **Failure to Trip - Other Than Fault** - A failure of a Protection System to operate for a non-Fault condition for which the Protection System was intended to operate, such as a power swing, under-voltage, over excitation, or loss of excitation. ~~(~~The failure of a Protection System component is not a Misoperation as long as the overall performance of the Protection System for ~~an~~the Element it is designed to protect is correct~~.)~~.

3. **Slow Trip - During Fault** - A Protection System operation that is slower than intended for a Fault within the zone it is designed to protect. ~~(~~Delayed Fault clearing associated with an installed high-speed protection scheme is not a Misoperation if the high-speed performance ~~is required~~has not been identified to meet the dynamic stability performance requirements of the TPL standards ~~or by~~nor is it required to ensure coordination ~~requirements~~ with other Protection Systems~~.)~~.

4. **Slow Trip - Other Than Fault** - A Protection System operation that is slower than intended for a non-Fault condition such as a power swing, under-voltage, over excitation, or loss of excitation for which the Protection System was intended to operate.

5. **Unnecessary Trip - During Fault** - A Protection System operation for a Fault for which the Protection System is not intended to operate~~, excluding any remote Protection System operation that resulted from a failure to trip or slow trip of a local Protection System in a faulted adjacent zone.~~.

6. **Unnecessary Trip - Other Than Fault** - A Protection System operation for a non-Fault condition for which the Protection System is not intended to operate, and is unrelated to on-site maintenance, testing, inspection, construction or commissioning activities.

When this standard has received ballot approval, the text boxes will be moved to the Application Guidelines Section of the Standard.

A. Introduction

1. **Title: Protection System Misoperation Identification and Correction**
2. **Number:** PRC-004-3
3. **Purpose:** Identify and correct the causes of Misoperations of Bulk Electric System (BES) Protection Systems.
4. **Applicability:**

   4.1. Functional Entities:

   4.1.1 Transmission Owner

   4.1.2 Generator Owner

   4.1.3 Distribution Provider

~~**Applicability:** SPS and RMS schemes are not included in this version of the standard because they will be handled in the second phase of this project. UVLS is covered by PRC-022. Some functions of relays are not used as protection but as control function or for automation, therefore, any operation of the control function portion of the automation portion of relays are excluded from this standard.~~

Applicability: Special Protection Systems (SPS) and Remedial Action Schemes (RAS) are not included in this version of the standard because they will be handled in the second phase of this project. UVLS is covered by PRC-022-1. Some functions of relays are not used as protection but as control function or for automation, therefore, any operation of the control function portion or the automation portion of relays are excluded from this standard. See the Guidelines and Technical Basis section of the standard for detailed examples of non-protective functions.

4.2. Facilities

4.2.1 Protection Systems for ~~Facilities that are part of the BES~~BES Elements

~~**4.2.2** Facilities not included~~

4.2.2 Underfrequency Load Shedding (UFLS) that trips a BES Element

~~**4.2.2.1**~~ Special Protection Systems (SPS~~) or~~), Remedial Action Schemes (RAS~~)~~

~~**4.2.2.2**~~), and Undervoltage Load Shedding (UVLS)

4.2.3 ~~Relay functions not included (these~~ are ~~non~~excluded

~~**4.2.3**~~**4.2.4** Non-protective functions that may be imbedded within a Protection System~~)~~ are excluded

~~**4.2.3.1** Control (e.g. controlled shut down of generators or capacitor bank switching. Also see Guidelines and Technical Basis section for detailed examples)~~

~~**4.2.3.2** **Automation (e.g.** data collection)~~

5. Background:

A key element for BES reliability is the correct performance of Protection Systems. Monitoring BES Protection System events, as well as identifying and correcting the causes of Misoperations, will improve Protection System performance. PRC-004-3 Protection System ~~Misoperations~~Misoperation Identification and Correction is a revision of PRC-004-2a Analysis and Mitigation of Transmission and Generation Protection System Misoperations with the stated purpose: Ensure all transmission and generation Protection System Misoperations affecting the reliability of the Bulk Electric System (BES) are analyzed and mitigated. PRC-003-1 Regional Procedure for Analysis of Misoperations of Transmission and Generation Protection Systems required the Regions to establish procedures for analysis of Misoperations. In ~~the NOPR~~FERC Order No. 693, the Commission identified PRC-003-0 as a fill-in-the-blank standard. The ~~NOPR~~Order stated that because the regional procedures had not been submitted, the Commission proposed not to approve or remand PRC-003-0. Because PRC-003-0 (now PRC-003-1) is not enforceable, there is not a mandatory requirement for Regional procedures to support the requirements of PRC-004-2a. This is a potential reliability gap; consequently, PRC-004-3 combines the reliability intent of the two legacy standards PRC-003-1 and PRC-004-2a.

This project includes revising the existing definition of Misoperation, which reads:

Misoperation

- Any failure of a Protection System element to operate within the specified time when a fault or abnormal condition occurs within a zone of protection.
- Any operation for a fault not within a zone of protection (other than operation as backup protection for a fault in an adjacent zone that is not cleared within a specified time for the protection for that zone).
- Any unintentional Protection System operation when no fault or other abnormal condition has occurred unrelated to on-site maintenance and testing activity

In general, this definition needs more specificity and clarity. The terms "specified time" and "abnormal condition" are ambiguous. In the third bullet, more clarification is needed as to whether an unintentional Protection System operation for an atypical yet explainable condition is a Misoperation.

The SAR for this project also includes clarifying reporting requirements. Misoperation data, as currently collected and reported, is not usable to establish ~~a~~ consistent metrics for measuring Protection System performance. ~~The SAR includes establishing a~~ As such, the drafting team is removing the data obligation from the standard ~~with uniform applicability, revising the definition~~and is developing a data request under Section 1600 of ~~Misoperation, and clarifying reporting requirements~~the NERC Rules of Procedure. NERC will analyze the data to: develop meaningful metrics; identify trends in Protection System performance that negatively impact reliability; identify remediation techniques; and publicize lessons learned for the industry. The data submitted as part of the data request will not be used for compliance or enforcement purposes. The removal of the data collection from the standard does not result in a reduction of reliability as Responsible Entities are required to retain evidence of compliance for audit and compliance purposes under the Compliance Section C 1.2 Evidence Retention portion of the standard.

The proposed requirements of the revised Reliability Standard PRC-004-3 meet~~s~~ the following objectives:

- Review all Protection System operations on the BES to identify those that are Misoperations of Protection Systems for Facilities that are part of the BES.
- Analyze Misoperations of Protection Systems for Facilities that are part of the BES to determine the cause(s).

- Develop and implement Corrective Action Plans to address the cause(s) of Misoperations of Protection Systems for Facilities that are part of the BES.

Misoperations of or associated with Special Protection Schemes, Remedial Action Schemes, and Under-Voltage Load Shedding are not addressed in this standard due to their inherent complexities. NERC intends to address these areas through future projects.

Note that the WECC Regional Reliability Standard PRC-004-WECC-1 relates to the reporting of Misoperations for a limited set of WECC Paths and Remedial Action Schemes. In those cases where PRC-004-WECC-1 overlaps with the Continent-wide standard, entities are expected to comply with the more stringent standard.

B. Requirements and Measures

Rationale for R1: This requirement is the first step to ensuring that practices for reviewing and classifying Protection System operations and correcting Misoperations are consistently employed. The ~~SDT~~drafting team believes 120 calendar days takes into account the seasonal nature of Protection System operations; both the volume of Protection System operations as well as outage constraints for investigative purposes can be seasonal. This requirement mandates entities identify and review Protection System operations. Risks to the BES caused by Misoperations are reduced by reviewing all Protection System operations and investigating any Misoperations to find their cause(s). Requirement R1 places the responsibility on the BES interrupting device owner to investigate operations initiated by a Protection System. The initial investigation documentation should be provided to the owner of the Protection System component(s) that contributed to the Misoperation, upon request. The owner of the interrupting device and the entity that owned the component that contributed to the Misoperation should be communicating about the operation before this notification is transmitted. The owner of the component that contributed to the Misoperation will create the CAP, action plan or declaration required by Requirements R2 and R3.

R1. ~~Within 120 calendar days of an interrupting device operation in its Facility caused by a Protection System operation, each~~Each Transmission Owner, Generator Owner, and Distribution Provider shall: *[Violation Risk Factor: Medium][Time Horizon: Operations Assessment, Operations Planning]*

1.1 ~~Identify~~Within 120 calendar days of a BES interrupting device operation in its Facility caused by a Protection System operation, identify and review each Protection System operation.

- If the entity ~~suspects a~~owns both the BES interrupting device and the Protection System, determine if it was a correct operation or a Misoperation.

~~1.1~~
- If the entity owns the BES interrupting device but does not own all of the Protection System and cannot determine that the Protection System operation was correct, then notify the other owner(s) of the Protection System

component(s) ~~owned by another entity contributed to a Misoperation, notify the owner of that Protection System component~~ and provide any requested investigative information.

~~1.2 Designate each Misoperation (if any).~~

- ~~Investigate each~~The Protection System component owner(s) that was notified by the BES interrupting device owner shall determine if there was a correct operation or a Misoperation of their component.

~~1.3~~1.2 Within the same 120 day period of a BES interrupting device operation caused by a Protection System operation, the owner of the Protection System component identified as contributing to the Misoperation ~~(if any)~~shall investigate and document the findings ~~including a cause~~ for each Misoperation including a cause, if identified.

Rationale for R2: A formal CAP is a proven tool for resolving operational problems. Based on industry experience and operational coordination timeframes, the SDT believes 60 calendar days is reasonable for considering such things as alternative solutions, coordination of resources, or development of a schedule for a CAP. When the cause of a Misoperation is determined from implementing an action plan in accordance with Requirement R4, a CAP must be developed in accordance with Requirement R2.

In rare cases, altering the Protection System to avoid a Misoperation recurrence may lower the reliability or performance of the BES. In those cases, documenting the reasons for taking no corrective actions is essential for justifying the close of the Misoperation investigation process and for future reference.

M1. Each Transmission Owner, Generator Owner, and Distribution Provider shall have evidence for Part 1.1 that may include, but is not limited to, dated lists, logs, or a database (electronic or hard copy format) that documents the date and time of each applicable interrupting device operation and ~~an indication~~indicates when each related Protection System operation was reviewed. Acceptable evidence for the notification required by Part 1.1 may include, but is not limited to, emails, electronic files, or hard copy records demonstrating transmittal ~~and receipt~~ of information. Acceptable evidence for Part 1.2 may include, but is not limited to, dated lists, logs, or a database (electronic or hard copy format) that documents the date, time, Facility and equipment name associated with each Misoperation~~. Acceptable evidence for Part 1.3 may include, but is not limited to~~, a copy of a dated Misoperation investigation report or documented findings, which may include sequence of events, relay targets, summary of DME records for each Misoperation.

R2. ~~Within 60 calendar days of identifying the cause(s) of each Misoperation, the~~Each Transmission Owner, Generator Owner, or Distribution Provider shall, within 60 calendar days of identifying the cause of each Misoperation: [*Violation Risk Factor: Medium*] [*Time Horizon: Operations Planning, Long-Term Planning*]

- Develop ~~and document~~ a Corrective Action Plan (CAP) for the identified Protection System component(s) that includes an evaluation of the CAP's applicability to the entity's Protection Systems at other locations, or
- Explain in a declaration why corrective actions are beyond the entity's control or would reduce BES reliability.

M2. Each Transmission Owner, Generator Owner, and Distribution Provider shall have evidence for Requirement R2 that must include a dated CAP or a dated declaration explaining why there is no need to develop a CAP.

~~**Rationale for R2**: A formal CAP is a proven tool for resolving operational problems. Based on industry experience and operational coordination timeframes, the SDT believes 60 calendar days is reasonable for considering such things as alternative solutions, coordination of resources, development of a schedule, or procurement of funds for a CAP.~~

~~In rare cases, altering the Protection System to avoid a Misoperation recurrence may lower the reliability or performance of the BES. In those cases, documenting the reasons for taking no corrective actions is essential for justifying the close out the Misoperation investigation process and future reference.~~

R3. ~~For each Misoperation without an identified cause(s), the~~Each Transmission Owner, Generator Owner, or Distribution Provider shall, within 180 calendar days of the associated BES interrupting device operation, complete for each Misoperation without an identified cause: [*Violation Risk Factor: Medium*] [*Time Horizon: Operations Planning, Long-Term Planning*]

- Development of an action plan that identifies any additional investigative actions and/or Protection System modifications, including a work timetable, or
- A declaration explaining why no further actions will be taken.

Rationale for R3: Where a Misoperation cause is not determined during the initial investigation~~,~~; implementing an action plan of additional investigation/monitoring may determine a cause~~.~~ and lead to the development of a CAP in accordance with Requirement R2. The 180 calendar ~~days~~day period is the sum of 120 calendar days (investigative period in Requirement R1) and a 60 calendar day period (similar timeframe as in Requirement R2 for developing a CAP.)

If the ~~investigation~~action plan completion does not provide direction for identifying the cause, then pursuing further action is not warranted. In these cases, documenting the reasons is essential for justifying the close ~~out~~of the Misoperation investigation process and for future reference.

M3. Each Transmission Owner, Generator Owner, and Distribution Provider shall have evidence for Requirement R3 that must include a dated action plan or a dated declaration.

R4. ~~For each CAP or action plan, the~~Each Transmission Owner, Generator Owner, or Distribution Provider shall~~:~~ implement each CAP or action plan, and revise as needed through completion. [*Violation Risk Factor: High] [Time Horizon: Operations Planning, Long-Term Planning]*

~~**4.1** Implement the CAP or action plan~~

~~**4.2** Maintain detailed implementation records of each CAP or action plan including dated information~~

~~**Rationale for R4**: The CAP or action plan must be fully implemented to accomplish all identified objectives. During the course of implementing a CAP or action plan, revisions may be necessary for a variety of reasons such as scheduling conflicts or resource issues. Documenting the CAP or action plan provides auditable progress and completion confirmation on any plan.~~

Rationale for R4: The CAP or action plan must be completed to accomplish all identified objectives. During the course of implementing a CAP or action plan, revisions may be necessary for a variety of reasons such as scheduling conflicts or resource issues. Documenting the CAP or action plan provides auditable progress and completion confirmation on any plan. When the cause of a Misoperation is determined from implementing an action plan, a CAP must be developed in accordance with Requirement R2.

~~surrounding any revision(s) and completion~~

M4. Each Transmission Owner, Generator Owner, and Distribution Provider shall have evidence for Requirement R4 that must include, but is not limited to, dated electronic or hard copy records which document the implementation of each CAP and action plan~~,~~ and the completion of actions ~~and revisions~~ for each CAP or action plan~~;~~. The evidence may also include dated work management program records, dated work orders, or dated maintenance records.

C. Compliance

1. **Compliance Monitoring Process**

1.1. Compliance Enforcement Authority (CEA)

- As defined in the NERC Rules of Procedure, "Compliance Enforcement Authority" means NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.~~Regional Entity or if the Responsible Entity is owned, operated or controlled by the Regional Entity, then the Regional Entity will establish an agreement with the ERO or another entity approved by the ERO and FERC (i.e. another Regional Entity) to be responsible for compliance enforcement.~~

1.2. Evidence Retention

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. ~~For instances where the evidence retention period specified below is shorter than the time since the last audit, the Compliance Enforcement Authority may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.~~

The Transmission Owner, Generator Owner and Distribution Provider that owns a BES Protection System shall keep data or evidence to show compliance with Requirements R1, R2, R3, and R4 and Measures M1, M2, M3, and M4, since the last audit unless directed by its ~~Compliance Enforcement Authority~~CEA to retain specific evidence for a longer period of time as part of an investigation.

The Transmission Owner, Generator Owner and Distribution Provider that owns a BES Protection System shall retain evidence for all Misoperations with an open investigation, action plan, or CAP even if the BES interrupting device operation occurred prior to the current audit period.

If a Transmission Owner, Generator Owner and Distribution Provider that owns a BES Protection System is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved, or for the time specified above, whichever is longer.

~~The Compliance Enforcement Authority~~The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

Compliance Audit

Self-Certification

Spot Checking

Compliance Investigation

Self-Reporting

Complaint

Periodic Data Submittal

1.4. Additional Compliance Information

~~Each Transmission Owner, Generator Owner, and Distribution Provider that owns BES protection Systems will submit the data identified in PRC-004 - Attachment 1 to the CEA within two calendar months following the end of each calendar quarter.~~

~~The CEA will report the Misoperation information provided by the responsible entities to NERC on a quarterly basis.~~

Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operations Assessment, Operations Planning**	**Medium**	The responsible entity performed the actions in accordance with Requirement R1, Parts 1.1 ~~–~~and 1.~~3~~2 in more than 120 calendar days but less than or equal to ~~130~~150 calendar days of the operation's occurrence. OR The responsible entity	The responsible entity performed the actions in accordance with Requirement R1, Parts 1.1 ~~–~~and 1.~~3~~2 in more than ~~130~~150 calendar days but less than or equal to ~~140~~160 calendar days of the operation's occurrence.	The responsible entity performed the actions in accordance with Requirement R1, Parts 1.1 ~~–~~and 1.~~3~~2 in more than ~~140~~160 calendar days but less than or equal to ~~150~~170 calendar days of the operation's occurrence.	The responsible entity performed the actions in accordance with Requirement R1, Parts 1.1 ~~–~~and 1.~~3~~2 in more than ~~150~~170 calendar days of the operation's occurrence. OR The responsible entity failed to identify and

			identified a Protection System operation that operated one of its BES interrupting devices but failed to review the operation in accordance with Requirement R1, Part 1.1. OR The responsible entity completed its review of a Protection System ~~O~~operation that operated one of its BES interrupting devices in 120 calendar days and determined the operation was a Misoperation and failed to document the findings in accordance with Requirement R1, Part 1.~~3~~2.			review a Protection System operation that operated one of its BES interrupting devices in accordance with Requirement R1, Part 1.1. ~~OR~~ ~~The responsible entity completed its review of a Protection System operation that operated one of its interrupting devices in 120 calendar days and determined the operation was a Misoperation and failed to designate the operation as a Misoperation in accordance with Requirement R1, Part 1.2.~~ OR The responsible entity failed to investigate a Misoperation and document the findings in accordance with Requirement R1, Part 1.~~3~~2.

						OR The ~~responsible~~ entity ~~completed its investigation of a~~that owns the BES interrupting device but does not own the entire Protection System ~~Operation that operated one of its interrupting devices in 120 calendar days and suspected that another entity's~~could not determine if the operation was correct and failed to notify the other owner(s) of the Protection System component ~~contributed to the Misoperation, and failed to notify~~ (s) and provide any requested investigative information ~~to that entity~~ in accordance with Requirement R1, Part 1.1.
R2	**Operations Planning, Long-Term Planning**	**Medium**	The responsible entity developed a CAP, or a declaration in accordance with Requirement R2, in	The responsible entity developed a CAP, or a declaration in accordance with Requirement R2, in	The responsible entity developed a CAP, or a declaration in accordance with Requirement R2, in	The responsible entity developed a CAP, or a declaration in accordance with Requirement R2, more

			more than 60 calendar days but less than or equal to 70 calendar days following the ~~completion~~identification of the ~~investigation or receiving notification~~cause of the Misoperation.	more than 70 calendar days but less than or equal to 80 calendar days following the ~~completion~~identification of the ~~investigation or receiving notification~~cause of the Misoperation.	more than 80 calendar days but less than or equal to 90 calendar days following the ~~completion~~identification of the ~~investigation or receiving notification~~cause of the Misoperation.	than 90 calendar days following the ~~completion~~identification of the ~~investigation or receiving notification~~cause of the Misoperation. OR The responsible entity failed to develop a CAP or make a declaration in accordance with Requirement R2.
R3	**Operations Planning, Long-Term Planning**	**Medium**	The responsible entity developed an action plan, or made a declaration in accordance with Requirement R3, in more than 180 calendar days but less than or equal to ~~190~~210 calendar days following the associated BES interrupting device operation.	The responsible entity developed an action plan, or made a declaration in accordance with Requirement R3, in more than ~~190~~210 calendar days but less than or equal to ~~200~~220 calendar days following the associated BES interrupting device operation.	The responsible entity developed an action plan, or made a declaration in accordance with Requirement R3, in more than ~~200~~220 calendar days but less than or equal to ~~210~~230 calendar days following the ~~completion of the investigation~~associated BES interrupting device operation.	The responsible entity developed an action plan, or made a declaration in accordance with Requirement R3, more than ~~210~~230 calendar days following the ~~completion of the investigation~~associated BES interrupting device operation. OR The responsible entity failed to develop~~, implement, and documented~~ an action plan~~,~~ or a declaration in

						accordance with Requirement R3.
R4	**Operations Planning, Long-Term Planning**	**High**	The responsible entity failed to revise ~~maintained records of~~ a CAP or action plan as needed in accordance with Requirement R4. ~~but the records were incomplete.~~	N/A	N/A	The responsible entity failed to implement a CAP or action plan in accordance with Requirement R4. ~~OR~~ ~~The responsible entity failed to maintain records of a CAP or action plan.~~

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

The composite Protection System in the context of this standard is the total complement of protection for a system Element. All protection for a given Element such as primary, secondary, backup, pilot and non-pilot relay schemes are included in the composite Protection System for the Element. These individual schemes or systems may be isolated or function independently, but aggregate as part of one composite Protection System.

A Protection System is defined in the NERC Glossary of Terms as:

- Protective relays which respond to electrical quantities,
- Communications systems necessary for correct operation of protective functions,
- Voltage and current sensing devices providing inputs to protective relays,
- Station dc supply associated with protective functions (including station batteries, battery chargers, and non-battery-based dc supply), and
- Control circuitry associated with protective functions through the trip coil(s) of the circuit breakers or other interrupting devices.

Circuit breaker and other interrupting device mechanisms are not part of a Protection System.

A revised Misoperation definition is being proposed for industry adoption~~. It~~; the failure of an Element's composite Protection System to operate as intended. The definition includes the following ~~conditions:~~ categories:

(1) A failure of a Protection System to operate for a Fault within the zone it is designed to protect. ~~A lack of target information, e.g. when a high-speed pilot system does not trip because a high-speed zone element trips first, is not a Misoperation. If a fault or abnormal condition is cleared within the time normally expected with proper functioning of at least one Protection System element, then failure of another Protection System element associated with the protection scheme is not a Misoperation~~**The failure of a Protection System component is not a Misoperation as long as the overall performance of the Protection System for the Element it is designed to protect is correct.**

A failure of a transformer's composite Protection System to operate for a transformer Fault is an example of a "failure to trip" Misoperation. This type of Misoperation typically results in the Fault being cleared by remote backup Protection System operations.

A failure of a "primary" transformer relay (or any other component) to operate for a transformer Fault is not a "failure to trip" Misoperation as long as another component of the transformer's composite Protection System operated to clear the Fault. Please see category 3 to see if the "slow trip" classification applies to the operation.

A lack of target information, e.g. when a high-speed pilot system does not target because a high-speed zone element trips first, does not by itself constitute a Misoperation.

(2) A failure of a Protection System to operate for a non-Fault condition for which the Protection System was intended to operate, such as a power swing, under-voltage, over excitation, or loss of excitation. ~~For example,~~**The failure** ~~to trip the generator by loss~~ **of** ~~field protection for~~ **a** ~~loss of field condition on that generator~~**Protection System component is not a Misoperation**~~.~~ **as long as the overall performance of the Protection System for the Element it is designed to protect is correct.**

A failure of a generator's composite Protection System to operate for a loss of field condition is an example of a "failure to trip" Misoperation. This type of Misoperation may require manual operator intervention.

A failure of a "primary" reverse power relay (or any other component) is not a "failure to trip" Misoperation as long as another component of the generator's composite Protection System operated to shut down the generator. Please see category 4 to see if the "slow trip" classification applies to the operation.

The non-Fault conditions cited in the definition are examples only, and do not constitute an all inclusive list.

(3) A Protection System operation that is slower than intended for a Fault within the zone it is designed to protect. Delayed ~~f~~**Fault clearing associated with an installed high-speed protection scheme is not a Misoperation if the high**~~-~~**-speed performance** ~~is~~**has not** ~~required by planning studies associated with~~**been identified to meet the dynamic stability performance requirements of the TPL standards** ~~or by~~**nor is it required to ensure coordination**~~ requirements~~ **with other Protection Systems.**

A failure of a line's composite Protection System to operate as quickly as intended for a line Fault is an example of a "slow trip" Misoperation. This type of Misoperation typically results in remote backup Protection System operations before the Fault is cleared.

In many cases, high-speed protection is installed as part of the utility's standard practice without having the need for high-speed protection for meeting TPL requirements. A slow trip of this Protection System would not negatively impact the dynamic performance of the BES; so, it does not need to be reported. However, even if high-speed clearing is not required, the Protection Systems must coordinate to prevent an "unnecessary trip" Misoperation (e.g. an over trip).

The phrase "slower than intended" means the Protection System operated slower than the objective of the owner(s). It would be impossible to provide a precise tolerance in the definition that would be applicable to every type of Protection System. Rather, the owner(s) reviewing each Protection System operation should have an understanding of the objectives of its Protection Systems, whether those systems operated fast enough to prevent additional harm, and ultimately be able to decide whether the speed or outcome of its Protection System operation was adequate.

The reference to the TPL standards is meant to place some bounds on the time to clear a Fault and prevent dynamic instability. The performance requirements in the TPL standards are found in Table 1, and are applicable to all contingencies mentioned for Type A, B and C contingencies.

Coordination with other Protection Systems refers to the need to ensure that relaying operates in the proper or planned sequence (i.e. the primary relaying for a faulted Element operates before the remote backup relaying for the faulted Element).

(4) A Protection System operation that is slower than intended for a non-Fault condition such as a power swing, under-voltage, over excitation, or loss of excitation for which it was intended to operate. ~~An example of this type of Misoperation is an over excitation condition where the protection designed to detect this condition operated slower than intended resulting in a higher degree of insulation stress than desired.~~

A failure of a generator's composite Protection System to operate as quickly as intended for an over excitation condition is an example of a "slow trip" Misoperation. This type of Misoperation may result in equipment damage.

The phrase "slower than intended" means the composite Protection System operated slower than the objective of the owner(s). It would be impossible to provide a precise tolerance in the definition that would be applicable to every type of Protection System. Rather, the owner(s) reviewing each Protection System operation should have an understanding of the objectives of its Protection Systems, whether those systems operated fast enough to prevent additional harm, and ultimately be able to decide whether the speed or outcome of its Protection System was adequate.

The non-Fault conditions cited in the definition are examples only, and do not constitute an all inclusive list.

(5) A Protection System operation for a Fault for which the Protection System is not intended to operate~~, excluding any remote Protection System operation that resulted from a failure to trip or slow trip of a local Protection System in a faulted adjacent zone.~~ .

An ~~example of~~ operation of a transformer's composite Protection System which over trips for a properly cleared line Fault is an example of an "unnecessary trip" Misoperation. For this type of Misoperation~~is an over-reaching trip due to a lack of coordination between remote and local Protection Systems. Note: Operation of~~, the Fault is typically cleared properly by the faulted equipment's composite Protection System (line relaying, in this case) without the need for an external Protection System's operation.

An operation of a properly coordinated remote Protection Systems is not a Misoperation if the Fault has persisted for a sufficient time to allow the correct operation of the local Protection System to clear the Fault~~in adjacent zones is not~~. An interrupting device failure, a "failure to trip" Misoperation~~of the~~, or a "slow trip" Misoperation may result in a proper remote Protection System ~~if the local Protection System of the faulted Element~~

~~fails to clear the Fault within the intended time; however, the failure of the local Protection System for the faulted zone is a Misoperation~~operation.

(6) A Protection System operation for a non-Fault condition for which the Protection System is not intended to operate~~. These non~~, and is unrelated to on-site maintenance, testing, inspection, construction or commissioning activities.

Non-Fault conditions ~~may~~ include but are not limited to power swings, over excitation~~ or~~, loss of excitation~~ but could include even~~, frequency excursions and normal conditions. ~~For example,~~

An operation of a line's composite Protection System due to a relay failure during normal conditions ~~could conceivably cause~~is an ~~incorrect~~example of an "unnecessary trip ~~and a~~other than Fault" Misoperation.

In a second example, tripping a generator by the operation of loss of field protection during an off-nominal frequency condition while the field is intact is a Misoperation. In a third example, an impedance line relay trip for a power swing that entered the relay's characteristic is a Misoperation if the power swing was stable and the relay operated because it was set with an excessive reach that unnecessarily restricted the line's load carrying capability.~~ This category of Misoperation cannot address at this time other operations during power swings unless the relay is clearly improperly set. Additional clarity on this specific issue will need to await completion of Phase III of Project 2010-13 on Relay Loadability which will address protective relay operations due to power swings as directed by FERC Order No. 733. Finally, an example of an operation that is not a Misoperation under this category is an unintended operation as a result of on-site maintenance, testing, construction or commissioning.~~

An operation that occurs during a non-fault condition but was initiated by on-site maintenance, testing, inspection, construction or commissioning is not a Misoperation. However, once the maintenance, testing, inspection, construction or commissioning has been completed, the "on-site" Misoperation exclusion no longer applies, regardless of the presence of the technical personnel.

This definition is based on the established IEEE/PSRC I3 Working Group on 'Transmission Protective Relay System Performance Measuring Methodology' categories (excluding Failure to Reclose) of Relay System Misoperation. The phrase abnormal condition has been replaced with "non-fault condition" to remove ambiguity.

The exclusion of a component failure, as long as the composite Protection System operates correctly, was based on recommendations by the NERC SPCS. Entities still need to review each Protection System operation. Covering these types of component failures within the standard constitutes additional administrative burden for types of failures that have no immediate reliability impacts.

Failure to automatically reclose after a Fault is not included as a Misoperation because reclosing equipment is not included under the definition of Protection Systems.

~~Interrupting Device~~BES interrupting device operations which are initiated by ~~control systems~~non-protective functions, such as those associated with generator controls, or turbine/boiler controls, Static VAR Compensators (SVCs), Flexible AC Transmission Systems (FACTS), High-Voltage DC (HVDC) transmission systems, circuit breaker mechanisms, or other facility control systems are not operations of a Protection System. Additionally, operations initiated by control functions within protective relays are not considered Protection System operations. For example, in cases where a component of the Protection System or a function of a component within the Protection System is used for control of a generator, such as when a reverse power relay is used to trip a breaker during generator shutdown, the operation of the control component or the function when not providing protection is not included in the definition of Misoperation and its operation would not be reviewed under this standard. Automation (e.g. data collection) is also not a protective function and is not subject to this standard.

A generator Protection System operation prior to closing the unit breaker(s) is not considered a Misoperation~~.~~ provided no in-service BES Elements are tripped. These types of operations are excluded ~~because~~when the generating unit is not synchronized and is isolated from the BES. Protection System operations which occur with the protected Element out of service, that do not trip any in-service Elements are not Misoperations. Protection System operations unrelated to on-site maintenance, testing, inspection, construction or commissioning activities which occur with the protected Element out of service, that trip any in-service Elements are Misoperations.

In some cases where zones of protection overlap, the owner of BES Elements may decide to allow a Protection System to operate faster in order to gain better overall Protection System performance for an Element. For example, the high side of a transformer connected to a line may be within the zone of protection of the supplying line's relaying. In this case, the line relaying is planned to protect the area of the high side of the transformer and into its primary winding. ~~-~~In order to provide faster protection for the line, the line relaying may be designed and set to operate without direct coordination (or coordination is waived) with local protection for Faults on the high side of the connected transformer. Therefore, the operation of the line relaying for a high side transformer Fault would not be considered a Misoperation.

This standard addresses the reliability issues identified in the letter[1] from Gerry Cauley, NERC President and CEO, dated January ~~17, 2010~~7, 2011. "Nearly all major system failures include misoperation of relays as a factor contributing to the propagation of the events…….. Reducing the risk to reliability from relay Misoperations requires consistent collection of misoperation information by regional entities, along with systematic analysis and correction of the underlying causes of preventable Misoperations." The standard also addresses the findings in the 2011 Risk Assessment of Reliability Performance[2]; July 2011 "….a number of multiple outage events were initiated by protection system Misoperations. These events, which go beyond their design expectations and operating procedures, represent a tangible threat to reliability. A deeper review of the root causes of dependent and common mode events, which include three or more automatic outages, is a high priority for NERC and the industry."

[1] http://www.nerc.com/news_pr.php?npr=723
[2] http://www.nerc.com/files/2011_RARPR_FINAL.pdf

In the event of a natural disaster, note that the Sanction Guidelines of the North American Electric Reliability Corporation effective January 15, 2008 provides that the Compliance Monitor will consider extenuating circumstances when considering any sanctions in relation to the timelines outlined in this standard.

Requirement R1

This requirement promotes the prudent evaluation of ~~all~~each Protection System operation~~s~~ to ~~designate~~determine if the operation was correct or a Misoperation, even those Misoperations~~, even those~~ difficult to detect. Unless all BES Protection System operations and Faults that challenge them are reviewed, it cannot be determined with certainty that all Misoperations are identified. For example, if you only reviewed ~~Faults~~operations resulting in an overtrip, you would not necessarily identify Misoperations caused by slow trips.

Requirement ~~1~~R1 places the responsibility on the BES interrupting device owner to investigate operations initiated by a Protection System.~~-~~ The ~~SDT~~drafting team believes the owner of the BES interrupting device that operated would be in the best position to analyze the Protection System operation, determine if a Misoperation occurred, and perform the initial investigation to determine the cause of the Misoperation. If the BES interrupting device owner ~~suspects~~does not own all of the Protection System and cannot determine that the ~~Misoperation~~Protection System operation was ~~caused by a~~correct, then notify the other owner(s) of the Protection System component~~ owned by another entity, they must notify that component owner and document the notification~~(s) and provide any requested investigative information. In this case, it is expected that both entities will work together to investigate the cause of the operation.

Protection Systems are made of many components. These components may be owned by more than one entity. For example, a Generator Owner may own a current transformer that sends information to a Transmission Owner's differential relay. All of these components and many more are part of a Protection System. It is expected that all the owners will communicate with each other, sharing any information freely, so that operations can be analyzed, Misoperations identified and corrective actions taken. If an entity feels it cannot get the level of cooperation it needs to adequately address a Misoperation, the entity should appeal to its Regional Entity for help in resolving the situation.

Determining the cause of Protection System Misoperations is essential in developing an effective remedy to avoid future Misoperations. ~~The SDT~~The drafting team recognizes that there may be multiple causes for a Misoperation; in these circumstances the CAP would include a remedy for the identified causes. The 60 day clock for developing the CAP will be associated with the determination of the first cause. A CAP can be revised if additional causes are found. The drafting team believes 120 calendar days is a reasonable period of time to investigate operations, determine the cause for most Misoperations and document findings in ~~an~~a Misoperation investigation report. This time frame takes into account the seasonal nature of Protection System operations. Both the volume of Protection System operations as well as outage constraints for investigative purposes can be seasonal.

Regardless of whether a cause is identified, the BES interrupting device owner must document the investigation as a potential aid in possible future Misoperation investigations. If a single Protection System causes multiple BES interrupting device owners to be affected, the entities may work together to produce a common Misoperation investigation report. Similarly, if the BES interrupting device owner and the Protection System component owner that caused a Misoperation are different entities, they may work together to produce a common report. ~~Each TO, GO, or DP would be expected to have a copy of the common investigation report.~~

~~An~~A Misoperation investigation report or documented findings may include the following information: 1) initial evidence, 2) probable causes, 3) tests and studies, and 4) conclusions. A brief description of the event surrounding the Misoperation may be included if not separately documented. The initial evidence, which may also be documented separately, contains the sequence of events, relay targets and a summary of Disturbance Monitoring Equipment (DME) records~~.~~ as appropriate. Probable causes are those causes which are most likely to have contributed to the Misoperation and could be considered for further testing. The test and studies documented in the report would describe and provide findings of those tests if the entity was able to perform them during the initial investigation phase (e.g. relay calibration and simulation tests, communication noise and attenuation tests, CT/VT ratio tests, DC continuity checks and functional tests) and studies (e.g. short circuit and coordination studies) performed in the attempt to determine the cause. The conclusions should summarize the cause(s) substantiated by the evidence and findings of the tests and studies.

Requirement ~~2~~R2

If the Misoperation cause is identified within 120 days of the event, Requirement R2 requires Protection System owners to develop a CAP or to make a declaration of no additional action within 60 calendar days of determining the cause. The drafting team recognizes there may be multiple causes for a Misoperation; in these circumstances the CAP would include a remedy for the identified causes. The 60 day clock for developing the CAP will be associated with the determination of the first cause. A CAP can be revised if additional causes are found. Based on industry experience and operational coordination timeframes, the ~~SDT~~drafting team believes 60 calendar days is reasonable for considering such things as alternative solutions, coordination of resources, or development of a schedule~~, or procurement of funds~~ for a CAP, or to prepare a declaration justifying the lack of a CAP.

The 120 day time period and the 60 day time period are distinct and within the context of Requirement R1 and Requirement R2 respectively, need to remain separate. With the ultimate goal of keeping the implementation time of a CAP as short as possible, if a cause of a Misoperation is determined quickly the CAP creation timeframe (60 days) becomes applicable and requires the CAP implementation be less than 180 days. Also, if the interrupting device owner is tardy in informing another Protection System component owner and using up much of the 120 day period, it still leaves a considerable amount of time (at least 60 days) to develop an action plan for further investigation by the Protection System component owner, or if a cause is determined the creation of the CAP.

Where there are multiple Protection System owners involved in a Misoperation, the one or more owners whose Protection System component(s) contributed to the Misoperation will create a CAP or declaration as required by Requirement ~~2~~R2. Owners whose Protection System components operated correctly do not need to create a CAP~~. All owners should update their investigation documentation to indicate which party or parties are performing a CAP to address the Misoperation~~.

Resolving Misoperations benefits the Protection System owner and the BES by ~~improving~~maintaining reliability and security. The CAP is an established tool for resolving operational problems. The NERC Glossary of Terms defines a Corrective Action Plan as "A list of actions and an associated timetable for implementation to remedy a specific problem".

Protection System owners are expected to exercise due diligence in the development and implementation of a CAP. Typically included would be any corrective actions taken to prevent recurrence (along with the date performed), ~~and~~ any corrective actions planned to be taken to prevent recurrence (along with the planned date~~).~~), and an evaluation of the CAP's applicability to other Protection Systems owned by the entity.

~~An example~~The evaluation of ~~a CAP for a Misoperation determined~~the CAP's applicability to ~~have been caused~~other Protection Systems owned by the entity is intended to encourage diligence in preventing similar Misoperations. The Protection System owner is responsible for determining the scope of the problem, and for including appropriate actions in the CAP. The evaluation may result in adding preemptive actions to the CAP. The CAP is complete when all specified actions are completed.

The following are examples of Corrective Action Plans (CAPs):

CAP Example 1 – Corrective actions for a failed relay ~~that has not been repaired might be: "Temporarily~~only:

> The impedance relay was removed ~~failed relay~~ from service on ~~xx/xx/xx. Plan to repair then return~~6/2/12 because it was applying a standing trip. Relay testing was performed on 6/4/12. A failed capacitor was found within the impedance relay. The capacitor was replaced on 6/5/12. The impedance relay functioned properly during testing after the capacitor was replaced. The impedance relay was returned to service on ~~xx/xx/xx."~~6/5/12.
>
> ~~An example of a CAP for a Misoperation determined to have been caused by~~ Applicability to other Protection Systems: Undesired trips of this type of impedance relay due to capacitor failures have occurred only occasionally within our system. This type of impedance relay is gradually being replaced with microprocessor relays as Protection Systems are modernized. It is therefore our assessment that a program for wholesale preemptive replacement of capacitors in this type of impedance relay does not need to be established for our system.

CAP Example 2 - Corrective actions for a failed relay ~~that has been repaired might be: "Temporarily~~, and a program for preemptive actions at similar installations:

The impedance relay was removed ~~failed relay~~ from service on ~~xx/xx/xx. Repaired then returned relay~~ 6/2/12 because it was applying a standing trip. Relay testing was performed on 6/4/12. A failed capacitor was found within the impedance relay. The capacitor was replaced on 6/5/12. The impedance relay functioned properly during testing after the capacitor was replaced. The impedance relay was returned to service on ~~xx/xx/xx."~~6/5/12.

~~An example~~Applicability to other Protection Systems: Undesired trips of this type of impedance relay due to capacitor failures have occurred frequently. It is therefore our assessment that a program should be established by 12/1/12 for wholesale preemptive replacement of capacitors in this type of impedance relay.

A program for wholesale preemptive replacement of capacitors in this type of impedance relay was established on 10/28/12.

CAP Example 3 - Corrective actions for a ~~Misoperation suspected to have been caused by an intermittent relay failure might be: "Temporarily~~failed relay; and preemptive actions for similar installations:

The impedance relay was removed ~~suspect relay~~ from service on ~~xx/xx/xx. Replaced with like kind, and placed in~~ 6/2/12 because it was applying a standing trip. Relay testing was performed on 6/4/12. A failed capacitor was found within the impedance relay. The capacitor was replaced on 6/5/12. The impedance relay functioned properly during testing after the capacitor was replaced. The impedance relay was returned to service on ~~xx/xx/xx."~~6/5/12.

Applicability to other Protection Systems: Undesired trips of this type of impedance relay due to capacitor failures have occurred frequently. It is therefore our assessment that preemptive replacement of capacitors in this type of impedance relay should be pursued.

It is planned to replace the impedance relay capacitors at stations A, B, and C by 9/1/12. It is planned to replace the impedance relay capacitors at stations D, E, and F by 11/1/12. It is planned to replace the impedance relay capacitors at stations G, H, and I by 2/1/13.

The impedance relay capacitor replacement was completed at stations A, B, and C on 8/16/12. The impedance relay capacitor replacement was completed at stations D, E, and F on 10/26/12. The impedance relay capacitor replacement was completed at stations G, H, and I on 1/9/13.

CAP Example 4 - Corrective actions for a firmware problem; and preemptive actions for similar installations:

Fault records were provided to the manufacturer on 6/4/12. On 6/11/12, the manufacturer responded that the misoperation was caused by a bug in version 2 firmware, and recommended installing version 3 firmware. Version 3 firmware was installed on 6/12/12.

Applicability to other Protection Systems: Based on our risk assessment, we plan to install firmware version 3 at all of our installations that are determined to be version 2. Proposed completion date is 12/31/12.

The firmware replacements were completed on 12/4/12.

If the Misoperation cause is identified within 120 days, and no corrective action has been or is intended to be taken, Protection System owners are required to make a declaration to this effect. A "no CAP declaration" would typically include the Misoperation cause and justification for taking no corrective action.

An example of a "no CAP declaration" due to BES reliability might be: "The investigation showed the Misoperation occurred due to transients associated with energizing transformer ABC at Station Y. Our studies show that de-sensitizing the relay to the recorded transients may cause the relay to fail to operate as intended during power system oscillations." A "no CAP declaration" due to BES reliability is expected to be used sparingly.

~~CAPs should include an evaluation as to whether the entity's Protection Systems at other locations are also vulnerable to the same type of Misoperation.~~

~~Requirement 3~~

There are some cases where a Misoperation cause is outside of an entity's control and would result in a "no CAP declaration." Items that may be considered outside of an entity's control could be a non-registered entity communications provider problem or a transmission transformer tapped industrial customer who initiates a direct transfer trip to a registered entity's transmission breaker. Generally, situations where a Misoperation cause emanates from a non-registered outside entity, there may be limited influence an entity can exert on an outside entity and is considered outside of an entity's control. The "outside an entity's control" declaration is expected to be used sparingly.

Requirement R3

If the Misoperation cause is not identified within 120 days, and reasonable investigative actions have not been exhausted, Protection System owners are expected to exercise due diligence in the development and implementation of an action plan for additional investigation. This action plan would typically include any investigative actions taken to determine the cause (along with the date performed), and any investigative actions planned to be taken to determine the cause (along with the planned date).

At the end of 180 days, the Protection System owner must have an action plan or a declaration why no further actions will be taken. The action plan does not need to have been implemented within the 180 days, but it must have been developed within this time frame. The 180 calendar days ~~is~~are the sum of 120 calendar days (investigative period in Requirement R1) and a 60 calendar day period (similar timeframe as in Requirement R2 for developing a CAP.)

Where there are multiple Protection System owners involved in a Misoperation and no cause has been determined, then each Protection System owner must either develop an action plan or declare why no further actions will be taken.

An example of an investigative action plan for more testing might be: "All relays at station A functioned properly during testing on xx/xx/xx. An outage is required to test the relays at station B. The outage is scheduled for xx/xx/xx."

An example of an action plan for adding monitoring might be: "All relays at station A and B functioned properly during testing on xx/xx/xx. It is planned to install a temporary DFR at station A on xx/xx/xx and to monitor the currents for at least 3 months."

An example of an action plan for reviewing relay settings might be: "All relays at station A functioned properly during testing on xx/xx/xx. All relays at station B functioned properly during testing on xx/xx/xx. The carrier system functioned properly during testing on xx/xx/xx. It is planned to complete a relay settings review by xx/xx/xx."

If the Misoperation cause is not identified and reasonable investigative actions have been exhausted within 180 days, Protection System owners are required to make a declaration to this effect. A "no action plan" declaration~~"~~ would typically include any investigative actions taken to determine the cause (along with the date performed), and justification for taking no additional investigative actions.

An example of a "no action plan" declaration~~"~~ might be: "All relays at station A and B functioned properly during testing on xx/xx/xx. The carrier system functioned properly during testing on xx/xx/xx. The carrier coupling equipment functioned properly during testing on xx/xx/xx. A settings review completed on xx/xx/xx indicated the relay settings were proper. Since the equipment involved in the operation functioned properly during testing, the settings were reviewed and found to be proper, and the equipment at station A and station B is already monitored, we have decided to close this investigation."

Requirement R4

~~Finally, the~~The goal of the standard has not been met unless ~~CAP(s)~~CAPs or action plans are actually implemented, as is required in Requirement R4. The responsible entity is required to implement and complete a CAP or action plan to accomplish the purpose of this standard, which is to prevent future Misoperations, thereby minimizing risk to the BES. The responsible entity is also required to complete the CAP or action plan, document the plan implementation, and retain the appropriate evidence to demonstrate implementation and completion.

The goal of an action plan created in Requirement R3 is to determine a cause so a CAP can be created to ultimately remedy the cause of the Misoperation. If the cause is determined as a result of the action plan, the entity must develop a CAP or a declaration within 60 days of determination of cause per Requirement ~~2~~R2. This requirement sets the expectation that the work identified in the CAP or action plan will be completed on schedule as planned. Deferrals or other relevant changes to the CAP or action plan need to be documented so that the record includes not only what was planned, but what was implemented. Depending on the planning and documentation format used by the responsible entity, evidence of successful CAP or action plan execution could consist of signed-off work orders, printouts from work management systems, spreadsheets of planned versus completed work, timesheets, work inspection reports, paid invoices, photographs, walk-through reports or other evidence.

Documentation of a CAP or action plan provides an auditable progress and completion confirmation for specific Misoperations. In addition, the investigative documentation may aid the responsible entity in remedying future Misoperations of a similar nature.

~~**Reporting:**~~

~~A review of the Transmission Availability Data System (TADS) data for the years 2008 – 2010 revealed that the fourth ranked initiating cause of BES outages not related to weather was "Failed Protection System Equipment." Given the high ranking of this metric, it is appropriate to collect data on Protection System Misoperations for analysis to drive improvements in Protection System reliability.~~

~~**Section C-1.4** requires periodic data reporting and references a common reporting format to facilitate consistent reporting of Misoperation data by all Transmission Owners, Generator Owners, and Distribution Providers. Reporting Misoperation data in a common format permits the ERO to analyze the data, develop meaningful metrics for measuring Protection System performance, identify trends in Protection System performance that negatively impact reliability, and identify lessons learned.~~

~~Analysis of data from all Misoperations across North America makes possible identification of issues and trends that may not be identifiable through analysis of smaller data sets on an entity or regional basis. Information regarding identified issues and trends and recommended actions will be shared with Transmission Owners, Generator Owners, and Distribution Providers through lessons learned or industry alerts. Sharing this information will permit recipients to take appropriate actions to drive improvements in Protection System performance.~~

~~The common reporting template also will improve the usefulness of metrics developed to track Protection System performance. While the most relevant category defined in TADS is titled "Failed Protection System Equipment," the title is not an accurate description of the information reported in the metric. This metric includes all Protection System Misoperations that are not related to human error, which is only a subset of all Protection System Misoperations. The Protection System Misoperations related to human error (e.g., miscoordinated settings, incorrect setting calculations, and errors in applying settings to the relay, etc.) are tracked separately from Protection System equipment-related Misoperations, and are grouped together with other human errors by a utility employee or contractor. Similarly, Protection System Misoperations related to failed equipment such as a failed CVT on the primary insulation side are reported under "Failed AC Substation Equipment." Reporting of Misoperations data using the common format specified in C-1.4 will permit development of metrics specific to Protection System Misoperations, with the potential to break down the metric by category of Misoperation (e.g., failure to trip, slow trip, unnecessary trip, etc.) and cause of Misoperation (ac system, dc system, as-left personnel error, incorrect setting/logic/design, and relay failures/malfunctions).~~

~~Reporting Misoperations and their CAPs or action plans provides a means of monitoring and assessing Misoperations. Reviewing and tracking this information provides a method~~

~~of validating the actions taken to address the causes of Misoperations. A second need for reporting Misoperations is to facilitate the identification of trends in Protection System performance that negatively impact reliability. Analyzing data from all Misoperations across North America will make it possible to identify trends that may not be discernible through analysis of smaller data sets on an entity or regional basis.~~

~~Misoperations and updates will be submitted to the Regional Entity on a quarterly basis per the following schedule:~~

~~**Reporting Quarter**~~	~~**Submission Date**~~
~~1st Quarter (Jan 1 – March 31)~~	~~May 31~~
~~2nd Quarter (Apr 1 – June 30)~~	~~August 31~~
~~3rd Quarter (July 1 – Sept 30)~~	~~November 30~~
~~4th Quarter (Oct 1 – Dec 31)~~	~~February 28~~

~~The two calendar months reporting of Misoperations that occurred within the quarterly reporting period corresponds to the recommendations provided by ERO-RAPA and also correlates to the time which the majority of Regional Entities were using in 2011. It is believed that two calendar months is a reasonable time for an entity to submit their Misoperations data after the close of a reporting period. Reporting and updating on a limited time interval and lag (from occurrence) aids in focusing on high trend items of common mode failures. A longer period of time for reporting could prevent high trend failures from being quickly recognized.~~

~~Examples of reporting:~~

1. ~~If a Misoperation occurred on March 30 but was not identified as a Misoperation until June 2, then this Misoperation would be reported in the second quarter reporting period.~~
2. ~~If the Misoperation in example 1 was not completely investigated in the second quarter but a cause was determined on July 2, then a resubmittal should be reported in the third quarter.~~
3. ~~If the Misoperation in examples 1 and 2 had its CAP completed on November 2, then a resubmittal indicating that the CAP was completed should be reported in the fourth quarter.~~