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. SC authorized moving the SAR forward to standard development at the June 9, 2011 meeting.
3. First posting of Draft Version 1 on June 10, 2011 with a comment period closed on July 11, 2011.

Description of Current Draft

This is a 45 day formal comment period with parallel initial ballot.

Anticipated Actions	Anticipated Date
45-day Formal Comment Period with Parallel Initial Ballot	July, 2012
Recirculation ballot	October, 2012
BOT Approval	November, 2012

Effective Dates: First day of the first calendar quarter that is six 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 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 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 Element 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 Element 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 a Misoperation if the high-speed performance is required to meet the performance requirements of the TPL standards or by 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, 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

4.2. Facilities

4.2.1 Protection Systems for Facilities that are part of the BES

4.2.2 Facilities not included

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

4.2.2.2 Undervoltage Load Shedding (UVLS)

4.2.3 Relay functions not included (these are non-protective functions that may be imbedded within a Protection System)

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)

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.

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 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, the Commission identified PRC-003-0 as a fill-in-the-blank standard. The NOPR 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.

Misoperation data, as currently collected and reported, is not usable to establish a consistent metric for measuring Protection System performance. The SAR includes establishing a standard with uniform applicability, revising the definition of Misoperation, and clarifying reporting requirements.

The proposed requirement of the revised Reliability Standard PRC-004-3 meets 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 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

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

1.1 Identify and review each Protection System operation. If the entity suspects a 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).

1.3 Investigate each Misoperation (if any) and document the findings including a cause for each Misoperation, if identified.

M1. Each Transmission Owner, Generator Owner, and Distribution Provider shall have evidence for Part 1.1

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 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). 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.

that may include, but is not limited to, dated lists, logs, or a database that documents the date and time of each interrupting device operation and an indication 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 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 investigation report or documented findings for each Misoperation.

R2. Within 60 calendar days of identifying the cause(s) of each Misoperation, the Transmission Owner, Generator Owner, or Distribution Provider shall: [*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 Transmission Owner, Generator Owner, or Distribution Provider shall, within 180 calendar days of the associated interrupting device operation, complete: [*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 investigation, implementing an action plan of additional investigation/monitoring may determine a cause. The 180 calendar days 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 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 the Misoperation investigation process and 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 Transmission Owner, Generator Owner, or Distribution Provider shall: [*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 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, completion of actions and revisions for each CAP or action plan; dated work management program records, dated work orders, or dated maintenance records.

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.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority (CEA)

- 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 to retain specific evidence for a longer period of time as part of an investigation.

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 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 – 1.3 in more than 120 calendar days but less than or equal to 130 calendar days of the operation's occurrence. OR The responsible entity identified a Protection System operation that operated one of its interrupting devices but failed to review the operation in	The responsible entity performed the actions in accordance with Requirement R1, Parts 1.1 – 1.3 in more than 130 calendar days but less than or equal to 140 calendar days of the operation's occurrence.	The responsible entity performed the actions in accordance with Requirement R1, Parts 1.1 – 1.3 in more than 140 calendar days but less than or equal to 150 calendar days of the operation's occurrence.	The responsible entity performed the actions in accordance with Requirement R1, Parts 1.1 – 1.3 in more than 150 calendar days of the operation's occurrence. OR The responsible entity failed to identify and review a Protection System operation that operated one of its interrupting devices in accordance with Requirement R1, Part

			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 document the findings in accordance with Requirement R1, Part 1.3.			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. OR The responsible entity completed its investigation of a Protection System

						Operation that operated one of its interrupting devices in 120 calendar days and suspected that another entity's Protection System component contributed to the Misoperation, and failed to notify and provide 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 more than 60 calendar days but less than or equal to 70 calendar days following the completion of the investigation or receiving notification.	The responsible entity developed a CAP, or a declaration in accordance with Requirement R2, in more than 70 calendar days but less than or equal to 80 calendar days following the completion of the investigation or receiving notification.	The responsible entity developed a CAP, or a declaration in accordance with Requirement R2, in more than 80 calendar days but less than or equal to 90 calendar days following the completion of the investigation or receiving notification.	The responsible entity developed a CAP, or a declaration in accordance with Requirement R2, more than 90 calendar days following the completion of the investigation or receiving notification. 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 calendar days following the associated interrupting device operation.	The responsible entity developed an action plan, or made a declaration in accordance with Requirement R3, in more than 190 calendar days but less than or equal to 200 calendar days following the associated interrupting device operation.	The responsible entity developed an action plan, or made a declaration in accordance with Requirement R3, in more than 200 calendar days but less than or equal to 210 calendar days following the completion of the investigation.	The responsible entity developed an action plan, or made a declaration in accordance with Requirement R3, more than 210 calendar days following the completion of the investigation. 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 maintained records of a CAP or action plan but the records were incomplete.			The responsible entity failed to implement a CAP or action plan. 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

A revised Misoperation definition is being proposed for industry adoption. It includes the following conditions:

(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.

(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, failure to trip the generator by loss of field protection for a loss of field condition on that generator is a Misoperation.

(3) 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 not required by planning studies associated with the TPL standards or by coordination requirements with other Protection Systems.

(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.

(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 this type of Misoperation is an over-reaching trip due to a lack of coordination between remote and local Protection Systems. Note: Operation of properly coordinated remote Protection Systems to clear the Fault in adjacent zones is not a Misoperation of the 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.

(6) A Protection System operation for a non-Fault condition for which the Protection System is not intended to operate. These non-Fault conditions may include power swings, over excitation or loss of excitation but could include even normal conditions. For example, a relay failure during normal conditions could conceivably cause an incorrect trip and a 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.

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.

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 operations which are initiated by control systems, 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.

A generator Protection System operation prior to closing the unit breaker(s) is not considered a Misoperation. These types of operations are excluded because 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 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 from Gerry Cauley, NERC President and CEO, dated January 17, 2010. "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; 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."

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 Protection System operations to designate 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 resulting in an overtrip, you would not necessarily identify Misoperations caused by slow trips.

Requirement 1 places the responsibility on the interrupting device owner to investigate operations initiated by a Protection System. The SDT believes the owner of the 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 interrupting device owner suspects that the Misoperation was caused by a Protection System component owned by another entity, they must notify that component owner and document the notification. 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 believes 120 calendar days is a reasonable period of time to investigate operations, determine the cause for most Misoperations and document findings in an 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 interrupting device owner must document the investigation as a potential aid in possible future Misoperation investigations. If a single Protection System causes multiple interrupting device owners to be affected, the entities may work together to produce a common investigation report. Similarly, if the 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 investigation report 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. 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

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. 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, or to prepare a declaration justifying the lack of a 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. 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 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).

An example of a CAP for a Misoperation determined to have been caused by a failed relay that has not been repaired might be: "Temporarily removed failed relay from service on xx/xx/xx. Plan to repair then return relay to service on xx/xx/xx."

An example of a CAP for a Misoperation determined to have been caused by a failed relay that has been repaired might be: "Temporarily removed failed relay from service on xx/xx/xx. Repaired then returned relay to service on xx/xx/xx."

An example of a CAP for a Misoperation suspected to have been caused by an intermittent relay failure might be: "Temporarily removed suspect relay from service on xx/xx/xx. Replaced with like kind, and placed in service on xx/xx/xx."

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

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 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 goal of the standard has not been met unless CAP(s) 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. 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.