A. Introduction

1. Title: **Protection System Misoperation Identification and Correction**

2. Number: PRC-004-4(i)

3. Purpose: Identify and correct the causes of Misoperations of Protection Systems for Bulk Electric System (BES) Elements.

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 BES Elements, with the following exclusions:

4.2.1.1 Non-protective functions that are embedded within a Protection System.

4.2.1.2 Protective functions intended to operate as a control function during switching.[1]

4.2.1.3 Special Protection Systems (SPS).

4.2.1.4 Remedial Action Schemes (RAS).

4.2.1.5 Protection Systems of individual dispersed power producing resources identified under Inclusion I4 of the BES definition where the Misoperations affected an aggregate nameplate rating of less than or equal to 75 MVA of BES Facilities.

4.2.2 Underfrequency load shedding (UFLS) that is intended to trip one or more BES Elements.

5. Background:

A key factor for BES reliability is the correct performance of Protection Systems. The monitoring of Protection System events for BES Elements, as well as identifying and correcting the causes of Misoperations, will improve Protection System performance. This Reliability Standard PRC-004-3 – Protection System Misoperation Identification and Correction is a revision of PRC-004-2.1a – Analysis and Mitigation of Transmission and Generation Protection System Misoperations. The Reliability Standard PRC-003-1 – Regional Procedure for Analysis of Misoperations of Transmission and Generation Protection Systems requires Regional Entities to establish procedures for analysis of

[1] For additional information and examples, see the "Non-Protective Functions" and "Control Functions" sections in the Application Guidelines.

Misoperations. In the FERC Order No. 693, the Commission identified PRC-003-0 as a "fill-in-the-blank" standard. The 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 Entity procedures to support the Requirements of PRC-004-2.1a. This is a potential reliability gap; consequently, PRC-004-3 combines the reliability intent of the two legacy standards PRC-003-1 and PRC-004-2.1a.

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 needed 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 included clarifying reporting requirements. Misoperation data, as currently collected and reported, is not optimal to establish consistent metrics for measuring Protection System performance. As such, the data reporting obligation for this standard is being removed and is being developed under the NERC Rules of Procedure, Section 1600 – Request for Data or Information ("data request"). As a result of the data request, 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 removal of the data collection obligation from the standard does not result in a reduction of reliability. The standard and data request have been developed in a manner such that evidence used for compliance with the standard and data request are intended to be independent of each other.

The proposed Requirements of the revised Reliability Standard PRC-004-3 meet 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 identify 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 associated with Special Protection Schemes (SPS) and Remedial Action Schemes (RAS) are not addressed in this standard due to their inherent complexities. NERC plans to handle SPS and RAS in the second phase of this project.

The Western Electric Coordinating Council (WECC) Regional Reliability Standard PRC-004-WECC-1 – Protection System and Remedial Action Scheme Misoperation relates to the reporting of Misoperations of Protection Systems and RAS for a limited set of WECC Paths. The WECC region plans to conduct work to harmonize the regional standard with this continent-wide proposed standard and the second phase of this project concerning SPS and RAS.

Undervoltage load shedding (UVLS) has not been included in this standard's applicability because Misoperations of UVLS relays are currently addressed by Reliability Standard PRC-022-1 – Under-Voltage Load Shedding Program Performance, Requirement R1.5. Underfrequency load shedding (UFLS) was added to PRC-004-3 to close a gap in reliability as Misoperations of UFLS relays are not covered by a Reliability Standard currently.

6. Effective Dates:

See the Implementation Plan for this Standard.

B. Requirements and Measures

R1. Each Transmission Owner, Generator Owner, and Distribution Provider that owns a BES interrupting device that operated under the circumstances in Parts 1.1 through 1.3 shall, within 120 calendar days of the BES interrupting device operation, identify whether its Protection System component(s) caused a Misoperation: *[Violation Risk Factor: High][Time Horizon: Operations Assessment, Operations Planning]*

1.1 The BES interrupting device operation was caused by a Protection System or by manual intervention in response to a Protection System failure to operate; and

1.2 The BES interrupting device owner owns all or part of the Composite Protection System; and

1.3 The BES interrupting device owner identified that its Protection System component(s) caused the BES interrupting device(s) operation or was caused by manual intervention in response to its Protection System failure to operate.

M1. Each Transmission Owner, Generator Owner, and Distribution Provider shall have dated evidence that demonstrates it identified the Misoperation of its Protection System component(s), if any, that meet the circumstances in Requirement R1, Parts 1.1, 1.2, and 1.3 within the allotted time period. Acceptable evidence for Requirement R1, including Parts 1.1, 1.2, and 1.3 may include, but is not limited to the following dated documentation (electronic or hardcopy format): reports, databases, spreadsheets, emails, facsimiles, lists, logs, records, declarations, analyses of sequence of events, relay targets, Disturbance Monitoring Equipment (DME) records, test results, or transmittals.

R2. Each Transmission Owner, Generator Owner, and Distribution Provider that owns a BES interrupting device that operated shall, within 120 calendar days of the BES interrupting device operation, provide notification as described in Parts 2.1 and 2.2. *[Violation Risk Factor: High][Time Horizon: Operations Assessment, Operations Planning]*

2.1 For a BES interrupting device operation by a Composite Protection System or by manual intervention in response to a Protection System failure to operate, notification of the operation shall be provided to the other owner(s) that share Misoperation identification responsibility for the Composite Protection System under the following circumstances:

2.1.1 The BES interrupting device owner shares the Composite Protection System ownership with any other owner; and

2.1.2 The BES interrupting device owner has determined that a Misoperation occurred or cannot rule out a Misoperation; and

2.1.3 The BES interrupting device owner has determined that its Protection System component(s) did not cause the BES interrupting device(s) operation or cannot determine whether its Protection System components caused the BES interrupting device(s) operation.

2.2 For a BES interrupting device operation by a Protection System component intended to operate as backup protection for a condition on another entity's BES Element, notification of the operation shall be provided to the other Protection System owner(s) for which that backup protection was provided.

M2. Each Transmission Owner, Generator Owner, and Distribution Provider shall have dated evidence that demonstrates notification to the other owner(s), within the allotted time period for either Requirement R2, Part 2.1, including subparts 2.1.1, 2.1.2, and 2.1.3 and Requirement R2, Part 2.2. Acceptable evidence for Requirement R2, including Parts 2.1 and 2.2 may include, but is not limited to the following dated documentation (electronic or hardcopy format): emails, facsimiles, or transmittals.

R3. Each Transmission Owner, Generator Owner, and Distribution Provider that receives notification, pursuant to Requirement R2 shall, within the later of 60 calendar days of notification or 120 calendar days of the BES interrupting device(s) operation, identify whether its Protection System component(s) caused a Misoperation. *[Violation Risk Factor: High][Time Horizon: Operations Assessment, Operations Planning]*

M3. Each Transmission Owner, Generator Owner, and Distribution Provider shall have dated evidence that demonstrates it identified whether its Protection System component(s) caused a Misoperation within the allotted time period. Acceptable evidence for Requirement R3 may include, but is not limited to the following dated documentation (electronic or hardcopy format): reports, databases, spreadsheets, emails, facsimiles, lists, logs, records, declarations, analyses of sequence of events, relay targets, DME records, test results, or transmittals.

R4. Each Transmission Owner, Generator Owner, and Distribution Provider that has not determined the cause(s) of a Misoperation, for a Misoperation identified in accordance with Requirement R1 or R3, shall perform investigative action(s) to determine the cause(s) of the Misoperation at least once every two full calendar quarters after the Misoperation was first identified, until one of the following completes the investigation: *[Violation Risk Factor: High] [Time Horizon: Operations Assessment, Operations Planning]*

- The identification of the cause(s) of the Misoperation; or
- A declaration that no cause was identified.

M4. Each Transmission Owner, Generator Owner, and Distribution Provider shall have dated evidence that demonstrates it performed at least one investigative action according to Requirement R4 every two full calendar quarters until a cause is identified or a declaration is made. Acceptable evidence for Requirement R4 may include, but is not limited to the following dated documentation (electronic or hardcopy format): reports, databases, spreadsheets, emails, facsimiles, lists, logs, records, declarations, analyses of sequence of events, relay targets, DME records, test results, or transmittals.

R5. Each Transmission Owner, Generator Owner, and Distribution Provider that owns the Protection System component(s) that caused the Misoperation shall, within 60 calendar days of first identifying a cause of the Misoperation: [*Violation Risk Factor: High*] [*Time Horizon: Operations Planning, Long-Term Planning*]

- Develop a Corrective Action Plan (CAP) for the identified Protection System component(s), and an evaluation of the CAP's applicability to the entity's other Protection Systems including other locations; or
- Explain in a declaration why corrective actions are beyond the entity's control or would not improve BES reliability, and that no further corrective actions will be taken.

M5. Each Transmission Owner, Generator Owner, and Distribution Provider shall have dated evidence that demonstrates it developed a CAP and an evaluation of the CAP's applicability to other Protection Systems and locations, or a declaration in accordance with Requirement R5. Acceptable evidence for Requirement R5 may include, but is not limited to the following dated documentation (electronic or hardcopy format): CAP and evaluation, or declaration.

R6. Each Transmission Owner, Generator Owner, and Distribution Provider shall implement each CAP developed in Requirement R5, and update each CAP if actions or timetables change, until completed. *[Violation Risk Factor: High][Time Horizon: Operations Planning, Long-Term Planning]*

M6. Each Transmission Owner, Generator Owner, and Distribution Provider shall have dated evidence that demonstrates it implemented each CAP, including updating actions or timetables. Acceptable evidence for Requirement R6 may include, but is not limited to the following dated documentation (electronic or hardcopy format): records that document the implementation of each CAP and the completion of actions for each CAP including revision history of each CAP. Evidence may also include work management program records, work orders, and maintenance records.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

As defined in the NERC Rules of Procedure, "Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.

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 CEA 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 shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation.

The Transmission Owner, Generator Owner, and Distribution Provider shall retain evidence of Requirements R1, R2, R3, and R4, Measures M1, M2, M3, and M4 for a minimum of 12 calendar months following the completion of each Requirement.

The Transmission Owner, Generator Owner, and Distribution Provider shall retain evidence of Requirement R5, Measure M5, including any supporting analysis per Requirements R1, R2, R3, and R4, for a minimum of 12 calendar months following completion of each CAP, completion of each evaluation, and completion of each declaration.

The Transmission Owner, Generator Owner, and Distribution Provider shall retain evidence of Requirement R6, Measure M6 for a minimum of 12 calendar months following completion of each CAP.

If a Transmission Owner, Generator Owner, or Distribution Provider 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 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

1.4. Additional Compliance Information

None**.**

D. Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	Operations Assessment, Operations Planning	High	The responsible entity identified whether its Protection System component(s) caused a Misoperation in accordance with Requirement R1, but in more than 120 calendar days and less than or equal to 150 calendar days of the BES interrupting device operation.	The responsible entity identified whether its Protection System component(s) caused a Misoperation in accordance with Requirement R1, but in more than 150 calendar days and less than or equal to 165 calendar days of the BES interrupting device operation.	The responsible entity identified whether its Protection System component(s) caused a Misoperation in accordance with Requirement R1, but in more than 165 calendar days and less than or equal to 180 calendar days of the BES interrupting device operation.	The responsible entity identified whether its Protection System component(s) caused a Misoperation in accordance with Requirement R1, but in more than 180 calendar days of the BES interrupting device operation. OR The responsible entity failed to identify whether its Protection System component(s) caused a Misoperation in accordance with Requirement R1.

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R2	Operations Assessment, Operations Planning	High	The responsible entity notified the other owner(s) of the Protection System component(s) in accordance with Requirement R2, but in more than 120 calendar days and less than or equal to 150 calendar days of the BES interrupting device operation.	The responsible entity notified the other owner(s) of the Protection System component(s) in accordance with Requirement R2, but in more than 150 calendar days and less than or equal to 165 calendar days of the BES interrupting device operation.	The responsible entity notified the other owner(s) of the Protection System component(s) in accordance with Requirement R2, but in more than 165 calendar days and less than or equal to 180 calendar days of the BES interrupting device operation.	The responsible entity notified the other owner(s) of the Protection System component(s) in accordance with Requirement R2, but in more than 180 calendar days of the BES interrupting device operation. OR The responsible entity failed to notify one or more of the other owner(s) of the Protection System component(s) in accordance with Requirement R2.

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R3	Operations Assessment, Operations Planning	High	The responsible entity identified whether or not its Protection System component(s) caused a Misoperation in accordance with Requirement R3, but was less than or equal to 30 calendar days late.	The responsible entity identified whether or not its Protection System component(s) caused a Misoperation in accordance with Requirement R3, but was greater than 30 calendar days and less than or equal to 45 calendar days late.	The responsible entity identified whether or not its Protection System component(s) caused a Misoperation in accordance with Requirement R3, but was greater than 45 calendar days and less than or equal to 60 calendar days late.	The responsible entity identified whether or not its Protection System component(s) caused a Misoperation in accordance with Requirement R3, but was greater than 60 calendar days late. OR The responsible entity failed to identify whether or not a Misoperation of its Protection System component(s) occurred in accordance with Requirement R3.

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R4	Operations Assessment, Operations Planning	High	The responsible entity performed at least one investigative action in accordance with Requirement R4, but was less than or equal to one calendar quarter late.	The responsible entity performed at least one investigative action in accordance with Requirement R4, but was greater than one calendar quarter and less than or equal to two calendar quarters late.	The responsible entity performed at least one investigative action in accordance with Requirement R4, but was greater than two calendar quarters and less than or equal to three calendar quarters late.	The responsible entity performed at least one investigative action in accordance with Requirement R4, but was more than three calendar quarters late. OR The responsible entity failed to perform investigative action(s) in accordance with Requirement R4.

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R5	Operations Planning, Long-Term Planning	High	The responsible entity developed a CAP, or explained in a declaration in accordance with Requirement R5, but in more than 60 calendar days and less than or equal to 70 calendar days of first identifying a cause of the Misoperation. OR (See next page)	The responsible entity developed a CAP, or explained in a declaration in accordance with Requirement R5, but in more than 70 calendar days and less than or equal to 80 calendar days of first identifying a cause of the Misoperation. OR (See next page)	The responsible entity developed a CAP, or explained in a declaration in accordance with Requirement R5, but in more than 80 calendar days and less than or equal to 90 calendar days of first identifying a cause of the Misoperation. OR (See next page)	The responsible entity developed a CAP, or explained in a declaration in accordance with Requirement R5, but in more than 90 calendar days of first identifying a cause of the Misoperation. OR The responsible entity failed to develop a CAP or explain in a declaration in accordance with Requirement R5. OR (See next page)

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R5	(Continued)		The responsible entity developed an evaluation in accordance with Requirement R5, but in more than 60 calendar days and less than or equal to 70 calendar days of first identifying a cause of the Misoperation.	The responsible entity developed an evaluation in accordance with Requirement R5, but in more than 70 calendar days and less than or equal to 80 calendar days of first identifying a cause of the Misoperation.	The responsible entity developed an evaluation in accordance with Requirement R5, but in more than 80 calendar days and less than or equal to 90 calendar days of first identifying a cause of the Misoperation.	The responsible entity developed an evaluation in accordance with Requirement R5, but in more than 90 calendar days of first identifying a cause of the Misoperation. OR The responsible entity failed to develop an evaluation in accordance with Requirement R5.
R6	Operations Planning, Long-Term Planning	High	The responsible entity implemented, but failed to update a CAP, when actions or timetables changed, in accordance with Requirement R6.	N/A	N/A	The responsible entity failed to implement a CAP in accordance with Requirement R6.

E. Regional Variances

None.

F. Interpretations

None.

G. Associated Documents

NERC System Protection and Controls Subcommittee of the NERC Planning Committee, Assessment of Standards: PRC-003-1 – Regional Procedure for Analysis of Misoperations of Transmission and Generation Protection Systems, PRC-004-1 – Analysis and Mitigation of Transmission and Generation Protection Misoperations, PRC-016-1 – Special Protection System Misoperations, May 22, 2009.[2]

Version History

Version	Date	Action	Change Tracking
0	April 1, 2005	Effective Date	New
1	December 1, 2005	1. Changed incorrect use of certain hyphens (-) to "en dash" (–) and "em dash (—)." 2. Added "periods" to items where appropriate. Changed "Timeframe" to "Time Frame" in item D, 1.2.	01/20/06
2		Modified to address Order No. 693 Directives contained in paragraph 1469.	Revised
2	August 5, 2010	Adopted by NERC Board of Trustees	
1a	February 17, 2011	Added Appendix 1 - Interpretation regarding applicability of standard to protection of radially connected transformers	Project 2009-17 interpretation

[2] http://www.nerc.com/comm/PC/System%20Protection%20and%20Control%20Subcommittee%20SPCS%20DL/PRC-003-004-016%20Report.pdf

1a	February 17, 2011	Adopted by NERC Board of Trustees	
1a	September 26, 2011	FERC Order issued approving the interpretation of R1 and R3 (FERC's Order is effective as of September 26, 2011)	
2a	September 26, 2011	Appended FERC-approved interpretation of R1 and R3 to version 2	
2.1a		Errata change: Edited R2 to add "…and generator interconnection Facility…"	Revision under Project 2010-07
2.1a	February 9, 2012	Errata change adopted by NERC Board of Trustees	
2.1a	September 19, 2013	FERC Order issued approving PRC-004-2.1a (approval becomes effective November 25, 2013).	
3	August 14, 2014	Adopted by NERC Board of Trustees	Revision under Project 2010-05.1
4	November 13, 2014	Adopted by NERC Board of Trustees	Applicability revised in Project 2014-01 to clarify application of Requirements to BES dispersed power producing resources.
4	May 29, 2015	FERC Letter Order issued	
4(i)	June 22, 2015	Adopted by Board of Trustees	Revision to VRF designations from "Medium" to "High" for Requirements R1 through R6, in compliance with the Federal Energy Regulatory Commission's directive in N. Am. Elec. Reliability Corp., 151 FERC ¶ 61,129 (2015)

Guidelines and Technical Basis

Introduction

This standard addresses the reliability issues identified in the letter[3] from Gerry Cauley, NERC President and CEO, dated January 7, 2011.

> "Nearly all major system failures, excluding perhaps those caused by severe weather, have misoperations of relays or automatic controls as a factor contributing to the propagation of the failure. …Relays can misoperate, either operate when not needed or fail to operate when needed, for a number of reasons. First, the device could experience an internal failure – but this is rare. Most commonly, relays fail to operate correctly due to incorrect settings, improper coordination (of timing and set points) with other devices, ineffective maintenance and testing, or failure of communications channels or power supplies. Preventable errors can be introduced by field personnel and their supervisors or more programmatically by the organization."

The standard also addresses the findings in the *2011 Risk Assessment of Reliability Performance*[4]; 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."

The *State of Reliability 2014*[5] report continued to identify Protection System Misoperations as a significant contributor to automatic transmission outage severity. The report recommended completion of the development of PRC-004-3 as part of the solution to address Protection System Misoperations.

Definitions

The Misoperation definition is based on the IEEE/PSRC Working Group I3 "Transmission Protective Relay System Performance Measuring Methodology[6]." Misoperations of a Protection System include failure to operate, slowness in operating, or operating when not required either during a Fault or non-Fault condition.

---

3 http://www.nerc.com/pa/Stand/Project%20201005%20Protection%20System%20Misoperations%20DL/20110209130708-Cauley%20letter.pdf

4 "2011 Risk Assessment of Reliability Performance." NERC. http://www.nerc.com/files/2011_RARPR_FINAL.pdf. July 2011. Pg. 3.

5 "State of Reliability 2014." NERC. http://www.nerc.com/pa/Stand/Pages/RelaibilityCoordinationProject20066.aspx. May 2014. Pg. 18 of 106.

6 "Transmission Protective Relay System Performance Measuring Methodology." Working Group I3 of Power System Relaying Committee of IEEE Power Engineering Society. 1999.

For reference, a "Protection System" is defined in the *Glossary of Terms Used in NERC Reliability Standards* ("NERC Glossary") 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.

A BES interrupting device is a BES Element, typically a circuit breaker or circuit switcher that has the capability to interrupt fault current. Although BES interrupting device mechanisms are not part of a Protection System, the standard uses the operation of a BES interrupting device by a Protection System to initiate the review for Misoperation.

The following two definitions are being proposed for inclusion in the NERC Glossary:

> **Composite Protection System –** *The total complement of Protection System(s) that function collectively to protect an Element. Backup protection provided by a different Element's Protection System(s) is excluded.*

The Composite Protection System definition is based on the principle that an Element's multiple layers of protection are intended to function collectively. This definition has been introduced in this standard and incorporated into the proposed definition of Misoperation to clarify that the overall performance of an Element's total complement of protection should be considered while evaluating an operation.

Composite Protection System – Line Example

The Composite Protection System of the Alpha-Beta line (Circuit #123) is comprised of current differential, permissive overreaching transfer trip (POTT), step distance (classic zone 1, zone 2, and zone 3), instantaneous-overcurrent, time-overcurrent, out-of-step, and overvoltage protection. The protection is housed at the Alpha and Beta substations, and includes the associated relays, communications systems, voltage and current sensing devices, DC supplies, and control circuitry.

Composite Protection System – Transformer Example

The Composite Protection System of the Alpha transformer (#2) is comprised of internal differential, overall differential, instantaneous-overcurrent, and time-overcurrent protection. The protection is housed at the Alpha substation, and includes the associated relays, voltage and current sensing devices, DC supplies, and control circuitry.

Composite Protection System – Generator Example

The Composite Protection System of the Beta generator (#3) is comprised of generator differential, overall differential, overcurrent, stator ground, reverse power, volts per hertz, loss-of-field, and undervoltage protection. The protection is housed at the Beta generating plant and at the Beta substation, and includes the associated relays, voltage and current sensing devices, DC supplies, and control circuitry.

Composite Protection System – Breaker Failure Example

Breaker failure protection provides backup protection for the breaker, and therefore is part of the breaker's Composite Protection System. Considering breaker failure protection to be part of another Element's Composite Protection System could lead to an incorrect conclusion that a breaker failure operation automatically satisfies the "Slow Trip" criteria of the Misoperation definition.

- An example of a correct operation of the breaker's Composite Protection System is when the breaker failure relaying tripped because the line relaying operated, but the breaker failed to clear the Fault. The breaker failure relaying operated because of a failed trip coil. The failed trip coil caused a Misoperation of the line's Composite Protection System.
- An example of a correct operation of the breaker's Composite Protection System is when the breaker failure relaying tripped because the line relaying operated, but the breaker failed to clear the Fault. Only the breaker failure relaying operated because of a failed breaker mechanism. This was not a Misoperation because the breaker mechanism is not part of the breaker's Composite Protection System.
- An example of an "Unnecessary Trip – During Fault" is when the breaker failure relaying tripped at the same time as the line relaying during a Fault. The Misoperation was due to the breaker failure timer being set to zero.

Misoperation – *The failure a Composite Protection System to operate as intended for protection purposes. Any of the following is a Misoperation:*

1. **Failure to Trip – During Fault** *– A failure of a Composite Protection System to operate for a Fault condition for which it is designed. The failure of a Protection System component is not a Misoperation as long as the performance of the Composite Protection System is correct.*
2. ***Failure to Trip – Other Than Fault*** *– A failure of a Composite Protection System to operate for a non-Fault condition for which it is designed, such as a power swing, undervoltage, overexcitation, or loss of excitation. The failure of a Protection System component is not a Misoperation as long as the performance of the Composite Protection System is correct.*

3. ***Slow Trip – During Fault*** *– A Composite Protection System operation that is slower than required for a Fault condition if the duration of its operating time resulted in the operation of at least one other Element's Composite Protection System.*
4. ***Slow Trip – Other Than Fault*** *– A Composite Protection System operation that is slower than required for a non-Fault condition, such as a power swing, undervoltage, overexcitation, or loss of excitation, if the duration of its operating time resulted in the operation of at least one other Element's Composite Protection System.*
5. ***Unnecessary Trip – During Fault*** *– An unnecessary Composite Protection System operation for a Fault condition on another Element.*
6. ***Unnecessary Trip – Other Than Fault*** *– An unnecessary Composite Protection System operation for a non-Fault condition. A Composite Protection System operation that is caused by personnel during on-site maintenance, testing, inspection, construction, or commissioning activities is not a Misoperation.*

The Misoperation definition is based on the principle that an Element's total complement of protection is intended to operate dependably and securely.

- Failure to automatically reclose after a Fault condition is not included as a Misoperation because reclosing equipment is not included within the definition of Protection System.
- A breaker failure operation does not, in itself, constitute a Misoperation.
- A remote backup operation resulting from a "Failure to Trip" or a "Slow Trip" does not, in itself, constitute a Misoperation.

This proposed definition of Misoperation provides additional clarity over the current version. A Misoperation is the failure of a Composite Protection System to operate as intended for protection purposes. The definition includes six categories which provide further differentiation of what constitutes a Misoperation. These categories are discussed in greater detail in the following sections.

Failure to Trip – During Fault

This category of Misoperation typically results in the Fault condition being cleared by remote backup Protection System operation.

> **Example 1a:** A failure of a transformer's Composite Protection System to operate for a transformer Fault is a Misoperation.
>
> **Example 1b:** A failure of a "primary" transformer relay (or any other component) to operate for a transformer Fault is not a "Failure to Trip – During Fault" Misoperation as long as another component of the transformer's Composite Protection System operated.
>
> **Example 1c:** A lack of target information does not by itself constitute a Misoperation. When a high-speed pilot system does not target because a high-speed zone element trips first, it would not in and of itself be a Misoperation.
>
> **Example 1d:** A failure of an overall differential relay to operate is not a "Failure to Trip – During Fault" Misoperation as long as another component such as a generator differential relay operated.

Example 1e: The Composite Protection System for a bus does not operate during a bus Fault which results in the operation of all local transformer Protection Systems connected to that bus and all remote line Protection Systems connected to that bus isolating the faulted bus from the grid. The operation of the local transformer Protection Systems and the operation of all remote line Protection Systems correctly provided backup protection. There is one “Failure to Trip – During Fault” Misoperation of the bus Composite Protection System.

In analyzing the Protection System for Misoperation, the entity must also consider whether the “Slow Trip – During Fault” category applies to the operation.

Failure to Trip – Other Than Fault

This category of Misoperation may have resulted in operator intervention. The “Failure to Trip – Other Than Fault” conditions cited in the definition are examples only, and do not constitute an all-inclusive list.

Example 2a: A failure of a generator's Composite Protection System to operate for an unintentional loss of field condition is a Misoperation.

Example 2b: A failure of an overexcitation relay (or any other component) is not a "Failure to Trip – Other Than Fault" Misoperation as long as the generator's Composite Protection System operated as intended isolating the generator from the BES.

In analyzing the Protection System for Misoperation, the entity must also consider whether the “Slow Trip – Other Than Fault” category applies to the operation.

Slow Trip – During Fault

This category of Misoperation typically results in remote backup Protection System operation before the Fault is cleared.

Example 3a: A Composite Protection System that is slower than required for a Fault condition is a Misoperation if the duration of its operating time resulted in the operation of at least one other Element’s Composite Protection System. The current differential element of a multiple function relay failed to operate for a line Fault. The same relay's time-overcurrent element operated after a time delay. However, an adjacent line also operated from a time-overcurrent element. The faulted line's time-overcurrent element was found to be set to trip too slowly.

Example 3b: A failure of a breaker's Composite Protection System to operate as quickly as intended to meet the expected critical Fault clearing time for a line Fault in conjunction with a breaker failure (i.e., stuck breaker) is a Misoperation if it resulted in an unintended operation of at least one other Element’s Composite Protection System. If a generating unit’s Composite Protection System operates due to instability caused by the slow trip of the breaker's Composite Protection System, it is not an “Unnecessary Trip – During Fault” Misoperation of the generating unit’s Composite Protection System. This event would be a “Slow Trip – During Fault” Misoperation of the breaker's Composite Protection System.

> **Example 3c:** A line connected to a generation interconnection station is protected with two independent high-speed pilot systems. The Composite Protection System for this line also includes step distance and time-overcurrent schemes in addition to the two pilot systems. During a Fault on this line, the two pilot systems fail to operate and the time-overcurrent scheme operates clearing the Fault with no generating units or other Elements tripping (i.e., no over-trips). This event is not a Misoperation.

The phrase “slower than required” means the duration of its operating time resulted in the operation of at least one other Element’s Composite Protection System. It would be impractical 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 understand whether the speed and outcome of its Protection System operation met their objective. The intent is not to require documentation of exact Protection System operation times, but to assure consideration of relay coordination and system stability by the owner(s) reviewing each Protection System operation.

The phrase “resulted in the operation of any other Composite Protection System” 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).

In analyzing the Protection System for Misoperation, the entity must also consider the “Unnecessary Trip – During Fault” category to determine if an “unnecessary trip” applies to the Protection System operation of an Element other than the faulted Element.

If a coordination error was at the local terminal (i.e., set too slow), then it was a "Slow Trip," category of Misoperation at the local terminal.

Slow Trip – Other Than Fault

The phrase “slower than required” means the duration of its operating time resulted in the operation of at least one other Element’s Composite Protection System. It would be impractical 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 understand whether the speed and outcome of its Protection System operation met their objective. The intent is not to require documentation of exact Protection System operation times, but to assure consideration of relay coordination and system stability by the owner(s) reviewing each Protection System operation.

> **Example 4:** A phase to phase fault occurred on the terminals of a generator. The generator's Composite Protection System and a transmission line's Composite Protection System both operated in response to the fault. It was found during subsequent investigation that the generator protection contained an inappropriate time delay. This caused the transmission line's correctly set overreaching zone of protection to operate. This was a Misoperation of the generator’s Composite Protection System, but not of the transmission line’s Composite Protection System.

The “Slow Trip – Other Than Fault” conditions cited in the definition are examples only, and do not constitute an all-inclusive list.

Unnecessary Trip – During Fault

An operation of a properly coordinated remote Protection System is not in and of itself a Misoperation if the Fault has persisted for a sufficient time to allow the correct operation of the Composite Protection System of the faulted Element to clear the Fault. A BES interrupting device failure, a “failure to trip” Misoperation, or a “slow trip” Misoperation may result in a proper remote Protection System operation.

> **Example 5:** An operation of a transformer's Composite Protection System which trips (i.e., over-trips) for a properly cleared line Fault is a Misoperation. The Fault is cleared properly by the faulted equipment's Composite Protection System (i.e., line relaying) without the need for an external Protection System operation resulting in an unnecessary trip of the transformer protection; therefore, the transformer Protection System operation is a Misoperation.
>
> **Example 5b:** An operation of a line's Composite Protection System which trips (i.e., over-trips) for a properly cleared Fault on a different line is a Misoperation. The Fault is cleared properly by the faulted line's Composite Protection System (i.e., line relaying); however, elsewhere in the system, a carrier blocking signal is not transmitted (e.g., carrier ON/OFF switch found in OFF position) resulting in the operation of a remote Protection System, single-end trip of a non-faulted line. The operation of the Protection System for the non-faulted line is an unnecessary trip during a Fault. Therefore, the non-faulted line Protection System operation is an “Unnecessary Trip – During Fault” Misoperation.
>
> **Example 5c:** If a coordination error was at the remote terminal (i.e., set too fast), then it was an "Unnecessary Trip – During Fault" category of Misoperation at the remote terminal.

Unnecessary Trip – Other Than Fault

Unnecessary trips for non-Fault conditions include but are not limited to: power swings, overexcitation, loss of excitation, frequency excursions, and normal operations.

> **Example 6a:** An operation of a line's Composite Protection System due to a relay failure during normal operation is a Misoperation.
>
> **Example 6b:** Tripping a generator by the operation of the loss of field protection during an off-nominal frequency condition while the field is intact is a Misoperation assuming the Composite Protection System was not intended to operate under this condition.
>
> **Example 6c:** 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 power swing blocking was enabled and should have prevented the trip, but did not.
>
> **Example 6d:** Tripping a generator operating at normal load by the operation of a reverse power protection relay due to a relay failure is a Misoperation.

Additionally, an operation that occurs during a non-Fault condition but was initiated directly by on-site (i.e., real-time) maintenance, testing, inspection, construction, or commissioning is not a Misoperation.

> **Example 6e:** A BES interrupting device operation that occurs at the remote end of a line during a non-Fault condition because a direct transfer trip was initiated by system maintenance and testing activities at the local end of the line is not a Misoperation because of the maintenance exclusion in category 6 of the definition of "Misoperation."

The "on-site" activities at one location that initiates a trip to another location are included in this exemption. This includes operation of a Protection System when energizing equipment to facilitate measurements, such as verification of current circuits as a part of performing commissioning; however, once the maintenance, testing, inspection, construction, or commissioning activity associated with the Protection System is complete, the "on-site" Misoperation exclusion no longer applies, regardless of the presence of on-site personnel.

Special Cases

Protection System operations for these cases would not be a Misoperation.

> **Example 7a:** A generator Protection System operation prior to closing the unit breaker(s) is not a Misoperation provided no in-service Elements are tripped.

This type of operation is not a Misoperation because the generating unit is not synchronized and is isolated from the BES. Protection System operations that occur when the protected Element is out of service and that do not trip any in-service Elements are not Misoperations.

In some cases where zones of protection overlap, the owner(s) of Elements may decide to allow a Protection System to operate faster in order to gain better overall Protection System performance for an Element.

> **Example 7b:** 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 operated as intended and would not be a Misoperation.

Below are examples of conditions that would be a Misoperation.

> **Example7c:** A 230 kV shunt capacitor bank was released for operational service. The capacitor bank trips due to a settings error in the capacitor bank differential relay upon energization.
>
> **Example 7d:** A 230/115 kV BES transformer bank trips out when being re-energized due to an incorrect operation of the transformer differential relay for inrush after being released for operational service. Only the high-side breaker opens since the low-side breaker had not yet been closed.

Non-Protective Functions

BES interrupting device operations which are initiated by non-protective functions, such as those associated with generator controls, excitation controls, or turbine/boiler controls, static voltampere-reactive compensators (SVC), 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. The standard is not applicable to non-protective functions such as automation (e.g., data collection) or control functions that are embedded within a Protection System.

Control Functions

The entity must make a determination as to whether the standard is applicable to each operation of its Protection System in accordance with the provided exclusions in the standard's Applicability, see Section 4.2.1. The subject matter experts (SME) developing this standard recognize that entities use Protection Systems as part of a routine practice to control BES Elements. This standard is not applicable to operation of protective functions within a Protection System when intended for controlling a BES Element as a part of an entity's process or planned switching sequence. The following are examples of conditions to which this standard is not applicable:

> **Example 8a:** The reverse power protective function that operates to remove a generating unit from service using the entity's normal or routine process.
>
> **Example 8b:** The reverse power relay enables a permissive trip and the generator operator trips the unit.

The standard is not applicable to operation of the protective relay because its operation is intended as a control function as part of a controlled shutdown sequence for the generator. However, the standard remains applicable to operation of the reverse power relay when it operates for conditions not associated with the controlled shutdown sequence, such as a motoring condition caused by a trip of the prime mover.

The following is another example of a condition to which this standard is not applicable:

> **Example 8c:** Operation of a capacitor bank interrupting device for voltage control using functions embedded within a microprocessor based relay that is part of a Protection System.

The above are examples only, and do not constitute an all-inclusive list to which the standard is not applicable.

Extenuating Circumstances

In the event of a natural disaster or other extenuating circumstances, the December 20, 2012 Sanction Guidelines of the North American Electric Reliability Corporation, Section 2.8, Extenuating Circumstances, reads: "In unique extenuating circumstances causing or contributing to the violation, such as significant natural disasters, NERC or the Regional Entity may significantly reduce or eliminate Penalties." The Regional Entities to whom NERC has delegated

authority will consider extenuating circumstances when considering any sanctions in relation to the timelines outlined in this standard.

The volume of Protection System operations tend to be sporadic. If a high rate of Protection System operations is not sustained, utilities will have an opportunity to catch up within the 120 day period.

Requirement Time Periods

The time periods within all the Requirements are distinct and separate. The applicable entity in Requirement R1 has 120 calendar days to identify whether a BES interrupting device operation is a Misoperation. Once the applicable entity has identified a Misoperation, it has completed its performance under Requirement R1. Identified Misoperations without an identified cause become subject to Requirement R4 and any subsequent Requirements as necessary. Identified Misoperations with an identified cause become subject to Requirement R5 and any subsequent Requirements as necessary.

In Requirement R2, the applicable entity has 120 calendar days, based on the date of the BES interrupting device operation, to provide notification to the other Protection System owners that meet the circumstances in Parts 2.1 and 2.2. For the case of an applicable entity that was notified (R3), it has the later of 120 calendar days from the date of the BES interrupting device operation or 60 calendar days of notification to identify whether its Protection System components caused a Misoperation.

Once a Misoperation is identified in either Requirement R1 or R3, and the applicable entity did not identify the cause(s) of the Misoperation, the time period for performing at least one investigative action every two full calendar quarters begins. The time period(s) in Requirement R4 resets upon each period. When the applicable entity's investigative actions identify the cause of the identified Misoperation or the applicable entity declares that no cause was found, the applicable entity has completed its performance in Requirement R4.

The time period in Requirement R5 begins when the Misoperation cause is first identified. The applicable entity is allotted 60 calendar days to perform one of the two activities listed in Requirement R5 (e.g., CAP or declaration) to complete its performance under Requirement R5.

Requirement R6 time period is determined by the actions and the associated timetable to complete those actions identified in the CAP. The time periods contained in the CAP may change from time to time and the applicable entity is required to update the timetable when it changes.

Time periods provided in the Requirements are intended to provide a reasonable amount of time to perform each Requirement. Performing activities in the least amount of time facilitates prompt identification of Misoperations, notification to other Protection System owners, identification of the cause(s), correction of the cause(s), and that important information is retained that may be lost due to time.

Requirement R1

This Requirement initiates a review of each BES interrupting device operation to identify whether or not a Misoperation may have occurred. Since the BES interrupting device owner typically monitors and tracks device operations, the owner is the logical starting point for identifying Misoperations of Protection Systems for BES Elements. A review is required when (1) a BES interrupting device operates that is caused by a Protection System or by manual intervention in response to a Protection System failure to operate, (2) regardless of whether the owner owns all or part of the Protection System component(s), and (3) the owner identified its Protection System component(s) as causing the BES interrupting device operation or was caused by manual intervention in response to its Protection System failure to operate.

Since most Misoperations result in the operation of one or more BES interrupting devices, these operations initiate a review to identify any Misoperation. If an Element is manually isolated in response to a failure to operate, the manual isolation of the Element triggers a review for Misoperation.

> **Example R1a:** The failure of a loss of field relay on a generating unit where an operator takes action to isolate the unit.

Manual intervention may indicate a Misoperation has occurred, thus requiring the initiation of an investigation by the BES interrupting device owner.

For the case where a BES interrupting device did not operate and remote clearing occurs due to the failure of a Composite Protection System to operate, the BES interrupting device owner would still review the operation under Requirement R1. However, if the BES interrupting device owner determines that its Protection System component operated as backup protection for a condition on another entity's BES Element, the owner would provide notification of the operation to the other Protection System owner(s) under Requirement R2, Part 2.2.

Protection Systems are made of many components. These components may be owned by different entities. 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 of the owners will communicate with each other, sharing information freely, so that Protection System operations can be analyzed, Misoperations identified, and corrective actions taken.

Each entity is expected to use judgment to identify those Protection System operations that meet the definition of Misoperation regardless of the level of ownership. A combination of available information from resources such as counters, relay targets, Supervisory Control and Data Acquisition (SCADA) systems, or DME would typically be used to determine whether or not a Misoperation occurred. The intent of the standard is to classify an operation as a Misoperation if the available information leads to that conclusion. In many cases, it will not be necessary to leverage all available data to determine whether or not a Misoperation occurred. The standard also allows an entity to classify an operation as a Misoperation if entity is not sure. The entity may decide to identify the operation as a Misoperation to satisfy Requirement R1 and continue its investigation for a cause of the Misoperation under Requirement R4. If the continued investigative actions are inconclusive, the entity may declare no cause found and end its investigation. The entity is allotted 120 calendar days from the date of its BES interrupting device operation to identify whether its Protection System component(s) caused a Misoperation.

The Protection System operation may be documented in a variety of ways such as in a report, database, spreadsheet, or list. The documentation may be organized in a variety of ways such as by BES interrupting device, protected Element, or Composite Protection System.

Repeated operations which occur during the same automatic reclosing sequence do not need a separate identification under Requirement R1. Repeated Misoperations which occur during the same 24-hour period do not need a separate identification under Requirement R1. This is consistent with the NERC *Misoperations Report*[7] which states:

> "In order to avoid skewing the data with these repeated events, the NERC SPCS should clarify, in the next annual update of the misoperation template, that all misoperations due to the same equipment and cause within a 24 hour period be recorded as one misoperation."

The following is an example of a condition that is not a Misoperation.

> **Example R1b:** A high impedance Fault occurs within a transformer. The sudden pressure relaying detects and operates for the Fault, but the differential relaying did not operate due to the low Fault current levels. This is not a Misoperation because the Composite Protection System was not required to operate because the Fault was cleared by the sudden pressure relay.

Requirement R2

Requirement R2 ensures notification of those who have a role in identifying Misoperations, but were not accounted for within Requirement R1. In the case of multi-entity ownership, the entity that owns the BES interrupting device that operated is expected to use judgment to identify those Protection System operations that meet the definition of Misoperation under Requirement R1; however, if the entity that owns a BES interrupting device determines that its Protection System component(s) did not cause the BES interrupting device(s) operation or cannot determine whether its Protection System components caused the BES interrupting device(s) operation, it must notify the other Protection System owner(s) that share Misoperation identification responsibility when the criteria in Requirement R2 is met.

This Requirement does not preclude the Protection System owners from initially communicating and working together to determine whether a Misoperation occurred and, if so, the cause. The BES interrupting device owner is only required to officially notify the other owners when it: (1) shares the Composite Protection System ownership with other entity(ies), (2) determines that a Misoperation occurred or cannot rule out a Misoperation, and (3) determines its Protection System component(s) did not cause a Misoperation or is unsure. Officially notifying the other owners without performing a preliminary review may unnecessarily burden the other owners with compliance obligations under Requirement R3, redirect valuable resources, and add little benefit to reliability. The BES interrupting device owner should officially notify other owners when appropriate within the established time period.

[7] "Misoperations Report." Reporting Multiple Occurrences. NERC Protection System Misoperations Task Force. http://www.nerc.com/docs/pc/psmtf/PSMTF_Report.pdf. April 1, 2013. pg. 37 of 40.

The following is an example of a notification to another Protection System owner:

> **Example R2a:** Circuit breakers A and B at the Charlie station tripped from directional comparison blocking (DCB) relaying on 03/03/2014 at 15:43 UTC during an external Fault. As discussed last week, the fault records indicate that a problem with your equipment (failure to transmit) caused the operation.
>
> **Example R2b:** A generator unit tripped out immediately upon synchronizing to the grid due to a Misoperation of its overcurrent protection. The Transmission Owner owns the 230 kV generator breaker that operated. The Transmission Owner, as the owner of the BES interrupting device after determining that its Protection System components did not cause the Misoperation, notified the Generator Owner of the operation. The Generator Owner investigated and determined that its Protection System components caused the Misoperation. In this example, the Generator Owner's Protection System components did cause the Misoperation. As the owner of the Protection System components that caused the Misoperation, the Generator Owner is responsible for creating and implementing the CAP.

A Composite Protection System owned by different functional entities within the same registered entity does not necessarily satisfy the notification criteria in Part 2.1.1 of Requirement R2. For example, if the same personnel within a registered entity perform the Misoperation identification for both the Generator Owner and Transmission Owner functions, then the Misoperation identification would be completely covered in Requirement R1, and therefore notification would not be required. However, if the Misoperation identification is handled by different groups, then notification would be required because the Misoperation identification would not necessarily be covered in Requirement R1.

> **Example R2c:** Line A Composite Protection System (owned by entity 1) failed to operate for an internal Fault. As a result, the zone 3 portion of Line B's Composite Protection System (owned by entity 2) and zone 3 portion of Line C's Composite Protection System (owned by entity 3) operated to clear the Fault. Entity 2 and 3 notified entity 1 of the remote zone 3 operation.

For the case where a BES interrupting device operates to provide backup protection for a non-BES Element, the entity reviewing the operation is not required to notify the other owners of Protection Systems for non-BES Elements. No notification is required because this Reliability Standard is not applicable to Protection Systems for non-BES Elements.

Requirement R3

For Requirement R3 (i.e., notification received), the entity that also owns a portion of the Composite Protection System is expected to use judgment to identify whether the Protection System operation is a Misoperation. A combination of available information from resources such as counters, relay targets, SCADA, DME, and information from the other owner(s) would typically be used to determine whether or not a Misoperation occurred. The intent of the standard is to classify an operation as a Misoperation if the available information leads to that conclusion. In many cases, it will not be necessary to leverage all available data to determine whether or not a Misoperation occurred. The standard also allows an entity to classify an operation as a Misoperation if an entity is not sure. The entity may decide to identify the operation as a

Misoperation to satisfy Requirement R1 and continue its investigation for a cause of the Misoperation under Requirement R4. If the continued investigative actions are inconclusive, the entity may declare no cause found and end its investigation.

The entity that is notified by the BES interrupting device owner is allotted the later of 60 calendar days from receipt of notification or 120 calendar days from the BES interrupting device operation date to determine if its portion of the Composite Protection System caused the Protection System operation. It is expected that in most cases of a jointly owned Protection System, the entity making notification would have been in communication with the other owner(s) early in the process. This means that the shorter 60 calendar days only comes into play if the notification occurs in the second half of the 120 calendar days allotted to the BES interrupting device owner in Requirement R1.

The Protection System review may be organized in a variety of ways such as in a report, database, spreadsheet, or list. The documentation may be organized in a variety of ways such as by BES interrupting device, protected Element, or Composite Protection System. The BES interrupting device owner's notification received may be documented in a variety of ways such as an email or a facsimile.

Requirement R4

The entity in Requirement R4 (i.e., cause identification), whether it is the entity that owns the BES interrupting device or an entity that was notified, is expected to use due diligence in taking investigative action(s) to determine the cause(s) of an identified Misoperation for its portion of the Composite Protection System. The SMEs developing this standard recognize there will be cases where the cause(s) of a Misoperation will not be revealed during the allotted time periods in Requirements R1 or R3; therefore, Requirement R4 provides the entity a mechanism to continue its investigative work to determine the cause(s) of the Misoperation when the cause is not known.

A combination of available information from resources such as counters, relay targets, SCADA, DME, test results, and studies would typically be used to determine the cause of the Misoperation. At least one investigative action must be performed every two full calendar quarters until the investigation is completed.

The following is an example of investigative actions taken to determine the cause of an identified Misoperation:

> **Example R4a**: A Misoperation was identified on 03/18/2014. A line outage to test the Protection System was scheduled on 03/24/2014 for 12/15/2014 as the first investigative action (i.e., beyond the next two full calendar quarters) due to summer peak conditions. The protection engineer contacted the manufacturer on 04/10/2014 (i.e., within two full calendar quarters) to obtain any known issues. The engineer reviewed manufacturer's documents on 05/27/2014. The outage schedule was confirmed on 08/29/2014 and was taken on 12/15/2014. Testing was completed on 12/16/2014 (i.e., in the second two full quarters) revealing the microprocessor relay as the cause of the Misoperation. A CAP is being developed to replace the relay.

Periodic action minimizes compliance burdens and focuses the entity's effort on determining the cause(s) of the Misoperation while providing measurable evidence. The SMEs recognize that

certain planned investigative actions may require months or years to schedule and complete; therefore, the entity is only required to perform at least one investigative action every two full calendar quarters. If an investigative action is performed in the first quarter of a calendar year, the next investigative action would need to be performed by the end of the third calendar quarter. If an investigative action is performed in the last quarter of a calendar year, the next investigative action would need to be performed by the end of the second calendar quarter of the following calendar year. Investigative actions may include a variety of actions, such as reviewing DME records, performing or reviewing studies, completing relay calibration or testing, requesting manufacturer review, requesting an outage, or confirming a schedule.

The entity's investigation is complete when it identifies the cause of the Misoperation or makes a declaration that no cause was determined. The declaration is intended to be used if the entity determines that investigative actions have been exhausted or have not provided direction for identifying the Misoperation cause. Historically, approximately 12% of Misoperations are unknown or unexplainable.[8]

Although the entity only has to document its specific investigative actions taken to determine the cause(s) of an identified Misoperation, the entity should consider the benefits of formally organizing (e.g., in a report or database) its actions and findings. Well documented investigative actions and findings may be helpful in future investigations of a similar event or circumstances. A thorough report or database may contain a detailed description of the event, information gathered, investigative actions, findings, possible causes, identified causes, and conclusions. Multiple owners of a Composite Protection System might consider working together to produce a common report for their mutual benefit.

The following are examples of a declaration where no cause was determined:

> **Example R4b**: A Misoperation was identified on 04/11/2014. All relays at station A and B functioned properly during testing on 08/26/2014 as the first investigative action. The carrier system functioned properly during testing on 08/27/2014. The carrier coupling equipment functioned properly during testing on 08/28/2014. A settings review completed on 09/03/2014 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 correct, and the equipment at station A and station B is already monitored. The investigation is being closed because no cause was found.
>
> **Example R4c:** A Misoperation was identified on 03/22/2014. The protection scheme was replaced before the cause was identified. The power line carrier or PLC based protection was replaced with fiber-optic based protection with an in-service date of 04/16/2014. The new system will be monitored for recurrence of the Misoperation.

Requirement R5

Resolving the causes of Protection System Misoperations benefits BES reliability by preventing recurrence. The Corrective Action Plan (CAP) is an established tool for resolving operational problems. The NERC Glossary defines a Corrective Action Plan as, *"A list of actions and an*

[8] NERC System Protection and Control Subcommittee. Misoperations Report. April 1, 2013: http://www.nerc.com/docs/pc/psmtf/PSMTF_Report.pdf. Figure 15: NERC Wide Misoperations by Cause Code. pg. 22 of 40.

associated timetable for implementation to remedy a specific problem." Since a CAP addresses specific problems, the determination of what went wrong needs to be completed before developing a CAP. When the Misoperation cause is identified in Requirement R1, R3 or R4, Requirement R5 requires Protection System owner(s) to develop a CAP, or explain why corrective actions are beyond the entity's control or would not improve BES reliability. The entity must develop the CAP or make a declaration why additional actions are beyond the entity's control or would not improve BES reliability and that no further corrective actions will be taken within 60 calendar days of first determining a cause.

The SMEs developing this standard recognize there may be multiple causes for a Misoperation. In these circumstances, the CAP would include a remedy for the identified causes. The CAP may be revised if additional causes are found; therefore, the entity has the option to create a single or multiple CAP(s) to correct multiple causes of a Misoperation. The 60 calendar day period for developing a CAP (or declaration) is established on the basis of industry experience which includes operational coordination timeframes, time to consider alternative solutions, coordination of resources, and development of a schedule.

The development of a CAP is intended to document the specific corrective actions needed to be taken to prevent Misoperation recurrence, the timetable for executing such actions, and an evaluation of the CAP's applicability to the entity's other Protection Systems including other locations. The evaluation of these other Protection Systems aims to reduce the risk and likelihood of similar Misoperations in other Protection Systems. The Protection System owner is responsible for determining the extent of its evaluation concerning other Protection Systems and locations. The evaluation may result in the owner including actions to address Protection Systems at other locations or the reasoning for not taking any action. The CAP and an evaluation of other Protection Systems including other locations must be developed to complete Requirement R5.

The following is an example of a CAP for a relay Misoperation that was applying a standing trip due to a failed capacitor within the relay and the evaluation of the cause at similar locations which determined capacitor replacement was not necessary.

For completion of each CAP in Examples R5a through R5d, please see Examples R6a through R6d.

> **Example R5a:** Actions: Remove the relay from service. Replace capacitor in the relay. Test the relay. Return to service or replace by 07/01/2014.
>
> Applicability to other Protection Systems: This type of impedance relay has not been experiencing problems and is systematically being replaced with microprocessor relays as Protection Systems are modernized. Therefore, it was assessed that a program for wholesale preemptive replacement of capacitors in this type of impedance relay does not need to be established for the system.

The following is an example of a CAP for a relay Misoperation that was applying a standing trip due to a failed capacitor within the relay and the evaluation of the cause at similar locations which determined the capacitors need preemptive correction action.

> **Example R5b:** Actions: Remove the relay from service. Replace capacitor in the relay. Test the relay. Return to service or replace by 07/01/2014.
>
> Applicability to other Protection Systems: This type of impedance relay is suspected to have previously tripped at other locations because of the same type of capacitor issue. Based on the evaluation, a program should be established by 12/01/2014 for wholesale preemptive replacement of capacitors in this type of impedance relay.

The following is an example of a CAP for a relay Misoperation that was applying a standing trip due to a failed capacitor within the relay and the evaluation of the cause at similar locations which determined the capacitors need preemptive correction action.

> **Example R5c:** Actions: Remove the relay from service. Replace capacitor in the relay. Test the relay. Return to service or replace by 07/01/2014.
>
> Applicability to other Protection Systems: This type of impedance relay is suspected to have previously tripped at other locations because of the same type of capacitor issue. Based on the evaluation, the preemptive replacement of capacitors in this type of impedance relay should be pursued for the identified stations A through I by 04/30/2015.
>
> A plan is being developed to replace the impedance relay capacitors at stations A, B, and C by 09/01/2014. A second plan is being developed to replace the impedance relay capacitors at stations D, E, and F by 11/01/2014. The last plan will replace the impedance relay capacitors at stations G, H, and I by 02/01/2015.

The following is an example of a CAP for a relay Misoperation that was due to a version 2 firmware problem and the evaluation of the cause at similar locations which determined the firmware needs preemptive correction action.

> **Example R5d:** Actions: Provide the manufacturer fault records. Install new firmware pending manufacturer results by 10/01/2014.
>
> Applicability to other Protection Systems: Based on the evaluation of other locations and a risk assessment, the newer firmware version 3 should be installed at all installations that are identified to be version 2. Twelve relays were identified across the system. Proposed completion date is 12/31/2014.

The following are examples of a declaration made where corrective actions are beyond the entity's control or would not improve BES reliability and that no further corrective actions will be taken.

> **Example R5e:** The cause of the Misoperation was due to a non-registered entity communications provider problem.
>
> **Example R5f:** The cause of the Misoperation was due to a transmission transformer tapped industrial customer who initiated a direct transfer trip to a registered entity's transmission breaker.

In 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 following are examples of declarations made why corrective actions would not improve BES reliability.

> **Example R5g:** The investigation showed that the Misoperation occurred due to transients associated with energizing transformer ABC at Station Y. 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.
>
> **Example R5h:** As a result of an operation that left a portion of the power system in an electrical island condition, circuit XYZ within that island tripped, resulting in loss of load within the island. Subsequent investigation showed an overfrequency condition persisted after the formation of that island and the XYZ line protective relay operated. Since this relay was operating outside of its designed frequency range and would not be subject to this condition when line XYZ is operated normally connected to the BES, no corrective action will be taken because BES reliability would not be improved.
>
> **Example R5i:** During a major ice storm, four of six circuits were lost at Station A. Subsequent to the loss of these circuits, a skywire (i.e., shield wire) broke near station A on line AB (between Station A and B) resulting in a phase-phase Fault. The protection scheme utilized for both protection groups is a permissive overreaching transfer trip (POTT). The Line AB protection at Station B tripped timed for this event (i.e., Slow Trip – During Fault) even though this line had been identified as requiring high speed clearing. A weak infeed condition was created at Station A due to the loss of 4 transmission circuits resulting in the absence of a permissive signal on Line AB from Station A during this Fault. No corrective action will be taken for this Misoperation as even under N-1 conditions, there is normally enough infeed at Station A to send a proper permissive signal to station B. Any changes to the protection scheme to account for this would not improve BES reliability.

A declaration why corrective actions are beyond the entity's control or would not improve BES reliability should include the Misoperation cause and the justification for taking no corrective action. Furthermore, a declaration that no further corrective actions will be taken is expected to be used sparingly.

Requirement R6

To achieve the stated purpose of this standard, which is to identify and correct the causes of Misoperations of Protection Systems for BES Elements, the responsible entity is required to implement a CAP that addresses the specific problem (i.e., cause(s) of the Misoperation) through completion. Protection System owners are required in the implementation of a CAP to update it when actions or timetable change, until completed. Accomplishing this objective is intended to reduce the occurrence of future Misoperations of a similar nature, thereby improving reliability and minimizing risk to the BES.

The following is an example of a completed CAP for a relay Misoperation that was applying a standing trip (See also, Example R5a).

> **Example R6a:** Actions: The impedance relay was removed from service on 06/02/2014 because it was applying a standing trip. A failed capacitor was found within the impedance relay and replaced. The impedance relay functioned properly during testing after the capacitor was replaced. The impedance relay was returned to service on 06/05/2014.
>
> CAP completed on 06/25/2014.

The following is an example of a completed CAP for a relay Misoperation that was applying a standing trip that resulted in the correction and the establishment of a program for further replacements (See also, Example R5b).

> **Example R6b:** Actions: The impedance relay was removed from service on 06/02/2014 because it was applying a standing trip. A failed capacitor was found within the impedance relay and replaced. The impedance relay functioned properly during testing after the capacitor was replaced. The impedance relay was returned to service on 06/05/2014.
>
> A program for wholesale preemptive replacement of capacitors in this type of impedance relay was established on 10/28/2014.
>
> CAP completed on 10/28/2014.

The following is an example of a completed CAP of corrective actions with a timetable that required updating for a failed relay and preemptive actions for similar installations (See also, Example R5c).

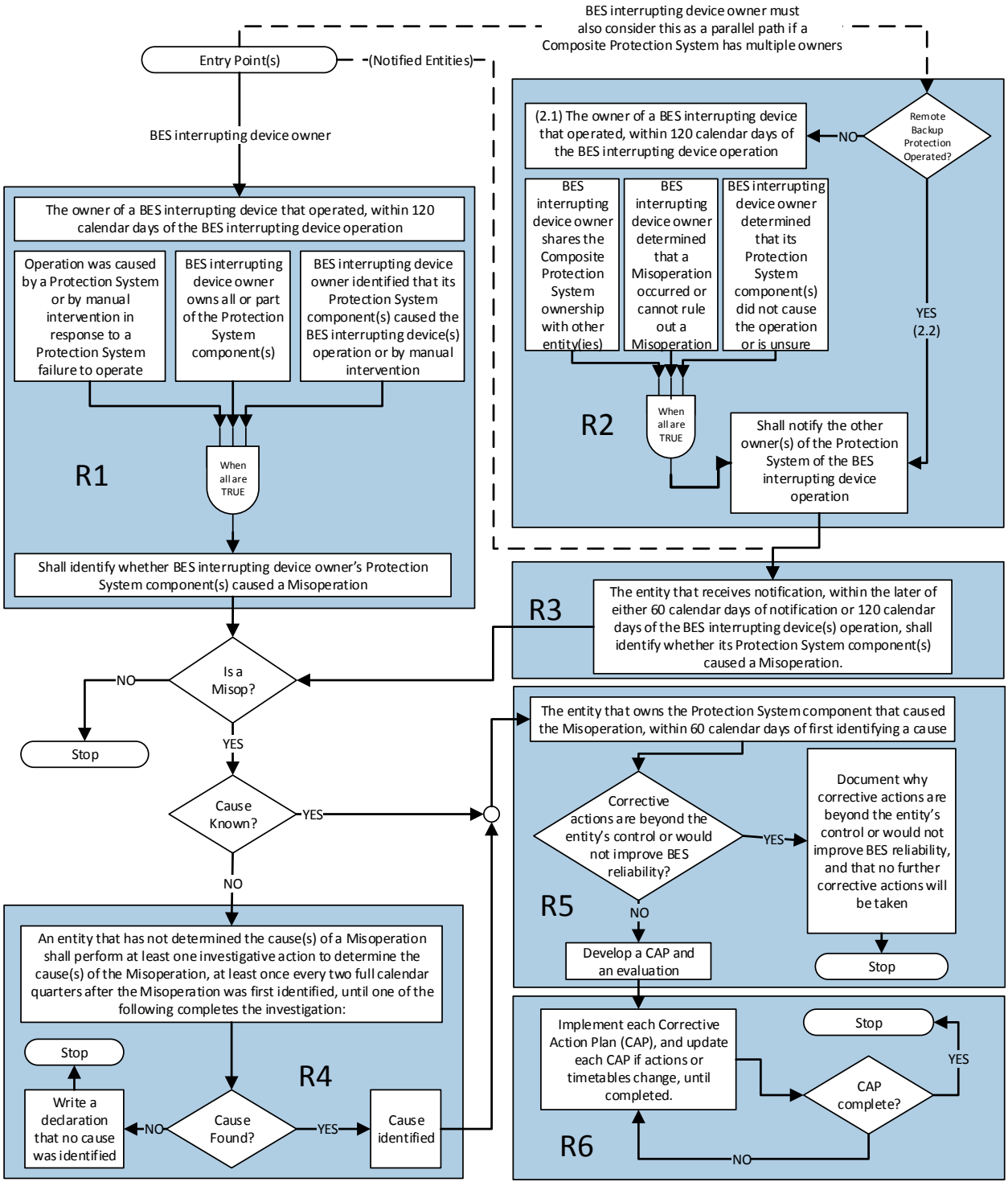
> **Example R6c:** Actions: The impedance relay was removed from service on 06/02/2014 because it was applying a standing trip. A failed capacitor was found within the impedance relay and replaced. The impedance relay functioned properly during testing after the capacitor was replaced. The impedance relay was returned to service on 06/05/2014.
>
> The impedance relay capacitor replacement was completed at stations A, B, and C on 08/16/2014. The impedance relay capacitor replacement was completed at stations D, E, and F on 10/24/2014. The impedance relay capacitor replacement for stations G, H, and I were postponed due to resource rescheduling from a scheduled 02/01/15 completion to 04/01/2015 completion. Capacitor replacement was completed on 03/09/2015 at stations G, H, and I. All stations identified in the evaluation have been completed.
>
> CAP completed on 03/09/2015.

The following is an example of a completed CAP for corrective actions with updated actions for a firmware problem and preemptive actions for similar installations. (See also, Example R5d).

> **Example R6d:** Actions: fault records were provided to the manufacturer on 06/04/2014. 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 08/12/2014.
>
> Nine of the twelve relays were updated to version 3 firmware on 09/23/2014. The manufacturer provided a subsequent update which was determined to be beneficial for the remaining relays. The remaining three of twelve relays identified as having the version 2 firmware were updated to version 3.01 firmware on 11/10/2014.
>
> CAP completed on 11/10/2014.

The CAP is complete when all of the actions identified within the CAP have been completed.

Process Flow Chart: Below is a graphical representation demonstrating the relationships between Requirements:



Rationale:

During development of this standard, text boxes were embedded within the standard to explain the rationale for various parts of the standard. Upon BOT approval, the text from the rationale text boxes was moved to this section.

Rationale for Introduction:
The only revisions made to this version of PRC-004 are revisions to section 4.2 Facilities to clarify applicability of the Requirements of the standard to generator Facilities. These applicability revisions are intended to clarify and provide for consistent application of the Requirements to BES generator Facilities included in the BES through Inclusion I4 – Dispersed Power Producing Resources.

Rationale for Applicability:
Protection Systems that protect BES Elements are integral to the operation and reliability of the BES. Some functions of relays are not used as protection but as control functions or for automation; therefore, any operation of the control function portion or the automation portion of relays is excluded from this standard. See the Application Guidelines for detailed examples of non-protective functions. Special Protection Systems (SPS) and Remedial Action Schemes (RAS) are excluded in this standard because they are planned to be handled in the second phase of Project 2010-05.1 .

Misoperations occurring on the Protection Systems of individual generation resources identified under Inclusion I4 of the BES definition do not have a material impact on BES reliability when considered individually; however, the aggregate capability of these resources may impact BES reliability if a number of Protection Systems on the individual power producing resources incorrectly operated or failed to operate as designed during a system event. To recognize the potential for the Protection Systems of individual power producing resources to affect the reliability of the BES, 4.2.1.5 of the Facilities section reflects the threshold consistent with the revised BES definition. See FERC Order Approving Revised Definition, P 20, Docket No. RD14-2-000. The intent of 4.2.1.5 of the Facilities section is to exclude from the standard requirements these Protection Systems for “common- mode failure” type scenarios affecting less than or equal to 75 MVA aggregated nameplate generating capability at these dispersed generating facilities.

Rationale for R1:

This Requirement ensures that entities review those Protection System operations meeting the circumstances in all three Parts (1.1, 1.2, and 1.3) and identify any that are Misoperations. The BES interrupting device owner is assigned the responsibility to initiate the review because the owner is in the best position to be aware of the operation. Manual intervention is included as a condition that initiates a review. Occasionally, Protection System failures do not yield other Protection System operations and manual intervention is required to isolate the problematic equipment. The 120 calendar day period accounts for the sporadic volumes of Protection

System operations, and provides the opportunity to identify any Misoperations which were initially missed.

Rationale for R2:

Part 2.1 ensures that the BES interrupting device owner notifies the other owners of the Composite Protection System. The phrase “owner(s) that share Misoperation identification responsibility” allows entities to notify the specific other owners that will actually review the operation to determine if a Misoperation occurred. Part 2.2 ensures that the Protection System owner(s) for which backup protection was provided receives notification, within the same 120 calendar day period as R1. This ensures other entities are notified to review their Protection System components. The expectation is that entities will communicate accordingly and when it is clear that Part 2.1, 2.2, or both are met, the entity would make the notification. It is not intended for entities to automatically and unnecessarily notify other entities before adequate detail is known.

Rationale for R3:

When an entity receives notification of a Protection System operation by the BES interrupting device owner, the other Protection System owner is allotted at least 60 calendar days to identify whether it was a Misoperation. A shorter time period is allotted on the basis that the BES interrupting device owner has already performed preliminary work, collaborated with the other owners, and that other owners generally have fewer associated Protection System components.