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 SC authorized moving the SAR forward for standard development at their June 9, 2011 meeting.
2. The SAR was posted for informal comment June 10 – July 11, 2011.
3. Draft 1 of PRC-004-3 was posted for a 30-day formal comment period from June 10 – July 11, 2011.
4. Draft 2 of PRC-004-3 was posted for a 45-day formal comment period from July 25 – September 7, 2012 and an initial ballot in the last ten days of the comment period from August 29 – September 7, 2012.
5. Draft 3 of PRC-004-3 was posted for a 30-day formal comment period from January 22 – February 20, 2013 and a successive ballot in the last ten days of the comment period from February 11-20, 2013.

Description of Current Draft

The Protection System Misoperations Standard Drafting Team (PSMSDT) is posting Draft 4 of PRC-004-3 – Protection System Misoperation Identification and Correction for a 45-day comment period and ballot in the last ten days of the comment period under the new Standards Process Manual (Effective: June 26, 2013).

Anticipated Actions	Anticipated Date
Additional 45-day Formal Comment Period with Parallel Ballot	January 2014
10-day Final Ballot	March 2014
BOT Approval	May 2014

Effective Dates

Except in the Western Interconnection, the standard and definitions shall become effective on the first day of the first calendar quarter that is twelve months after the date that the standard is approved by an applicable governmental authority or as otherwise provided for in a jurisdiction where approval by an applicable governmental authority is required for a standard to go into effect. Except in the Western Interconnection, where approval by an applicable governmental authority is not required, the standard and definitions shall become effective on the first day of the first calendar quarter that is twelve months after the date the standard is adopted by the NERC Board of Trustees or as otherwise provided for in that jurisdiction.

In the Western Interconnection, the standard and definitions shall become effective on the first day of the first calendar quarter that is twenty-four months after the date that the standard is approved by an applicable governmental authority or as otherwise provided for in a jurisdiction where approval by an applicable governmental authority is required for a standard to go into effect. In the Western Interconnection, where approval by an applicable governmental authority is not required, the standard and definitions shall become effective on the first day of the first calendar quarter that is twenty-four months after the date the standard is adopted by the NERC Board of Trustees or as otherwise provided for in that jurisdiction.

Version History

Version	Date	Action	Change Tracking
1	TBD	Project 2010-05.1 – Protection Systems: Phase 1 (Misoperations)	New

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 *Glossary of Terms used in NERC Reliability Standards* 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.

Composite Protection System:

The total complement of the Protection System(s) that function collectively to protect an Element, such as any primary, secondary, local backup, and communication-assisted relay systems. Backup protection provided by a remote Protection System is excluded.

Misoperation:

The failure of a Composite Protection System to operate as intended. 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 for which it is designed. Delayed clearing of a Fault condition is a Misoperation if high-speed performance was previously identified as being necessary to prevent voltage or dynamic instability, or resulted in the operation of any other Composite Protection System.
4. **Slow Trip – Other Than Fault** – A Composite Protection System operation that is slower than required for a non-Fault condition for which it is designed, such as a power swing, undervoltage, overexcitation, or loss of excitation. Delayed clearing of a non-Fault condition is a Misoperation if high-speed performance was previously identified as being necessary to prevent voltage or dynamic instability, or resulted in the operation of any other Composite Protection System.
5. **Unnecessary Trip – During Fault** – An unnecessary Protection System operation for a Fault condition on another Element.
6. **Unnecessary Trip – Other Than Fault** – An unnecessary Protection System operation for a non-Fault condition for which it is not designed. A Protection System operation that is caused by on-site maintenance, testing, inspection, construction, or commissioning activities is not a Misoperation.

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 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. Non-protective functions that are embedded within a Protection System are excluded. Protective functions intended to operate as a control function during switching are excluded.[1]

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

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 not included in this standard because they are planned to be handled in the second phase of this project.

5. **Background**:

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

The SAR for this project also includes clarifying reporting requirements. Misoperation data, as currently collected and reported, is not 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 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.

6. **Effective Dates:** See Implementation Plan

B. Requirements and Measures

R1. 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, identify whether its Protection System component(s) caused a Misoperation when: *[Violation Risk Factor: Medium][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.

M1. 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.

Rationale for R1: This requirement ensures that entities review those Protection System operations meeting the criteria in all three Parts (1.1, 1.2, and 1.3) and identify any that are Misoperations. The BES interrupting device owner has 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.

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, notify the other owner(s) of the Protection System of the operation when: *[Violation Risk Factor: Medium][Time Horizon: Operations Assessment, Operations Planning]*

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

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

2.3 The BES interrupting device owner 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.

M2. Acceptable evidence for Requirement R2, including Parts 2.1, 2.2, and 2.3 may include, but is not limited to, the following dated documentation (electronic or hardcopy format): emails, facsimiles, or transmittals.

Rationale for R2: This requirement ensures that the BES interrupting device owner notifies the other owners of the Composite Protection System when the criteria in all three Parts (2.1, 2.2, and 2.3) are met, 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 the three conditions 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.

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

M3. 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, Disturbance Monitoring Equipment (DME) records, test results, or transmittals.

Rationale for R3: When an entity receives notification of a Protection System operation by the BES interrupting device owner, the 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.

R4. Each Transmission Owner, Generator Owner, and Distribution Provider that has not determined the cause(s) of a Misoperation identified in accordance with Requirement R1 or R3 shall perform investigative action(s) to determine the cause 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: Medium] [Time Horizon: Operations Assessment, Operations Planning]*

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

M4. 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, Disturbance Monitoring Equipment (DME) records, test results, or transmittals.

Rationale for R4: If a Misoperation cause is not identified within the time period established by Requirements R1 or R3 (120 calendar days), the Protection System component owner must demonstrate investigative actions toward identifying the cause(s). Performing at least one action every two full calendar quarters from first identifying the Misoperation encourages periodic focus on finding the cause of the Misoperation.

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: Medium*] [*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. Acceptable evidence for Requirement R5 may include, but is not limited to, the following documentation (electronic or hardcopy format): a dated CAP or a dated declaration.

Rationale for R5: A formal CAP is a proven tool for resolving and reducing the possibility of reoccurrence of operational problems. A time period of 60 calendar days is based on industry experience and operational coordination time needed for considering such things as alternative solutions, coordination of resources, or development of a schedule. When the cause of a Misoperation is identified, a CAP will generally be developed. In rare cases, altering the Protection System to avoid a Misoperation recurrence may lower the reliability or performance of the BES. In those cases, a statement documenting the reasons for taking no corrective actions is essential for justifying the close of the Misoperation in lieu of a CAP and for future reference.

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: Medium][Time Horizon: Operations Planning, Long-Term Planning]*

M6. Acceptable evidence for Requirement R6 may include, but is not limited to, the following documentation (electronic or hard copy format): dated records that document the implementation of each CAP and the completion of actions for each CAP. Evidence may also include work management program records, work orders, and maintenance records.

Rationale for R6: The CAP must accomplish all identified objectives to be complete. During the course of implementing a CAP, updates may be necessary for a variety of reasons such as new information, scheduling conflicts, or resource issues. Documenting changes or completion of CAP activities provides measurable progress and confirmation of completion.

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 12 calendar months.
- The Transmission Owner, Generator Owner, and Distribution Provider shall retain evidence of Requirement R5, Measure M5 for 12 calendar months following completion of each CAP, evaluation, and declaration.
- The Transmission Owner, Generator Owner, and Distribution Provider shall retain evidence of Requirement R6, Measure M6 for 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

Periodic Data Submittal

1.4. Additional Compliance Information

None.

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 identified whether or not 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 or not 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 or not 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 or not 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 or not 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	Medium	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	Medium	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 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	Medium	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	Medium	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 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 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	Medium	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.

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

Introduction

This standard addresses the reliability issues identified in the letter[2] 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[3]; 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.”

Definitions

The Misoperation definition is based on the IEEE/PSRC Working Group I3 “Transmission Protective Relay System Performance Measuring Methodology[4].” 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.

[2] http://www.nerc.com/pa/Stand/Project%20201005%20Protection%20System%20Misoperations%20DL/20110209130708-Cauley%20letter.pdf
[3] http://www.nerc.com/files/2011_RARPR_FINAL.pdf
[4] “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 the Protection System(s) that function collectively to protect a Element, such as any primary, secondary, local backup, and communication-assisted relay systems. Backup protection provided by a remote Protection System is excluded.*

This definition has been introduced in this standard and incorporated into the proposed definition of Misoperation to clarify that the entity must consider the entire Protection System associated with the BES interrupting device that operated. Additionally, the definition accounts for those Protection Systems with multiple levels of protection (e.g., redundant systems), such that if one component fails, but the overall intended performance of the composite protection is met – it would not be identified as a Misoperation under the definition.

> **Misoperation –** *The failure a Composite Protection System to operate as intended. 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 for which it is designed. Delayed clearing of a Fault condition is a Misoperation if high-speed performance was previously identified as being necessary to prevent voltage or dynamic instability, or resulted in the operation of any other Composite Protection System.*
4. ***Slow Trip – Other Than Fault*** *– A Composite Protection System operation that is slower than required for a non-Fault condition for which it is designed, such as a power swing, undervoltage, overexcitation, or loss of excitation. Delayed clearing of a non-Fault condition is a Misoperation if high-speed performance was previously identified as being necessary to prevent voltage or dynamic instability, or resulted in the operation of any other Composite Protection System.*
5. ***Unnecessary Trip – During Fault*** *– An unnecessary Protection System operation for a Fault condition on another Element.*
6. ***Unnecessary Trip – Other Than Fault*** *– An unnecessary Protection System operation for a non-Fault condition for which it is not designed. A Protection System operation that is caused by on-site maintenance, testing, inspection, construction or commissioning activities is not a Misoperation.*

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.

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. The definition includes six categories which provide further differentiation and examples of what is 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 Misoperation as long as another component of the transformer's Composite Protection System operated to clear the Fault.
>
> **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 would not in and of itself be a Misoperation.

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 another component of the generator's Composite Protection System operated as intended (e.g., isolating the generator).

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 3:** A failure of a line's Composite Protection System to operate as quickly as intended for a line Fault is a Misoperation.

Installing high-speed protection may be a part of a utility’s standard practice without having the need for high-speed protection to prevent voltage or dynamic instability or to maintain relay coordination. For this case, a “Slow Trip – During Fault” of the high-speed protection is not a Misoperation because it would not negatively impact the dynamic BES performance, unless the Composite Protection System operation is slower than previously identified as being necessary to prevent voltage or dynamic instability. The Composite Protection System must also coordinate with other Protection Systems to prevent the trip (e.g., an over-trip) of additional Protection Systems.

The phrase “slower than required” means the Composite Protection System operated slower than the objective of the owner(s). 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 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.

Slow Trip – Other Than Fault

The phrase “slower than required” means the Composite Protection System operated slower than the objective of the owner(s). 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 stability by the owner(s) reviewing each Protection System operation.

> **Example 4:** A failure of a generator's Composite Protection System to operate as quickly as intended for an overexcitation condition is a Misoperation. This category of Misoperation could result in equipment damage.

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.

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.

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 6d:** 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.

The “on-site” activities at one location that initiates a trip to another location are included in this exemption; however, once the maintenance, testing, inspection, construction, or commissioning 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 which occur with the protected Element out of service, 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.

The above are examples only, and do not constitute an all-inclusive list of conditions that would not be a Misoperation.

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 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 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.

In the example above, the standard is not applicable; however, the standard remains applicable to the reverse power relay as a part of the generator Protection System when intended to provide generator anti-motoring protection. For example, reverse power relays are typically installed as the primary protection for a generating unit to guard against motoring. Though, operators often take advantage of this functionality and use the Protection System's reverse power protective function as a normal procedure to shutdown a generating unit.

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, says: "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 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 that its Protection System component(s) as causing the BES interrupting device operation.

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.

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 Disturbance Monitoring Equipment (DME) would typically be used to determine whether or not a Misoperation occurred. The entity is allotted 120 calendar days from the date of its BES interrupting device operation to identify whether or not a Misoperation of its Protection System component(s) occurred.

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.

Requirement R2

For Requirement R2 (i.e., 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) 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, 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.

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 or 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.

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 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 latter half of the 120 calendar days allotted to the BES interrupting device owner.

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 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, the entity 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 (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 to schedule and complete; therefore, the entity is only required to perform at least one investigative action every two full calendar quarters. 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, or requesting a necessary outage.

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.

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**: All relays at station A and B functioned properly during testing on 08/26/2014. 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:** 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 or CAP is an established tool for resolving operational problems. The NERC Glossary defines a Corrective Action Plan as, *"A list of actions and an associated timetable for implementation to remedy a specific problem."* 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 create 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 CAPs 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 time periods within Requirement R1, R3 and Requirement R5 are distinct and separate. If a cause of a Misoperation is identified quickly, the time period in Requirement R1 or R3 ends and the 60 calendar day period to develop the CAP becomes applicable. The ultimate goal is to keep all time periods as short as possible, including the correction of the cause(s) of the Misoperation. Where there are multiple Protection System owners involved in a Misoperation, each owner whose Protection System component(s) contributed to the Misoperation is subject to Requirement R5.

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 must include an evaluation of other Protection Systems including other locations to be complete.

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

> **Example R5a:** Actions: Remove the relay from service. Replace capacitor. 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 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. 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 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. 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 in an example of a declaration 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 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. The 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. The 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. The 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 resource rescheduling from 02/01/15 to 03/01/2015. Following the timetable change, 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 the documented actions to resolve the specific problem (i.e., Misoperation) are completed which may include those actions resulting from the entity's evaluation of other locations, if not addressed through a separate CAP.

Process Flow Chart: Below is a graphical representation of the expected process created by the standard, including the relationships between requirements: