Get Control of Yourself!

Public

By Denise Hunter, Principal Technical Auditor

Can you believe how quickly this year has flown by? Before you know it, it will be time to attend the **RF Internal Controls Workshop**! (I bet you thought I was going to say Christmas.) Here is my shameless plug: the workshop is Wednesday, Feb. 12, 2020 in Cleveland, and you can register here. This truly will be a working session where your company's SME and PCC will work to capture your company-specific internal controls for two Standards, one O&P and one CIP. The O&P Standard will be PRC-004-5(i). Therefore, I will continue with that subject in this issue and address the ERO risk element **Improper Determination of Misoperations**.

In order to dive into this subject, we need to have a common understanding of the risk presented by this ERO risk element. This risk lies in a number of areas, and some ERO documents have identified a few:

1) According to the 2019 Compliance Monitoring and Enforcement Program Implementation Plan,[1] "When protection systems are not coordinated properly, the order of execution can result in either incorrect elements being removed from service or more elements being removed than necessary."

2) The 2018 ERO Reliability Risk Priorities report [2] identifies in its Risk Profile #4: Increasing Complexity in Protection and Control Systems, that improper coordination of control system assets could negatively affect the resiliency of the BES due to control system misoperations or failures.

3) Additionally, I would offer that we also must include the coordination of operations, as well as lack of appropriate internal controls, tools, data, services and personnel necessary, to ensure the reliability of the BES.

When you consider the number of moving parts that could initiate a misoperation, it is understandable (and not lost on RF) how challenging a task it might be to determine the true cause. Regardless and however daunting the process might be, a strong internal control can reduce improper determinations of misoperations.

Before beginning the process of identifying possible internal controls that might help reduce improper determinations, and a few controls that could possibly help mitigate the possibility of a misoperation, let us review some facts from a few events. Specifically, let us examine the Arizona-Southern California Outages [3] and the Aug. 14, 2003 Blackout [4]. Additionally, some information from the NERC 2013 and 2019 State of Reliability (SOR) reports and the 2018 RISC Recommendations to the NERC Board of Trustee's report could prove useful in this review.

Arizona-Southern California VS August 14, 2003 Blackout

The Arizona-Southern California Outages Sept. 8, 2011 report noted a number of common underlying causes between that outage and the Aug. 14, 2003 Blackout. First, "both reports described relevant planning studies that:

(1) did not adequately identify and study critical external facilities;

(2) did not adequately analyze potential contingency scenarios; and

(3) were based on inaccurate models and invalid system operating limits (SOLs)."

Second, "in both events, the affected entities' real-time monitoring tools were not adequate to alert operators to system conditions and contingencies. In addition, some of the affected entities in both events did not use their real-time tools to monitor system conditions. As a result of these situational awareness issues, affected entities in both events were not aware that they were no longer operating in a secure N-1 state and were not alerted to the need to take corrective actions."

NERC 2013 and 2019 State of Reliability Report(s)

Next, the NERC SOR 2013 [5] (reporting on 2012 activity) identified that the main causes for misoperations are from incorrect settings/logic/design errors, communication failure, and relay failure or malfunction. (See Figure 1.6.)

[1] 2019 CMEP IP, pg 20

[2] [See 2018 RISC Recommendations to the NERC BoT

[3] [See Arizona-Southern California Outages Sept 8, 2011

[4] See August 14, 2003 Blackout Final report

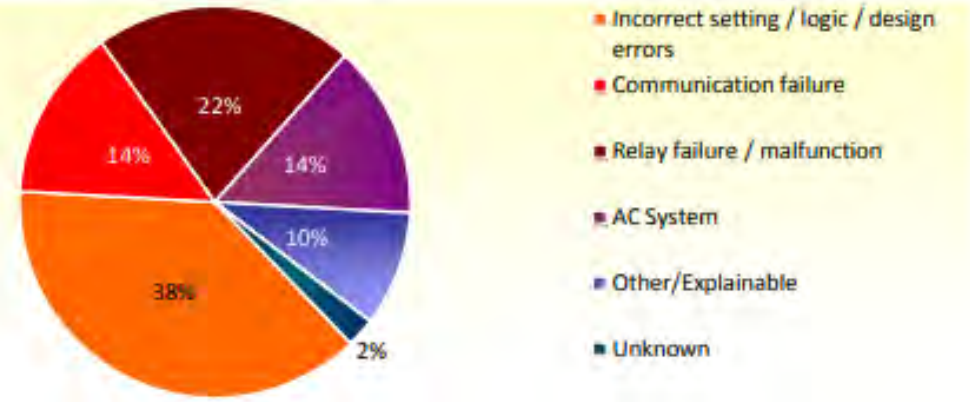
[5] NERC State of Reliability 2013

Continued on page 4

Get Control of Yourself!

Continued from page 3

Figure 1.6: Misoperations in 2012 Cause-Coded Disturbance Events (42 Misoperations within 33 Qualified Events)



The NERC SOR from 2019 [6] noted the same three largest causes of misoperations. (See Figure 5.5.)

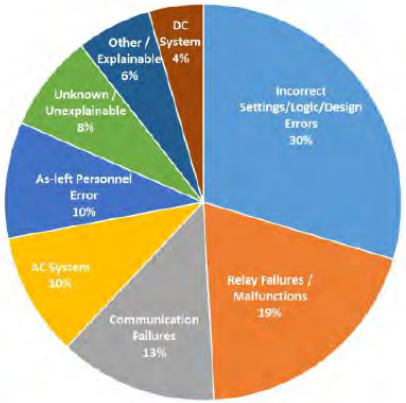


Figure 5.5: Misoperations by Cause Code (4Q 2013 through 3Q 2018)

Let us stop for a minute and look at those facts. How is it possible that issues identified in 2003 still prevailed eight years later? Moreover, how is it that the main causes for misoperations identified in 2012 remain the most common causes in 2018? Perhaps we need to look at these activities in a different light.

To recap, misoperations are sometimes due to protection systems being improperly coordinated; and the three main causes of misoperations have consistently been setting/logic/design errors, communication errors, and relay failures or malfunctions. We also learned that these problems have prevailed over the years. Based on that information, the next question begs "What exactly does proper coordination entail?" At the most basic, it is "the harmonious functioning of parts for effective results, the proper order or relationship, harmonious combination or interaction, as of function or parts." [7] Before dissecting what controls might help mitigate the risk of not being properly coordinated, let us review a few recommendations that were presented in the reports mentioned above.

Recommendations and Risk Based Compliance

Each of the reports noted in this article provided recommendations regarding misoperations and ideas to reduce them. Historically, these recommendations (taken directly from the NERC 2019 SOR and the 2018 RISC report) focused on areas such as:

1) Detailed data reporting instructions (DRI) for misoperations to create better alignment of entity understanding and more consistent submissions of misoperation data;

2) Expanded efforts on education, outreach and training;

3) Determining whether enhancements are required to the current family of protection and control (PRC) standards or related NERC guidance materials; and

4) Encouraging industry forums, research organizations and technical committees to share technologies or processes on condition monitoring, failure prevention, spare sharing, resilience and recovery.

[6] NERC State of Reliability 2019

[7] Merriam-Webster dictionary

Continued on page 5

Get Control of Yourself!

Continued from page 4

These are all great recommendations—however, I would like to offer a few more suggestions, specifically a few controls, which might help.

Let's get started with the controls!

The first of these controls speaks directly to the ERO risk element of Improper Determination of Misoperations. The NERC Cause Analysis methods for NERC, Regional Entities and Registered Entities [8] defines a strong incident management control. This control outlines the process of analyzing and reporting on the cause of an event.

The methodology:

1) Outlines the analysis process from data collection and the type of data collected;

2) Reviews the data and how it is assessed;

3) Identifies corrective actions, reporting and following up;

4) Describes a systematic process to identify the appropriate root cause analysis method to use, based on specific criteria;

5) Addresses team composition; and

6) Includes risk presented by Human Performance factor.

This control appears thorough and complete, and when followed should produce the desired product: a clear identification of the cause of an event.

However, I would like to provide a recommendation for the performance of this control. Section 3.5.3 Team Composition states, "The majority of human performance errors and equipment failures are investigated by one or two subject matter experts." The size of the team can sometimes present its own risks. If the team is too small, the investigation could lack the expertise and historical knowledge gained from a diverse, larger team and suffer from cognitive bias. Although, research has identified that smaller teams (less than three members) tend to be more disruptive. "Analyses uncovered a nearly universal pattern: whereas large teams tended to develop and further existing ideas and designs, their smaller counterparts tended to disrupt current ways of thinking with new ideas, inventions, and opportunities." [9] Small teams can produce just as well as larger counterparts, but I would caution that smaller teams present different risks (i.e., cognitive bias) that must be mitigated with secondary controls.[3] I suggest that anytime there are critical, technical steps performed, there should be consideration for segregation of duties.[4] If that is not possible, then a review should be performed by a knowledgeable second party, following key steps.

Next, I would like to offer some controls that could help mitigate the occurrence of a misoperation.

Based on the previously identified reoccurring causes, a defined Coordination Control should be considered. A well-defined Coordination Control is organized in multiple layers that integrate the operations of subsystems into one functioning system. It involves establishing lists of inputs and outputs that affect risks to grid reliability and brings subsystems, or components of a subsystem, together into one system. The aggregation of subsystems works together so that the system performs the overarching functionality.

When defining a Coordination Control, considerations should include:

1) Formulating the concept of coordination through identification of the various internal and external interfaces affecting an organization. Consideration might need to include areas outside the BPS (i.e., possible operations of external network facilities or the reliability of sub-100 kV facilities).

2) Ensuring appropriate communication, cooperation and coordination across all affected parties and planning horizons in order to build a distributed system and develop control synthesis for the coordinated systems.

3) Documenting the internal and external interfaces and the steps required for successful coordination.

4) Verifying and validating the design to ensure it functions correctly and as designed.

5) Identifying a strong Change Management process that properly addresses any changes that affect the control, including emergency conditions. (See my article on Gaps in Program Execution for a detailed discussion on a Change Management control.)

6) Establishing monitoring activities at the department level to be performed at risk-determined intervals.

[8] NERC Cause Analysis Methodology

[9] https://hbr.org/2019/02/research-when-small-teams-are-better-than-big-ones

[10] Secondary Control: An important control that typically takes place after the process it applies to (i.e., reconciliations or reviews) and could be replaced by monitoring. See the RF Knowledge Center/Internal Controls/Internal Control Program & Activities/Internal Control Flashcards

[11] Segregation of Duties: Based on shared responsibilities of a key process, disperse the critical functions of that process to more than one person or department.

Continued on page 6

Get Control of Yourself!

Continued from page 5

I believe a well-defined Coordination Control is a great first step toward reducing misoperations. However, that alone is not enough. To that end, RF has conducted numerous outreach activities over the years. These include conferences regarding technical aspects of misoperations; training sessions for communication technicians, field personnel and relay engineers; technical sessions on power line carrier equipment and issues; and human performance seminars, to name a few. All of these efforts have made progress in moving the needle in the right direction. (See SOR 2019 Figure 3.2.) Still, I believe designing, implementing and monitoring the appropriate controls will help improve those numbers even more.

Figure 3.20: Five-Year Protection System Misoperation Rate by Region Q4 2013 through Q3 2018

A peer review of protection system design and its applicable settings could be a good place to start—especially considering that it is the highest cause of misoperations in our region. This is not a difficult control to implement and would consist of an independent review of protection system design and the settings, during both the design phase and commissioning phase. This control should be a methodical review that systematically analyzes and appraises the data, while adhering to guidelines on the conduct of the review.

As stated in my article on Gaps in Program Execution, verification of your asset listing could mitigate a large risk to the BES. It warrants repeating because incorrect asset listings due to component replacements, setting changes, human error, etc. do occur, placing the reliability of the BES at risk. The risk of not performing this control could place any other controls established around asset performance and asset maintenance in a suspect position. Attacking this issue systematically by establishing a schedule that does not place your entity under undue stress would go a long way in ensuring your reliability to the BES. As in the old "eating an elephant" metaphor, it helps to approach this one bite at a time.

Additionally, in order to maintain an established baseline and all applicable supporting documentation accurately, a strong Change Management control is necessary. The settings/logic/design may be high because the relay settings were correct and reviewed when they were set, but as the system changed (due to fault current changed, generation retired, new substations/lines, etc.), the existing settings/logic/design was no longer ideal. The change itself is not the only challenge—it is all the other systems that the change could impact, such as relay settings busses away. A strong Change Management control addresses and updates all the systems affected by a change.

Finally, I suggest standardized forms to help when designing protection schemes. Considering this process includes obtaining information such as impedance of line information and technical data for the assets, standardized forms could help mitigate the risk of inaccurate or incomplete information. Standardized forms assist a process through familiarity of the form, less deviation from expected information, and higher confidence that all required information is included.

Statistically speaking, the next event is coming, and without the appropriate controls defined, implemented and monitored, the result may not be much different.

Until next time, stay warm and I hope to see you at the Internal Controls Workshop in February where RF will be facilitating the process of documenting your PRC-004-5(i) controls!