Evaluation of Unknown Outages and Misoperations

Related Entity Best Practices
WECC Performance Analysis
December 1, 2016

WECC
155 North 400 West, Suite 200
Salt Lake City, Utah 84103-1114
# Table of Contents

Table of Contents.......................................................................................................................... i  
Introduction...................................................................................................................................... 1  
Transmission Outages .................................................................................................................. 2  
Protection System Misoperations ................................................................................................. 4  
Methodology.................................................................................................................................... 6  
Summary of Findings....................................................................................................................... 7  
  Organizational Culture .................................................................................................................. 8  
  Process.......................................................................................................................................... 9  
  Data Analytics for Preventative Measures .................................................................................. 12  
  Management Involvement .......................................................................................................... 15  
Conclusion....................................................................................................................................... 17
Evaluation of Unknown Outages and Misoperations

Introduction

Transmission system outages and protection system misoperations represent times when the system is operating in a less reliable state. When the cause of the outage or misoperation is unknown, entities can only estimate the level of associated risk and are unable to mitigate or avoid the risk in the future. Analysis of outage and misoperation data indicates that there are some entities with a lower unknown rate than others. These entities maintain low unknown rates through their outage investigation practices. Understanding these best practices sheds light on how other entities may be able to reduce their unknown outage rate.

In its 2013 State of Reliability report, NERC identified the need for further analysis of transmission events with an unknown cause. Across the Electric Reliability Organization (ERO) from 2008 through 2012, 19 percent of the transmission events had an unknown cause. This increased to 32 percent for events lasting more than one minute. This number has remained constant since it was identified in 2013. In its 2016 State of Reliability report, NERC provided three observations:

1. Transmission events with an unknown cause code are one of the top three contributors to transmission severity risk. Transmission severity risk estimates the potential Bulk Electric System (BES) impact of a transmission outage.

2. There was an increase in this risk between 2014 and 2015.

3. The unknown cause code is used more often in the WECC Region than in all other Regions.

NERC has also identified protection system misoperations as a reliability issue. ERO-wide, from 2013 through 2015, 9 percent of misoperations have no known cause. In WECC, from 2013 through 2015, 11 percent of misoperations have no known cause, making it the third-largest cause for misoperations in the West.

---

1 Unknown rate is the percent of outages and misoperations with an unknown cause code from total outages and misoperations.
3 A transmission event may refer to a single transmission outage or the combination of two or more transmissions outages. The NERC State of Reliability analysis uses transmission events. WECC analyzed transmission outages.
5 Transmission risk is defined as the severity of a transmission outage calculated based on the assumed contribution of power flow capacity through transmission circuits based on voltage class normalized by the total number of transmission circuits from the same year and voltage as the event.
WECC has undertaken this initiative to better understand the data behind transmission outages and misoperations with an unknown cause, identify best practices, and provide information to entities to help them improve performance. This report provides analysis of the data and a summary of best practices used by entities in the Western Interconnection to identify outage causes.

Transmission Outages

NERC’s Transmission Availability Data System (TADS) collects transmission inventory and unplanned outage information from NERC-registered Transmission Owners (TO). As of January 1, 2015, TOs report information for the following Bulk Electric System elements:

- AC Circuits (Overhead and Underground)
- DC Circuits (Overhead and Underground)
- Transformers with ≥ 100-kV secondary voltage
- AC/DC Back-to-Back Converters

The outage information is separated into several different categories. Unplanned transmission outages include both automatic (i.e., from the automatic operation of a switching device) and operational (i.e., non-automatic or manual operation) categories. Automatic outages are further refined as either being momentary or sustained. A sustained outage has a duration of a minute or greater.

Figure 1: Unplanned Transmission Outage Categories

All entities are asked to provide a cause for unplanned outages. This allows each entity to determine what went wrong and how to avoid it in the future. This also provides an understanding of the level of risk associated with the outage and how an entity can mitigate or avoid the risk in the future. For
example, an automatic outage with a cause of “vegetation” may indicate an area where increased vegetation management is required. This allows the entity to anticipate similar outages in the area and possibly take preventative measures until the issue is corrected. When an entity assigns an outage an unknown cause, it is stating that it has not identified or understood the cause or risk. In these cases, the entity cannot anticipate possible risks or future impacts to the system.

All automatic outages are assigned:

- an initiating cause code (ICC), a description of what caused the outage; and
- a sustained cause code (SCC), a description of the cause that contributed to the longest duration of the outage.

Note: Momentary outages are assigned an N/A sustained cause code.

Anytime there is an outage, the system is operating in a less reliable state. When it does not know the cause, the entity is not able to provide an explanation or identify how to fix it. Momentary outages with an unknown cause represent a risk; however, a sustained outage with an unknown cause may pose a greater risk because the element remains out of service longer.

Figure 2: 2013-2015 Momentary and Sustained Automatic Outages with an Unknown Cause

From 2013 through 2015 transmission outages with an unknown cause code made up 28 percent of all reported automatic transmission outages (sustained and momentary) in the WECC Region, compared to 14 percent in other Regions.7

7 Source: Transmission Availability Data System, NERC.
In the WECC Region, 40 percent of momentary outages and 23 percent of sustained outages\(^8\) have an unknown ICC and 18 percent of sustained outages have an unknown SCC, or on average one every day.\(^9\)

Figure 3 illustrates the range of entity unknown outage rates. The majority of entities maintain a rate between 10 and 30 percent. Higher unknown outage rates may indicate programmatic, policy or process concerns with how an entity identifies, tracks and addresses unknown outages. Entities with rates below 10 percent employ best practices that directly contribute to their lower unknown rate.

**Figure 3: 2013-2015 Transmission Outages with an Unknown Cause**

---

**Protection System Misoperations**

Based on data from 2013 to 2015, the current top three causes of misoperations in the Western Interconnection are: incorrect setting/logic/design errors, relay failures/malfunctions, and unknown/unexplainable.\(^{10}\)

---

\(^8\) Momentary outages last less than one minute. Sustained outages last one minute or longer.

\(^9\) The sustained cause of an outage is the cause that contributed to its longest duration.

\(^{10}\) While the original NERC report uses data from Q2 2011 to Q3 2013, WECC references NERC data from 2013-2015 to allow for a direct comparison between NERC and WECC data.
In the Western Interconnection, 11 percent of misoperations are categorized as unknown/unexplainable, making it the third most common cause in the West. ERO-wide, unknown misoperations account for only 9 percent of misoperations and are not one of the top three causes. Misoperations with an unknown cause are particularly troublesome because they represent instances where the system was operating in a less reliable state and no reasons have been identified as to why. This means the root causes of these misoperations cannot be analyzed. Further, without an identified cause, it is difficult to determine solutions to reduce the number of these misoperations.

Entities with high numbers of unknown misoperations generally pose a greater risk to reliability. When an entity has a high ratio of unknown misoperations to total misoperations, it may indicate programmatic, policy or process concerns with how the entity identifies, tracks and addresses misoperations. Figure 5 illustrates the range of entity unknown misoperations rates. Approximately half of entities maintain a rate below 5 percent. These entities employ best practices that contribute directly to their lower rate.
Methodology

The distribution of entities with regard to unknown outage rates (Figure 6) indicates that there are entities that are less likely to assign transmission outages and misoperations an unknown cause code. It also shows that there are entities that do so more often.

Figure 6: All WECC Transmission Owners - Sustained Unknown Outage Rates
To explain this distribution, the team gathered information on the practices of entities with lower unknown rates. The team hypothesized that these entities have different practices than entities with higher unknown rates and that those practices may serve as benchmarks for improvement. To evaluate this, the team interviewed entities with the lowest unknown outage rates to understand how they record, investigate and report outages, and identify any best practices. This report shares those findings.

To ensure that the selection of entities appropriately reflected the varied makeup of entities in the Western Interconnection (e.g., a co-op in the Rocky Mountains or a vertically integrated utility in the Northwest), the team identified a group of possible best performers and selected a subset that reflected considerations like size, location and type.

WECC thanks the following entities for participating in the interview process:\textsuperscript{11}:

- Altalink
- Arizona Electric Power Cooperative
- Bonneville Power Administration
- Comisión Federal de Electricidad
- Imperial Irrigation District
- Pacific Gas and Electric Company
- Platte River Power Authority
- Portland General Electric Company
- Public Utility District No. 2 of Grant County, Washington
- Salt River Project
- Seattle City Light
- Tri-State Generation and Transmission Association
- Tucson Electric Power

Summary of Findings

Interviews with entities revealed four themes in their practices around outage investigation that impact their unknown outage rates:

1. Organizational culture
2. Well-defined, formal process
3. Data analytics for preventative measures
4. Management involvement

\textsuperscript{11} Interview entities have given us permission to share their names.
Organizational Culture

Underpinning their practices, each entity the team interviewed demonstrated a pervasive organizational attitude that unknown sustained outages are not acceptable. Entities made statements like, “unknown is not an answer, there is always an answer” or that they hunted answers “with dogged pursuit” and that “an unknown was an admission of defeat.” What also became clear was that each entity recognized the necessity of finding answers while remaining focused on learning and a desire to continually improve. The attitude entities displayed was to, “treat it as a challenge and a problem to solve,” without it being “a gotcha program.” Some entities identified their own company’s positive attitude as a reason for its success.

Best Practice: Establish an organizational attitude that unknown outages are not acceptable. Use outage investigation as a learning opportunity not a punitive activity.
Ownership

During interviews, some of the entities noted that the initiative to build a strong process came from management and was implemented down through the ranks. Other entities indicated the process was developed by workers, from the bottom up. Regardless of the origin of the process, each entity the team spoke to conveyed a clear sense of ownership. Maintaining a low or zero unknown outage number is a matter of professional and personal pride for employees.

A sense of ownership and pride is a difficult best practice to emulate. However, the interviews revealed that when an entity implements a well-designed process and applies a positive organizational attitude, its employees take ownership.

Process

Every entity interviewed has an established process for recording, investigating and reporting outages. Many have extensive process documentation. In some cases, this includes reference materials such as outage flow charts, cause code dictionaries, and department responsibility charts. For a majority of entities interviewed, their processes remain consistent across all outages, rarely deviating for variables such as length of outage or line voltage. In addition, many entities deliberately incorporate TADS and Misoperation Information Data Analysis System (MIDAS) participation in their process. Other practices common among the entities interviewed are that they assign roles and responsibilities, establish communication protocols and manage information.

Roles and Responsibilities

Having a defined process that outlines roles and responsibilities reduces operational ambiguity and confusion. It is important that a process details who is responsible for which tasks and assigns accountability.

Several entities identify individuals or establish groups outside the normal business hierarchy to be responsible for outage
evaluation and root-cause analysis. This individual or group is responsible for ensuring that all the entity’s departments and individuals follow established processes. One entity charged this group with investigating “anything that interrupts current” on their system as part of their Disturbance Analysis Reporting (DAR) process. The entity’s DAR process has been in place for more than 20 years and, as the entity explained, there has been a lot of thought built into the process.

**Communication**

Entities acknowledged the critical importance of clear and consistent communication. Without it, their processes would break down and practices would lose value. For example, the process might instruct the system operator to collect and record specifics about the outage, but without a communication plan, that information will not be shared. The lack of communication can cause frustration with the process, making system operators feel like they have wasted time or the investigation team feel like they do not get necessary information. Successful outage investigation hinges on conveying the information among responsible parties in a detailed and timely manner. Communication methods vary across entities – e.g., by email or system-generated report – but a best practice is that information is communicated within 24 hours of the occurrence. This initial communication then “kicks off” the outage investigation process.

At one entity, the Operations Department sends an email immediately after an unplanned outage occurs to all involved groups such as Asset Management, Substation Maintenance, Transmission Line Maintenance, and System Protection. The entity’s process specifies details like the email title and content to ensure the email can be easily recognized and quickly acknowledged. As a result, recipients of the communication know exactly what their responsibility is and next steps to take. Once the original outage communication is received, the System Protection Department interrogates the relays to

**Best Practice:** Establish a communication plan to ensure clear and consistent communication.

**Best Practice:** Communicate information about an outage or misoperation immediately after it occurs.
determine the fault location and sends the information to initiate a physical patrol.

**Summary Reports and Review Meetings**

In addition to process-specific communication, a majority of the entities interviewed also use daily, weekly, or monthly group communication; e.g., summary reports, as a tool to ensure timely and thorough outage investigation. The reports are distributed widely, in some cases to a hundred or more individuals or everyone in the company. These reports serve as a check-in and big picture review as well as providing an opportunity for everyone, involved or not, to be kept up-to-date on the overall state of the entity’s system and the progress of ongoing outage investigations.

Summary reports are also created for specific groups or functions. For example, one entity will evaluate their relay setting design process when a protection system misoperates and use its internal Relay Protection Committee to investigate the logic and design used to create the setting schemes. This group review is built into the entity’s process as an added measure of protection against future issues.

Several entities use the summary reports as agendas for review meetings. These meetings provide a forum for active discussion to review open outage investigations, beyond what can be accomplished by reading an email or report. The review meetings allow entities to address challenges, roadblocks and possible trends, and to renew focus on identifying outage causes. Additionally, the review meetings often include department and division managers, vice presidents and executive officers.

**Best Practice:** Use daily, weekly, or monthly group communications to keep all parties up-to-date on progress of ongoing outage investigations.

**Best Practice:** Establish regular review meetings as a forum for active discussion and to address challenges, roadblocks and possible trends.
Information Management

Another common practice among the entities is that they establish a central location to store outage investigation and root-cause analysis information. Some entities use a spreadsheet while others have purchased or created programs to support their process. Regardless of the tool, the intent is the same: to store data in a central location and maintain consistency and quality. These tools outline what and how information should be collected. In some cases, operators are provided online forms that guide them through the data they are required to report.

Most of the entities use central information tools to support their investigation process. One entity relies on its tool for after-the-fact analysis. This entity uses web-based tools that house outage planning and scheduling management information, as well as after-the-fact outage information. This entity’s centralized data tools tie together its established processes and communication plans and allows the entity to perform data analytics and create reports used in regular communication throughout the company. These tools provide departments and individuals access to information necessary to complete robust outage investigation and root cause analysis.

Data Analytics for Preventative Measures

With processes in place to provide thorough and consistent data that is accessible in a centralized location, entities can use historical data for analytics. As one entity mentioned, “unknown is an invitation to happen again.” Analysis of past outages provides information that can help identify future issues.

Analyzing Historical Information to Identify Vulnerabilities

Tracking and reviewing past events can help entities identify troublesome patterns and trends in their settings and equipment as well as recognize possible vulnerabilities on their
systems. For example, one entity mentioned that by reviewing historical data, it was able to recognize a particular area in its footprint that experiences higher than average bird migration traffic and identified it as a “birding area.” The entity implements preventive measures specific to this area. Another entity uses historical data to understand different cause types, and identify issue-specific trends or problematic sections of transmission line. The entity then takes measures to avoid recurring issues and reduce the number and severity of transmission outages and misoperations, including those with an unknown cause. These examples demonstrate a proactive approach rather than simply waiting for an event to occur and then reacting accordingly.

**Inspecting similar elements or locations for common issues**

Almost all the entities the team spoke with indicated that when they discover the cause of an outage or misoperation, they inspect similar elements and locations for the same issue. If a misoperation occurs and has been attributed to incorrect settings, entities review all the protection system relays of the same type to verify and correct the settings. Some entities evaluate their entire system in response to an outage, rather than focusing on an individual outage or element. This practice can help prevent future occurrences. As one entity stated, “only the paranoid survive.”

**Applying Lessons Learned**

More than half of the entities the team spoke to review each individual outage and misoperation to identify “lessons learned.” Then they apply these lessons across their whole system to identify abnormalities that may not be noticeable on their own but could contribute to a future event if left unchecked. For example, after experiencing several outages with an unknown cause, an entity was able to attribute the cause to a combination of morning dew and temperature swings, issues that on their own seem benign. The issue
Evaluation of Unknown Outages and Misoperations

impacted more than one type of element so the entity applied changes across its system.

**Sharing lessons learned**

After the entities review their elements and system, they develop lessons learned. A majority of the entities share their lessons learned across the organization. Entities share and incorporate the lessons in multiple ways, including summary reports, review meetings, training topics, and process documentation. One entity the team spoke with holds an annual review of all of its lessons learned and produces a company report. This provides a great training opportunity and demonstrates good communication with personnel. It also promotes transparency and an atmosphere that encourages learning from mistakes rather than reprimanding or hiding from them.

**Building lessons into business processes**

Entities can further benefit from data analytics by incorporating lessons learned into business processes. One entity performs a physical asset evaluation. The entity has a maintenance engineer evaluate the summary reports prepared by its disturbance analysis team monthly. This particular review is focused on the fault and physical nature of the outage and the results of the analysis are incorporated into the entity’s asset management program.

One entity includes a list of Human Performance tools in its relay maintenance and testing manual as a way to mitigate Human Performance issues and provide additional resources to their employees. Some of these tools include various signage and tags that can be used to raise awareness of the task at hand. Continuous training is provided to ensure personnel are familiar with all of the tools available.

Best Practice: Incorporate lessons learned in summary reports, annual reports, training, and process documentation.

Best Practice: Include Human Performance tools in relay maintenance and testing manuals.
Creating performance metrics and incorporating into corporate goals

The majority of entities the team spoke to include outage investigation in their company’s performance metrics. For several entities this means going beyond the standard industry reliability metrics, like System Average Interruption Duration Index (SAIDI) and Customer Average Interruption Duration Index (CAIDI), to create their own metrics. This folds the outage investigation process into these companies’ performance and strategic goals.

Management Involvement

Management involvement ensures employees complete processes, take appropriate corrective actions, and perform thorough system review to identify similar situations so measures can be taken to prevent future outages. Management at many of the entities interviewed are active participants throughout their company’s process. This goes beyond inclusion on an email list. These managers, directors and other company leaders are actively involved in advancing investigations. They ensure the appropriate steps are taken to identify the cause of the outage and complete corrective actions. For many entities, management uses the reports on outage investigation status as a discussion tool to work with department representatives and identify where they are in the process and what steps still need to be taken.

Shared Accountability

One of the practices prevalent among the top performing entities is sharing accountability for the outage investigation process among different departments in the organization, including management. This collective responsibility ensures the appropriate departments are involved in accurately identifying causes of events and reporting them.

Assigning multiple departments responsibility to contribute to outage investigation creates multiple opportunities to include knowledge and experience. It also creates a natural tie to

Best Practice: Include outage investigation in company’s metrics and strategic goals.

Best Practice: Share accountability for the outage investigation process among different departments including management.
management as information flows from department to department. One of the entities interviewed described how a District Manager’s report is used to create transparency and accountability. The company creates the report each month and shares it with all the operation centers in the district. The report details the count of completed outage investigations and lists unknown outages as missing outage reports. This practice highlights transparency and accountability across the entity’s divisions because each center’s status can be seen by its peers. It also generates healthy competition to investigate and report on outages.

**Performance Incentives**

Many of the entities tie participation in the outage investigation process to year-end reviews and incentive programs. Management sets expectations for outage investigations and motivates employees to provide quality contributions. Employees know management will review investigation reports. Management involvement and acknowledgement heavily influence employee and department attitudes.

**Resource Commitment**

The entities interviewed represent a wide range of size and operating structure, but all of the entities commit time and resources to perform complete and thorough outage investigations. Management support and involvement is paramount to ensure each entity can dedicate the time and resources necessary.

Some entities, both large and small, perform physical patrols on every outage – momentary or sustained. These patrols can be incredibly time consuming and in some cases require additional investment in equipment, like helicopters for remote or hard-to-reach lines.

**Best Practice:** Include outage investigation to year-end reviews and incentive programs.

**Best Practice:** Perform physical patrols on every outage – momentary or sustained.
At a majority of entities, management support is key to ensuring adequate commitment of resources to tools and technology. A few examples of this commitment include:

- Upgrading relay technology to make fault information available immediately to operators through Supervisory Control and Data Acquisition (SCADA).
- Using weather and lightning programs correlated with a GIS system to assist in locating and determining outage causes.
- Using fault information to identify specific structures within a GIS system to target outage patrol areas.
- Installing fault recording devices in all major substations.

Other entities outlined the commitment of resources in terms of staff participation and time. Management at these entities create an environment where staff feels not only able but obligated to dedicate time to thorough outage investigations.

**Conclusion**

Outages and misoperations with an unknown cause represent a risk to the BES and, as one entity aptly put it, “are an invitation to happen again.” There are entities in the Western Interconnection that have demonstrated an ability to reduce, avoid and mitigate outages and misoperations with an unknown cause. The entities interviewed outlined several best practices that assist them in these efforts. Entities across the Western Interconnection, regardless of size or location, should review these best practices and evaluate their own practices to determine where they can make improvements.
Disclaimer

WECC receives data used in its analyses from a wide variety of sources. WECC strives to source its data from reliable entities and undertakes reasonable efforts to validate the accuracy of the data used. WECC believes the data contained herein and used in its analyses is accurate and reliable. However, WECC disclaims any and all representations, guarantees, warranties, and liability for the information contained herein and any use thereof. Persons who use and rely on the information contained herein do so at their own risk.