Protection System Misoperations

Report and Mitigation Approaches

January 2017

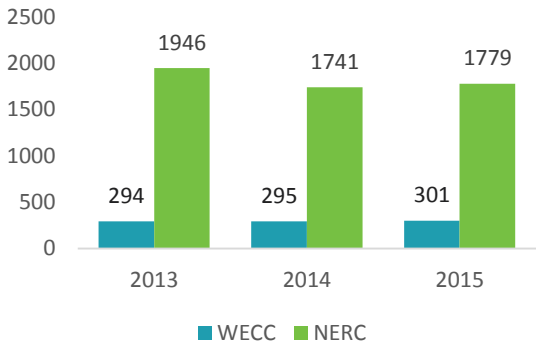
WECC

Table of Contents

Introduction

Protection systems protect sensitive equipment and help support the overall reliability of the Bulk Electric System (BES). When a protection system misoperates, the system is in a less reliable state. Protection system misoperations (misoperations) contribute to transmission outages and negatively impact system reliability.[1] The North American Electric Reliability Corporation (NERC) has set a target of a nationwide misoperation rate of 8 percent by 2020,[2] a decrease of approximately 15 percent from the current rate.[3] In the West, over the last three years, misoperations have increased by around 2 percent, while ERO-wide there was a 9 percent decrease in the total number of misoperations.

Figure 1 – Misoperations by Year



To help meet the NERC target, WECC and its members will 1) analyze misoperations to determine trends in causes, 2) identify potential risks and areas of improvement, and 3) develop a West-wide work plan to reduce the number of misoperations in the West. This document:

- addresses the first two of these activities;
- provides information based on WECC's analysis of misoperation data;
- highlights the top three misoperation cause categories in the Western Interconnection;
- identifies risks associated with each type;
- provides suggested practices for improvement; and
- lays the groundwork to develop a West-wide misoperations reduction plan, which will be the focus of this effort in 2017.

This document was developed through a partnership of WECC staff and the Relay Work Group (RWG). The RWG provides technical expertise on protection system relays and consists of representatives from entities across the Western Interconnection. Members are experts in the design, construction and operation of protection systems. WECC and the RWG work together to the review of misoperations reported by entities.

[1] State of Reliability 2015, NERC, May 2015.
[2] ERO Enterprise 2017-2020 Strategic Plan and Metrics, NERC, November 2016.
[3] NERC's 2015 State of Reliability report shows the ERO Misoperation rate at 9.4 percent.

Key Findings

Three causes account for three-quarters of misoperations

Three misoperation cause categories—1) incorrect setting/logic/design errors, 2) relay failures/malfunctions and 3) unknown/unexplainable—make up 73 percent of all misoperations. Entities can most effectively reduce misoperation rates by targeting these categories.

The complexity of new relay technology contributes to misoperations

Multifunctional programmability has made microprocessor-based relays the industry norm. However, the complexity of these relays presents human performance challenges. Ninety percent of misoperations in the incorrect setting/logic/design errors cause category involved microprocessors. Defined and documented control measures are key to managing this complexity.

Unnecessary trips make up 94 percent of misoperations in the Western Interconnection

Many entities err on the side of setting their relays to be highly sensitive. The result is a large number of unnecessary operations. Entities may be able to reduce unnecessary trips by thoroughly examining settings and assuring their systems appropriately balance between dependability and security.

Entities are addressing issues associated with past misoperations but not always how to prevent them from happening again

A high volume of misoperations with similar causes suggests some entities are implementing insufficient preventative measures. Eighty-eight percent of Corrective Action Plans filed by entities from 2013 through 2015 are complete; however, the number of misoperations during that time has not decreased. Entities should include preventive actions in their Corrective Action Plans.

Poor data reporting hinders analysis of misoperations Interconnection-wide

Good quality data is essential to an accurate analysis of misoperations and the potential risks misoperations pose to the reliability of the system. In many cases, the information submitted by entities about their misoperations lacks sufficient detail to allow for a thorough, high-quality analysis. Entities can support analysis activities by providing complete and consistent information.

A failure to identify the cause of a misoperation increases the possibility of it occurring again

A high proportion of unknown misoperations may indicate programmatic, policy or process concerns with how the entity identifies, tracks and addresses misoperations. Failure to identify the cause of a misoperation allows for a greater chance that the same misoperation will happen again because the entity does not know what went wrong or how to fix it. Addressing internal processes may result in fewer unknown misoperations and, by extension, fewer misoperations overall.

Overview

Protection systems detect certain conditions and react in a pre-determined way to protect sensitive equipment and help assure the overall reliability of the BES. A protection system consists of protective relays, associated communication systems, voltage and current sensing devices, station batteries and DC control circuitry.[4] A protection system element misoperates when it either fails to operate as designed, or operates unintentionally or outside of its zone of protection.

Protection system owners track and report information to NERC on the total number of correct operations and detailed information about all misoperations on a quarterly basis.[5] The detailed information on misoperations includes specifics on timing, element condition, and sequence of events, as well as a Corrective Action Plan (CAP) to address the issue. As part of the reporting process, entities assign each misoperation a cause category. (Table 1)

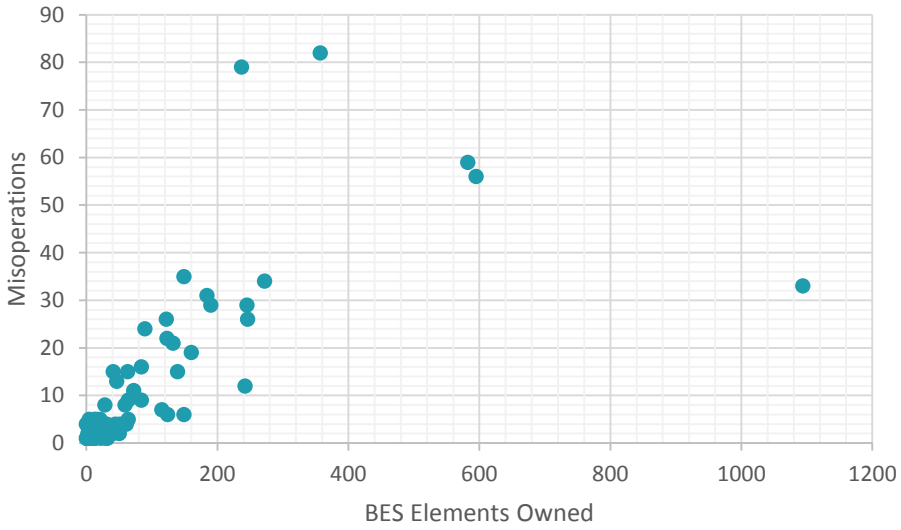
Table 1 – Misoperation Cause Categories

Cause Category	Description
AC System	Problems in the AC inputs to the protection system
As-left Personnel Error	As-left condition of the protection system following maintenance or construction procedures
Communication Failures	Failure of the communication systems associated with the protection system
DC System	Problems in the DC control circuits
Incorrect Setting/Logic/Design Errors	Errors in the settings, logic or physical design of the protection system
Relay Failures/Malfunctions	Improper relay operation
Other/Explainable	Identified cause not included in any other category
Unknown/Unexplainable	No cause can be determined

[4] Glossary of Terms Used in NERC Reliability Standards, NERC
[5] Request for Data or Information: Protection System Misoperation Data Collection, NERC, August 2014

The incidence of misoperations in the Western Interconnection is fairly evenly spread across entities and, with few exceptions, there are not clear best or worst performers. This means the concerns with misoperations, and any strategy to reduce the misoperations rate in the West, must focus broadly.

Figure 2 – Misoperations per Entity by BES Elements Owned



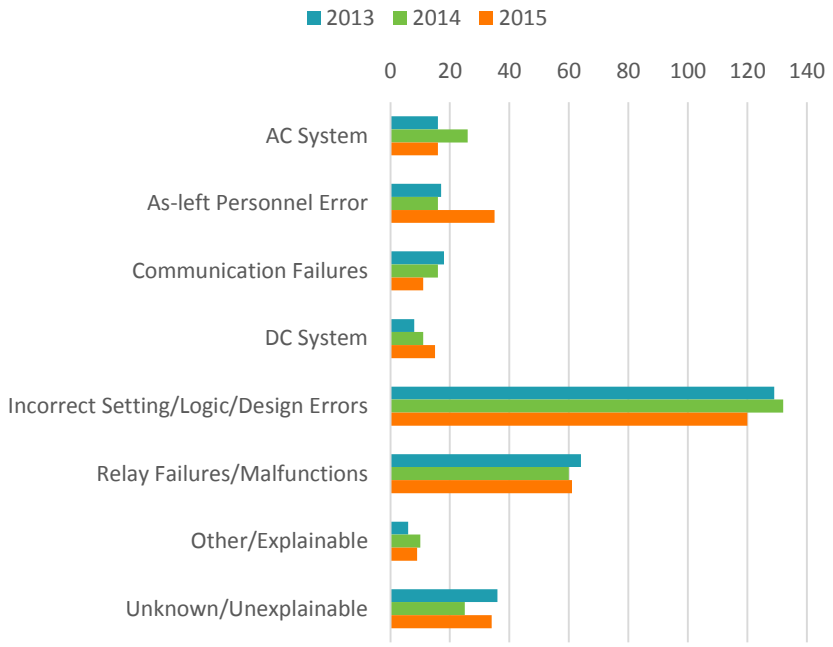
Top Cause Categories

The top three causes of misoperations in the Western Interconnection are: incorrect setting/logic/design errors, relay failures/malfunctions, and unknown/unexplainable.

The incorrect setting/logic/design errors category is the largest cause category and accounts for nearly half of all misoperations in the West. This includes misoperations due to errors in relay scheme logic and design, and application of designed settings to equipment.

The second largest cause category, relay failures/malfunctions, makes up 21 percent of the

Figure 3 – Misoperations by Cause Category



misoperations in the Western Interconnection. Relay failures and malfunctions primarily involve equipment issues. These can be the result of aging or defective equipment or a particular make and model that experiences frequent issues.

The third largest cause category in the Western Interconnection is unknown/unexplainable. This cause category is troubling because misoperations in this category indicate instances when the Interconnection was operating in a less reliable state but the reason is unknown.

Entities are responsible for investigating the causes of misoperations. The high number of misoperations in this cause category may indicate opportunities for improvement in entity investigation processes.

The remainder of this document breaks down each of the top three cause categories in the Western Interconnection and provides information and recommended best practices for improvement.

Incorrect Setting/Logic/Design Errors

Incorrect settings, logic or design errors account for 43 percent of misoperations in the Western Interconnection from 2013 - 2015. The high volume of these misoperations is concerning; however, because these misoperations are closely tied to human performance, this cause category represents ample opportunity for improvement. The complex process of bringing a protection system online provides many opportunities for human error, which may be more easily addressed than equipment issues or other misoperation causes.

The Incorrect setting/logic/design error cause category is broken down into four contributing factors, reflected in the subheadings of this section: Complex Setting Designs, Protection System Reliability, Corrective Action Plans and Data Quality.

Complex Setting Designs

As systems evolve, they frequently increase not just in sophistication, but also complexity. This is particularly true of protection systems found in modern substations, where entities are replacing electromechanical relays with newer, more advanced technology. This newer technology is capable of multiple functions, which increases the complexity of settings design compared to simpler, older technology.

Microprocessors have become the industry norm in protective relays. As older electromechanical and solid-state relays age, they are most frequently replaced by microprocessor technology. There are positive and negative aspects to this change. Microprocessor-based relays are multifunctional and allow for more detailed and precise settings such as:

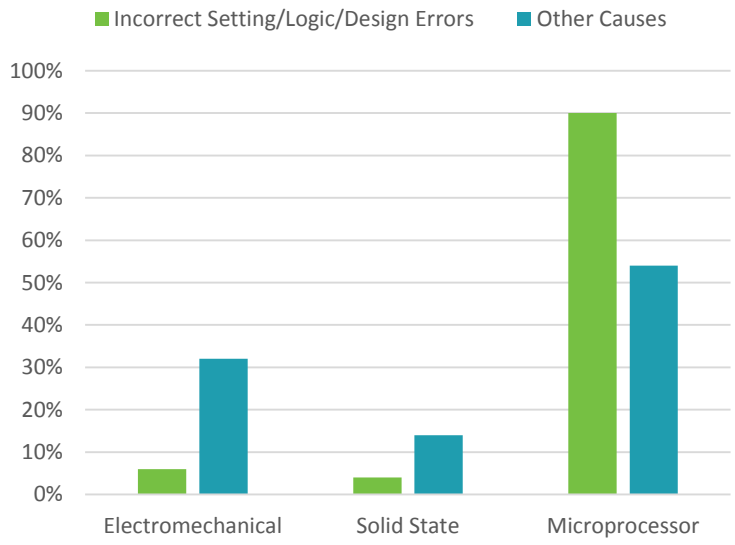
- provide programmable and adaptive logic;
- allow for multiple elements in a protection scheme;

- are self-monitoring;
- record sequence-of-events and oscillography; and
- have the ability to communicate with data acquisition computers and other relays.

This technology can help engineers and field technicians narrow the scope of investigation when a line trips, and focus resources appropriately.

However, microprocessor relays are also much more complicated than their predecessors. When designing relay setting schemes, engineers must consider many questions ranging from high level (e.g., how many functions and relays are necessary) to minutely detailed (e.g., which contact ratings are needed). Once the schemes have been created, technicians must correctly apply the settings to the protection system elements. There are many steps involved in designing and applying relay settings. This results in more opportunities for error in both the setting design process, the application of elements, and the installation of those settings in the field.

Figure 4 – Misoperations by Relay Technology 2013-2015



Compared to other types of relay technology, microprocessors represent a substantially larger proportion of misoperations. Ninety percent of misoperations in the incorrect setting/logic/design errors cause category involved microprocessor technology. This is largely a consequence of the growing use of microprocessors throughout the system. However, given its complexity, this type of technology may be more likely to misoperate due to incorrect setting/logic/design errors. Electromechanical and solid state relays may have a lower misoperation rate because many setting errors have already been corrected during their longer time in service. Older protective relays also

have a limited number of relay settings that require infrequent changes due to their long design life. In contrast, microprocessor relays have potentially thousands of different settings options, nearly always resulting in more complex schemes. There may be multiple hardware and software designs for relays from the same manufacturer, even though they may appear to be identical.

While microprocessor-based relays are useful tools, their complex nature presents human performance challenges in the absence of defined and documented control measures.

Recommendations for Improvement

Entities should review misoperations and trends in misoperations for human performance issues, particularly those resulting from setting/logic/design errors. Entities should then use the information to develop lessons learned and preventative measures to reduce human impact on the rate of misoperations. Some common human performance enhancements entities can employ include documenting processes for firmware updates and settings application, performing fault studies and testing, and enhancing their training and use of peer reviews.

Defined Process for Firmware Updates

Microprocessors require firmware. Firmware changes can lead to misoperations if different components of a composite system use different firmware versions. Frequent firmware updates from the manufacturer and different versions of firmware can lead to compatibility issues or new settings that have not been accounted for. Entities should be conscious of these issues when making changes to relay firmware. There should be an identified benefit for changing relay firmware, and these changes should be documented for future reference.

Firmware changes may require redefinition and repeated adjustment of relay settings, providing more opportunities for human error. Entities should have a defined process for documenting, testing and managing the firmware in place for each device. This process should contain specifics of when firmware for the various applications should be updated. In case of relay replacement, entities should ensure the new relay has the same firmware version as the original unit. To be most effective, the process should be mandatory and well-communicated to all employees involved with relay setting work. A clearly defined, well-communicated process can help avoid firmware compatibility issues.

Defined Processes

A documented process for applying relay setting changes in the field can help minimize mistakes and human error. For example, an entity could record existing ("As Found") settings, apply the setting change, and compare the new state ("As Set") to the previous "As Found" state. The difference between the two should be limited to only the intended changes. The entity should retain the "As Found" and "As Set" setting files for reference. Some manufacturers provide a comparison tool within their software that simplifies this practice. Entities could use the comparison tools in manufacturers software to track this information.

Fault Studies and Testing for Setting Changes

Entities should update their short circuit studies regularly, [6] especially when there is a change in system configuration. Entities should also ensure that the results of their short-circuit studies are comparable to their planning model studies. As part of this process, entities should review BES settings and make necessary setting adjustments. Validating their fault studies by comparing fault duty from actual events to that predicted by their latest fault study is another effective practice for entities.

Applications-based testing prior to issuing settings to relay technicians can provide enhanced quality assurance. For example, commissioning test plans can be prepared for playback through a power system simulator using modeling software to generate faults with expected values as fault quantities. This approach vets an application prior to issuance to field personnel. This practice is preferred to using an element-by-element testing philosophy that can only confirm a relay's accuracy to operate based on an entered setting that may be incorrect due to an entry error. Using the appropriate tools can help assure modeling and testing programs meet the needs of the entities.

Complex Setting Recommendations:

- Develop and maintain a documented process for managing firmware updates.
- Develop and follow a documented process for changing relay settings in the field.
- Perform short-circuit studies whenever there is a configuration change on the system.
- Review settings on a scheduled basis.
- Implement a formal training process for new employees.
- Perform peer reviews prior to implementing changes to relay settings.
- Review similar elements or setting schemes for known issues

[6] For example, PRC-027-1, currently pending regulatory approval, requires a maximum time interval of six years.

Training and Peer Review

It is important to maintain a consistent level of expertise among protection department personnel. Entities should provide expert training when new equipment is introduced or new personnel are brought in. A good training process may include:

- Using experienced personnel as mentors;
- Ensuring employees are familiar with company standards for protection systems;
- Involving new employees in the testing process; and
- Starting with simple models and escalating to more complex applications as skills develop.

Another good training practice is to have an experienced engineer create the settings and then have them peer reviewed by a person of equal or greater experience to confirm the basis for the calculations and communications used in the settings.[7]

For more complex schemes, entities should consider multiple peer reviews. Engineers should review the needs of their systems carefully when designing each scheme, and use simplified templates where possible, while still maintaining the appropriate level of security and dependability for their protection systems.

Other Recommendations and Resources

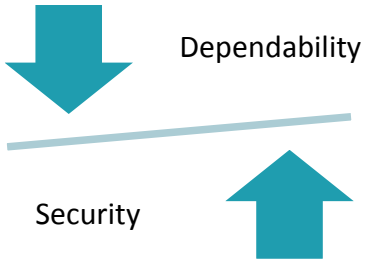
When a misoperation occurs, entities should review the system to identify where similar setting schemes/designs are used. Proactively addressing those locations and equipment may prevent a similar misoperation from occurring in the future.

The Institute of Electrical and Electronics Engineers (IEEE) has published several papers on protection system relay settings, including a report that specifically addresses microprocessor relays.[8] Additionally, NERC provides lessons learned as part of the Event Analysis Process on their website that frequently includes topics relevant to protection system operations.[9] These reports may provide beneficial information to entities looking for guidance.

[7] Processes, Issues, Trends and Quality Control of Relay Settings, IEEE PSRC Working Group, March 10, 2007.
[8] Relay Scheme Design Using Microprocessor Relays, IEEE Working Group C16, June 2014.
[9] Lessons Learned, NERC.

Protection System Reliability

Figure 5 – Protection System Qualities



Reliable protection systems must exhibit two qualities: dependability and security. Dependability refers to the certainty that a relay will operate correctly. Failure to operate when required or to operate at the designed speed raises concerns with the dependability of a protection system. Security refers to the certainty that a relay will not operate incorrectly. An unnecessary operation raises concerns with the security of a protection system.[10] A dependable protection system always trips for the condition (usually a fault) it is supposed to detect; it never fails to trip for this condition. Conversely, a secure protection system only trips when the condition it is designed to detect is present; it never trips for other conditions or in the absence of the condition it is supposed to detect.

When creating the settings for protection system relays, it can be difficult to achieve the optimal balance between dependability and security. These qualities often act in opposition to each other, and must be balanced when designing a protection system. For example, increasing the sensitivity of a relay will increase its dependability, ensuring the relay will operate. At the same time the security is reduced because it is so sensitive, it will more likely operate for faults outside its zone of protection.

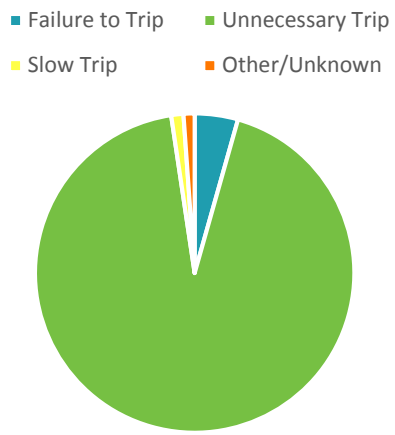
When reporting a misoperation, entities assign a misoperation category. The category classifies a misoperation based on the type of trip (unnecessary trip, slow trip, or failure to trip) and whether the misoperation occurred during a fault.[11] These categories indicate whether the misoperation was dependability-based or security-based.

Table 2 - Misoperations Categories

Dependability-based Failure	Security-based Failure
Failure to Trip – During Fault	Unnecessary Trip – During Fault
Failure to Trip – Other than Fault	Unnecessary Trip – Other than Fault
Slow Trip – During Fault	
Slow Trip – Other than Fault	

[10] NERC SPCS Report to the Planning Committee: Reliability Fundamentals of System Protection, December 2010.
[11] An event occurring on an electric system, such as a short circuit, a broken wire or an intermittent connection.

Figure 6 – Misoperations by Category



Recommendations for Improvement

Between 2013 and 2015, 94 percent of misoperations in the Western Interconnection were security-based. This is unsurprising as system impact is generally less severe when an unnecessary trip occurs, so entities often tend toward security-based settings. A failure to trip can lead to equipment damage and force remote protection systems to operate, isolating a larger part of the system. However, unnecessary trips are not without risk. Every unnecessary trip means that lines are not available during the time it takes them to come back online. The Southwest Outage on September 8, 2011 was exacerbated by unnecessary trips after the initial system fault had been cleared. Entities may be able to reduce unnecessary trips by thoroughly examining settings and assuring they have the most appropriate balance between dependability and security for their particular systems.

Corrective Action Plans

When reporting a misoperation, entities include information about what corrective actions have or will be taken to resolve the issue. If the Corrective Action Plan (CAP) is ongoing at the

Protection System Reliability Recommendations:

- Review protection system settings to ensure a proper balance between dependability and security.

time of the initial report, entities should make regular updates until all action items in the CAP have been completed.

Eighty-eight percent of all CAPs filed for misoperations in the incorrect setting/logic/design category have been completed from 2013–2015, indicating a positive effort from entities to correct identified issues. However, this high completion rate has not resulted in fewer misoperations. This suggests that entities may not be including, or may be including insufficient data for, preventative measures in their Corrective Action Plans.

Despite a high volume of CAP completion, similar issues continue to recur. This suggests insufficient preventative measures implemented during the corrective action stage.

Recommendations for Improvement

Entities should look beyond the individual element(s) that misoperated and be proactive in their CAPs. This may include:

- Reviewing settings of all relays at the station where the misoperation took place;
- Reviewing settings of directly connected stations;
- Looking for similar installations throughout their system to ensure correct settings are in place;
- For relay failures, looking for locations where the same make and model are in service, and reducing time between maintenance and testing; and
- Reviewing systems to ensure that no single failed element would induce a failure to trip, and adding redundancies where practical.

Entities may also consider reaching out to other entities or industry forums to see what actions have been successful in similar situations.

Corrective Action Plan Recommendations:

- Include preventative measures in CAPS, including examining similar equipment for identified issues.
- Engage with other entities or industry forums to identify potential common failures and solutions.
- Conduct a peer review of CAPS to see what similar entities have done in like situations.

Data Quality

The quality and sufficiency of information reported by entities on their misoperations is not consistent. Many entities do not report complete information resulting in an inability for WECC and the RWG to assess the root causes. To identify a root cause and conduct a meaningful analysis of a misoperation, analysts require a full description that details a sequence of events and equipment involved. Unfortunately, very often event descriptions are short and generic, limiting the ability to identify and analyze possible trends in misoperations across the Interconnection. The CAPs similarly contain vague or very high-level information.

Information submitted by entities about misoperations often lacks sufficient detail to allow for thorough, high-quality analysis. Missing information and inconsistencies must be filled in by the expertise of a third-party subject matter expert.

More concerning are the instances where the cause of a misoperation provided by an entity was contradictory to the description supplied. This places the burden for determining the cause on the subjective expertise of a third-party subject matter expert, who must fill in any holes in the information with judgement. In addition, it is unknown whether this demonstrates a deficiency in reporting practices or actual confusion surrounding the investigation and analysis of a given misoperation.

Recommendations for Improvement

Reporting Detail

For WECC, NERC and entities to perform thorough analysis, entities must include enough details in their misoperations reports to be able to determine:

- The initiating event;
- Whether the system was initially in a normal or abnormal condition;
- The specific facilities involved;
- The components that did not function correctly; and
- A detailed description of the root cause of the misoperation.

This information will allow those reviewing the submissions to be able to clearly step through the event, identify root causes, and analyze potential Interconnection-wide patterns and trends.

Training on Reporting Misoperation Information

With the changes surrounding misoperation reporting, WECC has revised its review processes. This includes working closely with the RWG to review each quarter's submissions, and following up with the entities to obtain more detailed information and clarification as needed.

As the new misoperation process matures and improves, WECC will communicate with entities regularly on data submission quality. WECC will continue to work with the RWG, NERC, and the entities to provide more training on reporting and to identify best practices in an effort to complete the missing information and improve overall data quality. This training will be open to all and entities are encouraged to attend. WECC also welcomes entity input on additional training they would like to receive related to misoperations.

Data Quality Recommendations:

- Document reported misoperations thoroughly, as outlined in the reporting template and data request.
- Attend WECC training on misoperation reporting

Relay Failures/Malfunctions

Relay failure or malfunction causes nearly a quarter of misoperations in the Western Interconnection. The most common course of action in Corrective Action Plans for these misoperations is to replace the failed relay or component. While replacing defective equipment is a good start, it only addresses the issues with the individual element that misoperated, rather than preventing similar issues from occurring across the composite protection system.

Recommendations for Improvement

Familiarity with known issues among particular makes, models and types of equipment can help an entity be proactive in monitoring its own inventory for potential vulnerabilities.

Tracking Failures

Some equipment failure may be expected as elements age or as a result of manufacturer defects. However, it is important to understand the manner and frequency of relay failures to better identify patterns and possible risks of failure. Tracking equipment failure can help identify potential problems and solutions and help reduce these types of misoperations. Entities should track relay failures to identify makes and models with the highest failure rates. Manufacturer websites often identify known problems, which can be helpful to entities in their own tracking. Entities can also engage in industry forums to learn about relays with high failure rates.

Relay Testing Intervals

As equipment approaches the end of its lifecycle, it may become more prone to fail. Monitoring and testing older equipment more frequently may prevent failures. Entities should reduce intervals for relay testing and maintenance for older equipment to better understand the state of aging equipment and monitor its functionality.

Relay Failures/Malfunctions Recommendations:

- Track the make and model of relay failures to identify potential trends across equipment types.
- Engage industry and manufacturer forums to hear about consistent and emerging equipment issues.
- Reduce testing and maintenance intervals for aging equipment and models with known issues.
- Verify the operation of the entire composite protection system after a misoperation.
- Have a defined process for managing firmware.

Proactive Replacement

If an entity identifies potential issues with a particular relay or type of relays, it should consider replacing those makes and models before they fail. To manage the costs of replacing relays, entities should start by identifying facilities that have the largest system impact.

Most manufacturers have a documented lifecycle for their equipment. Entities should be aware of this lifecycle, and track when equipment is reaching the end-of-service timeframe. Having a replacement program in place based on the manufacturer's lifecycle can reduce misoperations caused by relay failures or malfunction.

Component Review

Thorough analysis of an entire composite protection system can help avoid a related misoperation in the future. Sometimes a successful operation masks the failure of one of the system's components. That failure may cause a misoperation at a later time under different conditions. When a relay operation occurs, entities should verify that all components operated correctly.[12] After a relay failure, entities should identify similar installations or applications that may need repair or replacement.

[12] For example, by reviewing both A and B schemes.

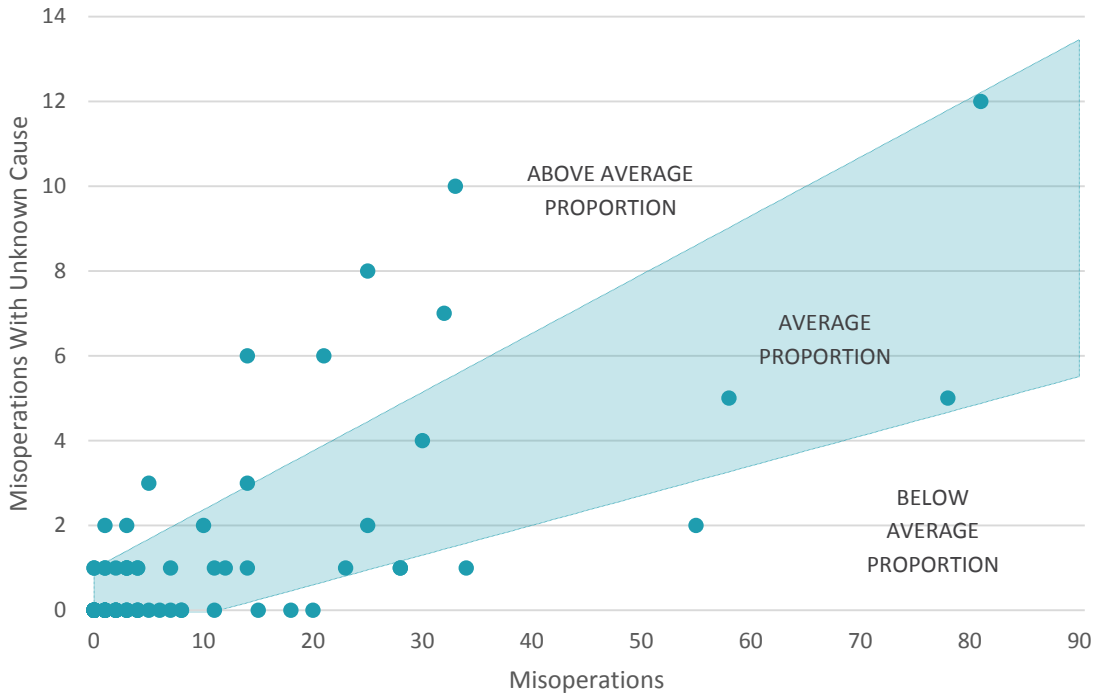
Unknown/Unexplainable

In the Western Interconnection, the cause of 11 percent of misoperations is unknown. When an entity does not know the cause of a misoperation, they cannot understand what happened and how to prevent it from happening again, or identify potential associated risks.

A failure to identify the cause of a misoperation allows for a greater chance that the same misoperation will occur again because entities do not understand what went wrong or how to fix it.

A high proportion of unknown misoperations generally poses a greater risk to reliability. There is a greater chance of the same misoperation occurring multiple times because entities can't identify what went wrong or how to fix it. An initial investigation suggested that at least one-fifth of misoperations are repeat misoperations.[13] This is a key area for further study. However, data currently available do not allow rigorous analysis of repeat misoperations. WECC recommends additional information, such as equipment make, model, year, and type be gathered as well as a way be provided for entities to indicate if a misoperation is a repetition of a previous misoperation.

Figure 7 – Unknown Misoperations by Entity



[13] A repeat misoperation was defined as an additional misoperation of a single element with the same cause code.

A high ratio of unknown to total misoperations may indicate programmatic, policy or process concerns with how the entity identifies, tracks and addresses misoperations. Approximately ten entities in the West have unknown misoperations rates that are significantly higher than average (Figure 6). These entities may have opportunities for improvement in their investigation processes. On the other hand, six entities have a proportion significantly lower than average. These entities' investigation processes may model best practices.

Recommendations for Improvement

Addressing internal processes may result in fewer unknown misoperations and fewer misoperations overall. Improving data gathering and reporting, conducting peer reviews, and conducting holistic reviews of misoperations may help entities improve.

Data and Information Gathering and Reporting

By improving information gathering practices, entities may improve their ability to ascertain the cause of misoperations.

Entities should have well-documented, rigorous processes to investigate the cause of a misoperation. The processes should include all information sources and avenues of investigation that may help identify a cause. Information gathering should span from the most general, like the system's initial operating state, to more specific information, like the status of protection and monitoring devices within each station associated with a misoperation. Information gathering should also include data from nearby stations with devices that may have detected the event. This will allow an entity to compile a more complete sequence of events that can help identify what caused the misoperation, and potentially how to prevent it from recurring.

Peer Review

The shared experience of industry experts can be very helpful to entities as they investigate misoperations. Peer groups may be able provide insight into potential causes of misoperations, with the added benefit of sharing potential issues across multiple

Unknown/Unexplainable Recommendations:

- Establish and document investigation processes, including:
  - Gathering information from protection and monitoring devices;
  - Reviewing event reports;
  - Including the entire composite protection scheme in the scope of an investigation; and
  - Compiling a detailed sequence of events.
- Incorporate industry expertise in investigation processes.
- Update misoperation reports if a cause is found after submitting the initial report.

entities to be addressed broadly. The RWG is a resource for these investigations. Entities should take advantage of this or other peer resources while investigating the causes of misoperations.

Holistic Review

The scope of investigations should include a review of how the entire composite protection system scheme operates, not only the relay that misoperated. Detailed review of available event reports will often point toward relay setting or logic errors, hardware failures, wiring problems, and other factors that contribute to misoperations. From there, entities should scheme test and troubleshoot the protection systems with the gathered event data to find possible causes, always documenting tests and results for later reference and analysis.

If the cause is not found after event review and testing, the entity should consider what can be done to ensure the cause can be identified if the same misoperation were to happen again. For example, the entity could install a temporary monitoring device that can record key signals to support analysis and troubleshooting.

Finally, investigation processes should include updating misoperation reports filed with NERC if the cause of a misoperation is identified after an initial report has been submitted. This will ensure that data used for future Regional and NERC analysis are a current and accurate representation of the status of misoperations.

Conclusion

Protection system misoperations exacerbate transmission outages and undermine BES reliability. The best way to reduce the incidence of misoperations and mitigate their impact is to implement a rigorous, documented misoperation investigation process that incorporates the suggestions contained in this report. Entities should approach misoperation prevention proactively, developing testing, maintenance and replacement programs that target high-risk relays. Entities should also act collaboratively by participating in industry work groups.

WECC and NERC will continue to analyze misoperations to identify best practices and recommendations, and to develop training programs. Entities can support these activities by ensuring misoperation reports are thorough and contain high-quality data, updating these reports as necessary.

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.