SERC Regional Best Practices for Reduction of Protection System Misoperations

Objective: This regional best practices document provides SERC entities with focus areas and suggested tools in order to reduce Protection System (PS) Misoperations.

Purpose: These best practices were compiled in support of the NERC objective for reducing Protection System Misoperations, stated in the December 2014, *NERC Staff Analysis of Protection System Misoperations*. This best practice document is offered as guidance to SERC entities but may not apply depending on individual company protection philosophies or applications. The SERC Protection and Controls Subcommittee (PCS) has identified those areas or tools that may occur more frequently or have more impact as they relate to system performance or events.

Best Practices: Misoperation evaluation and recommendations are based on NERC/SERC aggregate data. Each entity is unique and should assess their specific circumstances relative to the best practices listed in this document. Unique entity parameters may include, but are not limited to, legacy standards, legacy equipment, organizational structure, and maintenance practices.

1. Maintain internal performance metrics and performance goals for PS Misoperations. Create and use internal PS Misoperation cause categories and sub-categories that provide more granularity than the broader NERC PRC-004 cause categories.
2. Perform/participate in benchmarking to compare PS Misoperation performance with other entities. The new SERC PCS Composite Misoperations Performance metric is one benchmarking metric available (September 21, 2016) to SERC entities. *(References #6 and #7)*
3. Participate in industry peer reviews, working groups, or other industry formats where best practices from various perspectives are discussed in order to stay abreast of industry protection issues, relay applications and technology issues.
4. Review industry NERC Lessons Learned documents involving PS Misoperations for potential applicability. NERC Lessons Learned documents are developed from the NERC Event Analysis process. *(Reference #4)*
5. Review event records, fault records and relay data to verify correct functionality of communications assisted protection schemes following faults on lines that utilize high speed tripping, even if the Composite PS provided high speed clearing. (Faults may be cleared high-speed by other protection elements, thereby masking problems in the communications assisted protection scheme.)
6. Validate the fault study model's indicated currents and voltages with actual event data from faults of known locations. *(References #3 and #9)*
7. Review all Misoperations for potential human performance elements associated with the event to ensure that mitigation techniques are used and lessons learned are communicated to minimize the risk of errors and/or implement changes in order to eliminate or reduce human error impact. Common human performance mitigation techniques include, but are not limited to; peer reviews, technical training, use of standard relay settings and protection & control design templates, independent reviews of problematic steps/settings/designs/applications. *(References #1 & #9)*

8. Ensure Protection Systems are designed for simplicity and ease of use. Consideration should be given to standardizing Human Machine Interface (HMI) designs, standardizing protection schemes and relay products used, and other solutions that reduce the likelihood of human error while maintaining/operating the Protection System. *(Reference #11)*
9. Maintain a written policy documenting the entity's process for maintaining configuration control of relay settings. *(References #9 and #22)*
10. Utilize an internal program which includes training, tools, communications, etc. that is designed to minimize human performance errors and include all relay personnel in the internal program process. *(Reference #3)*
11. Maintain and utilize internal documentation of relay settings philosophy and design standards, in order to reduce human performance errors. Internal standards should consider industry standards and guidelines. *(References #3 and #9)*
12. Document reasoning/basis when any Protection System setting is set outside of an entity's standards. *(References #3 & #9)*
13. Maintain a written policy capturing the entity's philosophy for selecting communications assisted protection schemes that addresses the need for high speed protection and the risk to the Bulk Electric System for Protection System failure modes, capturing the inherent trade-offs between dependability and security of various communication assisted schemes.
14. Design digital Directional Carrier Blocking (DCB) schemes to prevent or reduce the opportunity for carrier holes. This should include proper design of an override timer. *(Reference #5)*
15. Regular periodic maintenance should be performed on carrier coupling tuning equipment, wave traps, and spark gaps which can improve communication performance for carrier based pilot Protection Systems. (Reference #5)
16. Utilize carrier periodic check-back tests to verify the carrier equipment is operational. (Reference #5)
17. For digital relays, avoid complex designs. If additional settings or logic do not add value or have limited/no justification, do not use. Attempt to keep digital settings and designs as simply as possible without giving up adequate protection for the application. *(Reference #11)*
18. Applications requiring coordination of functionally different relay elements should be avoided. Communication assisted Protection Systems are particularly vulnerable. *(Reference #5)*
19. Design protection schemes with full redundancy, where practical, so that no single failed element will lead to a failure to trip event. Where full redundancy is not practical, the scheme should include local or remote elements that backup the entire primary zone of protection. *(Reference #10)*
20. Utilize a settings implementation process to ensure settings are accurately communicated, properly installed and tested, and confirms as-left expectations and/or any settings variances. *(Reference #9)*
21. Utilize a periodic settings review process to identify needed revisions related to network changes. *(References #1, #3 and #9)*
22. Evaluate relay firmware updates and prioritize implementation of firmware updates that correct critical protection functions. *(References #5 and #9)*
23. Proactively implement equipment replacement programs to address relay models or applications prone to Misoperation. *(Reference #1 and #3)*
24. Reduce maintenance intervals on electromechanical relays with known setting drift issues. *(Reference #3)*

25. Within two years of a Misoperation, complete mitigating corrective actions of PS Misoperations. *(Reference SERC Protection System Operations Data Reporting Procedure)*
    For all high reliability impact Misoperations, and where practical for all other Misoperations, complete extent of condition corrective actions within three years of a Misoperation.
26. Participate in the voluntary NERC Event Analysis reporting program. *(References #2 and #4)*

References:

1. NERC Staff Analysis of System Protection Misoperations, December 2015
2. State of Reliability May 2015.
3. NERC Staff Analysis of System Protection Misoperations, December 2014
4. State of Reliability May 2014.
5. NERC Misoperations Report, April 1 2013; prepared by the Protection System Misoperation Task Force, approved by NERC Planning Committee April 8, 2013.
6. SERC PCS Misoperation Data Analysis Report, February 10, 2010.
7. SERC PCS Composite Misoperation Performance metric (September 21, 2016).
8. A Reliable Power Line Carrier Based Relay System (Access restricted to SERC Registered entities).
9. "Processes, Issues, Trends and Quality Control of Relay Settings", IEEE PSRC System Protection Subcommittee Working Group C3, March 2007.
10. "Redundancy Considerations for Protective Relaying Systems", Working Group I 19 of Power System Relaying Committee of IEEE Power Engineering Society, 2010.
11. "Relay Scheme Design Using Microprocessor Relays", IEEE PSRC System Protection Subcommittee Working Group C16, June 2014

LINKS:

NERC Staff Analysis of System Protection Misoperations, December 2015
http://www.nerc.com/pa/RAPA/PA/Performance%20Analysis%20DL/2015_Analysis_of_System_Protection_Misoperations_Final.pdf

NERC, State of Reliability, May 2015
http://www.nerc.com/pa/RAPA/PA/Performance%20Analysis%20DL/2015%20State%20of%20Reliability.pdf

NERC Staff Analysis of System Protection Misoperations, December 2014
http://www.nerc.com/pa/RAPA/PA/Performance%20Analysis%20DL/NERC%20Staff%20Analysis%20of%20Reported%20Misoperations%20-%20Final.pdf

NERC, State of Reliability, May 2014
http://www.nerc.com/pa/RAPA/PA/Performance%20Analysis%20DL/2014_SOR_Final.pdf

NERC, Misoperations Report, April 1 2013, prepared by Protection System Misoperations Task Force
http://www.nerc.com/docs/pc/psmtf/PSMTF_Report.pdf

NERC, Automatic Outages Caused by Failed Protection System Equipment /Human Error
http://www.nerc.com/pa/RAPA/ri/Pages/AutomaticTransOutagesInitiatedbyFailedProtSysHErr.aspx

NERC, Protection System Misoperations
http://www.nerc.com/pa/RAPA/ri/Pages/ProtectionSystemMisoperations.aspx

NERC, Event Analysis Lessons Learned documents
http://www.nerc.com/pa/rrm/ea/Lessons%20Learned%20Document%20Library/Forms/AllItems.aspx