OPERATIONS SERIES · EC-WP-306

System Protection & Misoperations

Protection systems, misoperations, and the audit-defensible response.

Protection systems act in milliseconds, without an operator in the loop, and the rest of the system lives with the result. This reference explains what NERC counts as a Misoperation, how PRC-004-6 and MIDAS reporting work, and why misoperation patterns are among the clearest early signals of reliability risk on a changing grid.

Energy Compliance, Inc. Professional Reference

energycomplianceinc.com **OCTOBER 2026**

Disclaimer & Legal Notice

This publication is the work product of Energy Compliance, Inc. and is provided for general information and educational purposes only. It does not constitute legal advice, regulatory guidance, engineering advice, or formal interpretation of any NERC Reliability Standard, FERC order, or Regional Entity directive.

This publication may not be used or cited as authority in any audit, enforcement, regulatory, or legal proceeding. Compliance with NERC Reliability Standards depends on facts and circumstances unique to each registered entity, and the reader should consult qualified counsel and subject matter experts when making compliance decisions.

This reference was first published in June 2026. This edition reflects the standards versions, NERC Glossary definitions, and MIDAS reporting instructions in effect on October 26, 2026. Standards change; confirm the current version on nerc.com before relying on any requirement cited here.

NERC, FERC, and the names of Regional Entities are referenced here for descriptive purposes only. Energy Compliance, Inc. is not affiliated with, sponsored by, or endorsed by the North American Electric Reliability Corporation, the Federal Energy Regulatory Commission, or any NERC Regional Entity.

Energy Compliance, Inc. assumes no responsibility or liability for errors, omissions, or outcomes resulting from the use of this publication.

Foreword

This professional reference is one of a series Energy Compliance, Inc. publishes for registered entities and the people who run their compliance programs.

I've spent more than thirty years on every side of the bulk electric system. I've operated control centers as a Reliability Coordinator, Transmission Operator, and Power System Operator. I've audited grid facilities and signed off on findings as a senior compliance auditor. I've worked enforcement matters from inside the regulator's process. For the last several years I've advised registered entities directly through the firm I founded.

The entities that do reliability well share a common habit. They take the standards seriously without confusing them with reliability itself. They know that a NERC Reliability Standard is a floor, not a ceiling. They know that compliance is something an auditor evaluates, but reliability is something a system either delivers or doesn't. They prepare for audits by building programs that survive real questions, not binders that look thick.

That's the perspective these references try to share. Each one focuses on a single topic: a standard family, an operational function, a regulatory framework, or an emerging industry challenge. Each one walks through how the topic actually works.

These references are written for the compliance manager who wants to understand the system, not just memorize requirements. For the legal counsel who has to brief a board honestly. For the senior operator who's been told that compliance and reliability are the

same thing and suspects they aren't. And for the new compliance hire who got handed a binder and told good luck.

These references aren't marketing material disguised as content. They're the result of three decades of doing this work and watching it succeed and fail. I've written them in the same voice I use in a control room or in front of a Regional Entity audit team: direct, evidence-grounded, honest about what the standards do and do not require.

Energy Compliance exists because, in my experience, too much of the consulting offered to registered entities is structured for billable hours rather than for outcomes. Every engagement is overseen by a senior practitioner. We don't bring five people to a meeting that needs one. We automate the work that should be automated. We apply senior judgment to the work that requires it. If that approach matches what you're looking for in a compliance partner, the back of this reference has our contact information.

If not, the reference still belongs to you. Take what's useful. Apply it well. And remember the only test that ultimately matters: when the system needs to perform, does it?

Rob Smith

Founder and Principal, Energy Compliance, Inc.

Executive Summary

Protection systems detect abnormal conditions and isolate them. The system depends on this happening correctly. When it doesn't, the system depends on the rest of the framework to limit the damage.

The numbers say this is not a niche topic. NERC's 2026 State of Reliability report counted 1,087 Misoperations across 18,397 Protection System operations in 2025, and found that 32 of the 51 transmission-related events analyzed through the ERO Event Analysis Process that year involved misoperations. Incorrect settings and relay failures remain the most common causes. Human performance accounted for 42 percent of 2025 misoperations. On the compliance side, NERC's annual report for 2025 named PRC-005 first among the most frequently reported operations and planning noncompliance and put PRC-019, PRC-024, and PRC-025 in the same top ten. One of the three serious-risk filings that year was a PRC-023 relay loadability violation on a 500 kV circuit.

Misoperations themselves are reproducible patterns: settings that no longer match the system, coordination that was never rechecked, maintenance that slipped, a test switch left in the wrong position. That is why they matter to reliability oversight and why they matter to an audit team. The core points of this reference:

- **The definition is precise.** A Misoperation is the failure of a Composite Protection System to operate as intended. The NERC Glossary names six types and, for non-Fault operations, it excludes those caused by personnel during on-site maintenance, testing, inspection, construction, or commissioning.
- **PRC-004-6 runs on clocks.** Owners have 120 calendar days from a BES interrupting device operation to decide whether their Protection System caused a Misoperation, and 60 calendar days from identifying a cause to produce a Corrective Action Plan or a declaration. The CAP must include an evaluation of whether the fix applies to other Protection Systems and locations.
- **Reporting is a separate track.** MIDAS reporting is a Section 1600 data request, due quarterly within 60 days of each quarter's end. It feeds industry analysis. It is not the same thing as a PRC-004 compliance record, and a program needs both.
- **Patterns carry the signal.** One misoperation tells you about one relay. A cluster tells you about a settings process, a commissioning practice, or a system that has changed underneath its protection.
- **The grid is changing faster than many settings files.** New Generator Owners, new inverter-based resource standards that took effect October 1, 2026, and shifting fault current levels all move the assumptions protection was coordinated against.

- **The standards prescribe process, not design.** Nobody tells an owner which relay to buy or what to set it to. The standards do tell owners how fast to find a Misoperation, how to fix it, how often to maintain and coordinate, and what loadability margins to hold.

> **From the Field**
>
> Protection misoperations don't always cause outages. But they always cause questions, and in my experience, questions in an investigation tend to become findings. I've also watched programs that treat protection as installed-and-forgotten see those findings escalate over time. A protection scheme that operated correctly during the contingency wasn't lucky. It was engineered, set, tested, and maintained for that exact moment.

Chapters 1 and 2 establish what protection systems do and what a Misoperation is. Chapter 3 covers PRC-004-6 and MIDAS. Chapters 4 through 8 work through risk, oversight, organizational boundaries, the changing grid, and pattern recognition. Chapters 9 through 12 set misoperations against reliability objectives and real events, correct a common misreading of how "non-prescriptive" the framework is, and pull the threads together.

1 The Role of Protection Systems in Bulk Electric System Reliability

1.1 What This Reference Covers

This reference looks at protection system misoperations from the reliability side of the house. It covers how NERC defines a Misoperation, how misoperations are identified, corrected, and reported, and why consistent identification and analysis matter to reliability oversight. It ties protection performance to the reliability functions that depend on it: fault isolation, system stability, and coordination across separately owned systems. It also covers the data that the industry gathers and shares so that protection performance can be judged across the whole system rather than one substation at a time.

Protection performance depends on more than the relay. Design, settings, maintenance and testing, system conditions, human error, and the operating procedures and controls around the equipment all affect the likelihood that a Protection System will misoperate. This reference treats all of them as part of the subject.

It is written for management, compliance, planning, operations, and engineering staff. Those roles are often asked to discuss protection at an operational level. Many people in them have a working knowledge of protection within their own organization's practices but have never seen how protection performance is measured against the Reliability Standards their organization is held to. The goal is a common vocabulary across those groups. This reference does not prescribe protection designs, settings, or operating practices.

1.2 Selective Fault Isolation

Protection systems are a basic reliability tool on the Bulk Electric System (BES). Their job is to detect abnormal conditions and act automatically to isolate faulted equipment, limit damage, and keep the rest of the interconnected system in reliable operation. They are local in nature and act in milliseconds, yet their cumulative effect shapes system-wide reliability across many substations, geographic areas, and owners.

When we judge protection from a reliability standpoint, the elegance of the design is not the point. What matters is that the protection system performs its function across a very large number of possible system configurations. That function is selective fault isolation. When a fault occurs, the protection system is expected to isolate the faulted component or section and keep as much of the rest of the system in service as possible. Done right, it preserves stability and keeps a disturbance from becoming a reliability problem.

1.3 Automatic by Design

Protection systems differ from other reliability controls in one important way: they act without waiting for an operator or another control system. Their performance is fixed in advance by design, settings, maintenance, and testing, and their action happens automatically. That is both their greatest strength and their greatest exposure. When they work, nothing responds faster. When they don't, they can hurt the system in two opposite ways:

- They can fail to act, or act too slowly, when their operation is needed, so the fault they exist to clear stays on the system longer than planning and operating studies assumed.
- They can act when they shouldn't, removing healthy equipment from service and changing the system's topology in an instant.

Either failure can then set up a second problem. Seconds later, the resulting stress on the remaining system can cause other equipment to trip, and the disturbance grows well beyond the initial fault.

1.4 A Shared, Interconnected Function

Protection on the BES operates in a coordinated environment. One registered entity's facilities are electrically connected to another's, and a protection action in one place can quickly affect large parts of the system across organizational and jurisdictional boundaries. The reliability dependency is not local.

The standards recognize this directly. The NERC Glossary defines a Composite Protection System as the total complement of Protection Systems that function collectively to protect an Element, and the Misoperation definition is built on that composite view. PRC-004-6 requires an owner whose BES interrupting device operated to notify the other owners that share the Composite Protection System when a Misoperation occurred or cannot be ruled out, and the owner has found that its own components did not cause the operation or cannot tell whether they did. PRC-027-1 requires owners whose settings protect Elements that electrically join separately owned Facilities to exchange proposed settings and resolve coordination issues before those settings go in. Protection performance is a question of collective risk, not of one component in isolation.

1.5 What the Standards Define and What They Leave to Engineering

Current NERC Reliability Standards on protection do not prescribe the detailed design of protection systems. They define expected performance, the process for finding and correcting Misoperations, maintenance programs, coordination processes, and specific loadability criteria. The table lists the protection standards this reference relies on, all in effect on October 26, 2026.

Standard	What it requires, in brief	Ch.
PRC-004-6, Protection System Misoperation Identification and Correction (effective April 1, 2021)	Identify Misoperations within 120 calendar days; notify co-owners; develop a CAP or declaration within 60 calendar days of identifying a cause; implement each CAP	2, 3, 8, 11

Standard	What it requires, in brief	Ch.
PRC-005-6, Protection System, Automatic Reclosing, and Sudden Pressure Relaying Maintenance (effective January 1, 2016)	Documented and implemented maintenance programs so Protection Systems are kept in working order	5, 11
PRC-027-1, Coordination of Protection Systems for Performance During Faults (effective April 1, 2021)	A settings process so Protection Systems operate in the intended sequence during Faults, with coordination studies at least every six calendar years, or on a 15 percent fault current trigger within that same limit	6, 7, 11
PRC-023-6, Transmission Relay Loadability (effective April 1, 2024)	Protective relay settings that do not limit transmission loadability and still detect fault conditions	11
PRC-030-1, Unexpected Inverter-Based Resource Event Mitigation (effective October 1, 2026)	Generator Owner process to identify, analyze, and mitigate unexpected changes in IBR output	7
PRC-029-2, Frequency and Voltage Ride-through Requirements for Inverter-Based Resources (effective October 1, 2026, replacing PRC-029-1)	Ride-through performance for BES and qualifying non-BES IBRs	7

The design and the settings remain the owner's. The outcomes, and the process for learning from bad outcomes, are what the framework watches.

1.6 Intent Versus Outcome

Two ideas run through the rest of this reference. Protection intent is what the Composite Protection System was supposed to do for a given condition. Protection outcome is what it actually did. Reliability oversight cares most about the gap between the two when that gap affects reliability.

Protection also interacts with system operations, planning, and asset management. Protection schemes are built on assumptions drawn from planning models and expected configurations. Real operation departs from those assumptions through topology changes and abnormal conditions, and over time changes in generation, load patterns, and system configuration change fault characteristics and relay behavior.

Protection is one layer in a defense-in-depth strategy. It is not expected to prevent every disturbance or make up for every shortcoming elsewhere in the system. It is expected to operate predictably and as intended, every time. When it doesn't, the risk does not stay with the original fault.

End-of-Chapter Summary

Protection systems are a reliability control on the BES because they provide fast, automatic fault detection and isolation that preserves stability and limits disturbances. They operate locally and without operator intervention, but their performance has wide-area consequences because the system is interconnected and separately owned protection works as a composite.

From a reliability view, protection is judged by outcome, not by design features. The gap between protection intent and protection outcome is what makes a misoperation a source of reliability risk, and the speed and autonomy of protection is what lets a local misoperation escalate quickly. The chapters that follow treat misoperations as reliability indicators and work through how they are defined, identified, corrected, and analyzed.

2 Protection System Misoperations as a Reliability Concept

2.1 The Definition

Protection system misoperations are a serious reliability concern. On the BES they are not treated as a single relay behaving oddly. They are treated as events that can affect stability, coordination, and the system's ability to confine a disturbance. Understanding them as a reliability concept starts with the definition.

The NERC Glossary defines a Misoperation as the failure of a Composite Protection System to operate as intended for protection purposes, and lists six types:

Type	During Fault	Other Than Fault
Failure to Trip	Fails to operate for a Fault it is designed to clear	Fails to operate for a designed non-Fault condition, such as a power swing, undervoltage, overexcitation, or loss of excitation
Slow Trip	Operates slower than required, and the delay caused at least one other Element's Composite Protection System to operate	Same test, for a designed non-Fault condition
Unnecessary Trip	Operates unnecessarily for a Fault on another Element	Operates unnecessarily for a non-Fault condition

Three details in the definition do a lot of work. First, the test is the composite. The failure of one Protection System component is not a Misoperation for the two Failure to Trip types as long as the Composite Protection System performed correctly. Second, a Slow Trip counts only if the delay caused another Element's protection to operate. Third, the personnel exclusion is narrower than it is often read. It sits in the sixth type, Unnecessary Trip, Other Than Fault: an operation for a non-Fault condition caused by personnel during on-site maintenance, testing, inspection, construction, or commissioning is not a Misoperation. It is not a blanket exclusion across all six types, and PRC-004-6 says it stops applying once the on-site activity is complete.

2.2 Outcome Over Design Intent

The definition judges what happened, not what the designer meant. That keeps the reliability framework out of decisions about protection technologies and methods. Misoperations range from unintended trips, to failures to trip for a fault, to tripping the wrong Element, to slow clearing that drags other protection into the event.

The technical cause matters for the correction. For reliability, the concern is the system impact. A misoperation can change topology in a way that removes important Elements from service. Another can leave a faulted Element energized longer than the system can tolerate.

2.3 Milliseconds Versus Operator Time

The reliability impact of a misoperation depends on timing and system conditions. The effects of a protection action arrive before any operator knows a disturbance is underway, and they cannot be undone in the moment. That makes misoperations different from most other reliability events. The protection action happens in milliseconds, but the conditions it creates can take seconds or minutes to develop, and an operator then has to recognize them and act.

2.4 Misoperations and Cascading

The Glossary defines Cascading as the uncontrolled successive loss of System Elements triggered by an incident at any location, resulting in widespread interruption that cannot be restrained from spreading beyond an area predetermined by studies. Misoperations are central to understanding Cascading because they can create the conditions for it. An unnecessary or poorly coordinated protection response can overload equipment that is still in service, push power in unintended directions, and erode reserves. A failure to operate can let a disturbance persist and produce equipment damage, unstable swings, and further protection operations at remote points.

The Guidelines and Technical Basis of PRC-004-6 open with the problem NERC described in a January 7, 2011 letter from its then President and CEO: "Nearly all major system failures, excluding perhaps those caused by severe weather, have misoperations of relays or automatic controls as a factor contributing to the propagation of the failure." The same letter observed that relays most commonly fail to operate correctly because of incorrect settings, improper coordination, ineffective maintenance and testing, or failures of communications channels or power supplies.

2.5 Small Consequences Still Count

From the oversight perspective, a misoperation is not judged by whether a major disturbance followed. The protection response is checked against what was required for the condition. A Misoperation exists when the Composite Protection System did not perform as intended, even if nothing much happened as a result. A minor consequence today does not excuse the event, because the same behavior under different conditions could be serious. That forward-looking stance is what risk-based oversight means in practice.

Consistent identification and classification matter for the same reason. Standardized definitions let misoperations be compared and aggregated across owners, control areas, and regions over time. Aggregated, they tell you about system reliability. Treated one at a time as equipment incidents, they mostly don't.

2.6 Not a Finding of Fault

Calling an event a Misoperation is not a finding that anyone was negligent. Misoperations are events with identifiable causes in protection design, settings, system operating characteristics, configuration, maintenance, or procedure. Treating them that way keeps the analysis objective.

Misoperations live in the space between what the design team assumed and how the power system actually behaves. Configuration changes, new generation, changing fault characteristics, and changed operating procedures all move the system away from those assumptions. That gap is widening as the grid changes, which is why misoperations belong in the reliability conversation and not only in the protection engineering one.

> **From the Field**
>
> A misoperation traceable to settings drift is traceable to a process gap. The standards expect the process to catch the drift. The useful question about a misoperation is not only what the relay did. It's what the organization knew about that relay before it did it.

End-of-Chapter Summary

Misoperations are defined precisely in the NERC Glossary: six types, judged at the Composite Protection System, with an exclusion, within the non-Fault Unnecessary Trip type, for operations caused by personnel during on-site work. For reliability purposes they are risk indicators, because they show protection behaving in a way that could lead to instability, loss of synchronism, or failure to contain a disturbance.

A practical way to weigh a misoperation's reliability significance is along three lines: how quickly its effects arrive, how far its system impact extends, and how much it adds to the potential for Cascading. Chapter 3 turns from concept to mechanics: how misoperations are identified, corrected, and reported.

3 Misoperation Identification, Classification, and Reporting Frameworks

3.1 Two Tracks: Compliance and Data

Identification and classification are what turn misoperations from random events into a reliability signal. In the NERC framework that work runs on two tracks that people often confuse.

The first is compliance. PRC-004-6 is a mandatory Reliability Standard. It applies to Transmission Owners, Generator Owners, and Distribution Providers, and it sets deadlines for identifying Misoperations and for correcting their causes. Missing those deadlines is a violation.

The second is data. NERC collects Protection System operation and Misoperation data through the Misoperation Information Data Analysis System (MIDAS) under a data request issued pursuant to Section 1600 of the NERC Rules of Procedure. Reporting is mandatory for U.S. registered Transmission Owners, Generator Owners, and Distribution Providers. The data feeds NERC and Regional Entity trend analysis. The Rules of Procedure state that Section 1600 does not apply to requirements in a Reliability Standard, and does not apply to data requested in connection with a compliance or enforcement action. The two tracks are related, but they are not the same obligation, and a program needs both.

3.2 PRC-004-6: Identification and Notification

PRC-004-6 starts the review from the operation of a BES interrupting device, typically a circuit breaker or circuit switcher. The breaker mechanism is not part of the Protection System, but its operation by a Protection System is what opens the clock.

Requirement	Trigger	Deadline
R1, identify	BES interrupting device operated by a Protection System, or by manual intervention in response to a Protection System failure to operate, where the owner owns all or part of the Composite Protection System, and the owner identified that its Protection System component(s) caused the operation, or that it was caused by manual intervention in response to its Protection System failure to operate	120 calendar days from the operation
R2, notify	Shared Composite Protection System, Misoperation occurred or cannot be ruled out, and the cause is not, or cannot be shown to be, the owner's components; or backup protection operated for another entity's Element	120 calendar days from the operation

Requirement	Trigger	Deadline
R3, identify after notice	Notification received under R2	Later of 60 calendar days from notification or 120 calendar days from the operation
R5, correct	Owner's Protection System components caused the Misoperation	60 calendar days from first identifying a cause
R6, implement	Each CAP developed under R5	Implement, and update when actions or timetables change, until complete

The Violation Severity Levels for R1 and R2 step up at 150, 165, and 180 calendar days. The deadline is not a target to aim for. It is the point where the compliance record starts working against you.

3.3 PRC-004-6: Correction

Requirement R5 is where the standard stops being about paperwork. Within 60 calendar days of first identifying a cause, the owner of the Protection System components that caused the Misoperation must do one of two things:

- Develop a Corrective Action Plan for the identified components, together with an evaluation of the CAP's applicability to the entity's other Protection Systems, including other locations; or
- Explain in a declaration why corrective actions are beyond the entity's control or would not improve BES reliability, and that no further corrective actions will be taken.

Requirement R6 then requires the owner to implement each CAP and update it if actions or timetables change, until it is complete. The Glossary defines a Corrective Action Plan as a list of actions and an associated timetable for implementation to remedy a specific problem.

The earlier version's Requirement R4, which required continued investigative action on Misoperations of unknown cause, was retired in PRC-004-6 under NERC's Standards Efficiency Review. Retiring the requirement did not retire the reliability problem. An unknown cause is still an unknown cause, and Chapter 5 shows that the "unknown" share of misoperations is one of the things NERC's analysts watch.

3.4 Applicability and Exclusions

PRC-004-6 applies to Protection Systems for BES Elements, plus UFLS and UVLS intended to trip one or more BES Elements. It excludes non-protective functions embedded in a Protection System, protective functions intended to operate as a control function during switching, Special Protection Systems and Remedial Action Schemes, and Protection Systems of individual dispersed power producing resources under BES Inclusion I4 where the Misoperations affected an aggregate nameplate rating of 75 MVA or less of BES Facilities. Those exclusions matter at wind and solar plants. An owner should know, in writing, which of its operations fall inside the standard and why.

3.5 MIDAS Reporting

The 2026 MIDAS Data Reporting Instructions took effect January 1, 2026. Three kinds of submissions are required:

- Composite Protection System Operation Summary data, quarterly when reportable operations occur, aggregated by facility voltage;
- Misoperation data, quarterly when reportable Misoperations occur, including BES Composite Protection Systems in temporary non-BES configurations; and
- An Opt-Out Waiver in quarters with no Protection System operations, or with operations but no Misoperations.

Data are due within 60 days after the end of each calendar quarter through the MIDAS Portal. NERC's posted deadlines are May 30 for the first quarter, August 29 for the second, November 29 for the third, and March 1 for the fourth quarter and for any updates to the prior year, extended to the next business day when a deadline falls on a weekend or holiday. Newly registered entities are expected to begin reporting when registration becomes effective, and to backfill data delayed by administrative setup.

MIDAS asks for cause codes, including As-left Personnel Error, Communication Failures, Design Errors, Incorrect Settings, Logic Errors, Relay Failures/Malfunctions, AC System, DC System, Other/Explainable, and Unknown/Unexplainable. Those categories are what make the industry data comparable. They also give an owner a ready-made vocabulary for its own cause analysis.

3.6 Why Consistency and Evidence Matter

Reporting serves two audiences. Inside the entity, it tells management how its protection is performing and how big its problems are. For NERC and the Regional Entities, it supports trend analysis, shows which problems recur, and helps decide whether new problems need action. Reporting procedures need enough detail to be useful and enough consistency to be comparable across the system. Timeliness matters because misoperation information describes a moment on the system, and accuracy matters because bad data aggregates into bad conclusions.

On the compliance side, PRC-004-6 expects dated evidence. The measures list the kinds of documentation that qualify: reports, databases, spreadsheets, emails, logs, declarations, sequence-of-events analyses, relay targets, Disturbance Monitoring Equipment records, test results, transmittals, and for R6, records of each CAP's implementation and revision history, which may include work orders and maintenance records. Evidence for R1 through R3 must be retained for at least 12 calendar months after each requirement is completed, and evidence for R5 and R6 for at least 12 calendar months after each CAP, evaluation, or declaration is completed, unless the Compliance Enforcement Authority directs longer.

> **From the Field**
>
> Treat PRC-004 as a clock problem as much as an engineering one. Knowing what the relay did is not enough. The determination needs a date on it, the owner at the other end of the line needs to be told when R2 applies, and the CAP needs to exist on paper well before day 60.

End-of-Chapter Summary

Identifying, classifying, and reporting misoperations is what lets them be treated as a reliability issue rather than as isolated events. PRC-004-6 sets the compliance clock: 120 days to identify, 60 days from a cause to a CAP or declaration, and implementation until complete. MIDAS sets the data clock: quarterly submissions within 60 days of quarter-end, with standardized cause codes.

The two tracks have different purposes and different legal footing. Programs that merge them in their own minds tend to do one well and the other late. Structured, consistent data is what allows industry-wide learning about protection risk.

4 Reliability Risk Implications of Protection System Misoperations

4.1 Unintended Topology Change

The consequences of a misoperation can run well beyond the instant of the event. When we evaluate a misoperation, we look not only at the immediate impact but at what it did to stability, coordination, and disturbance containment, and at how the same behavior would play out under more stressed conditions.

One of the largest risks is an unintended change in topology. An Unnecessary Trip removes lines, transformers, generators, or other equipment when no action was needed. Those removals shift power flows, load the remaining equipment more heavily, and reduce the margin available for the next contingency. A misoperation that does not cause instability in the moment can still leave the system more exposed to whatever comes next.

4.2 Slow and Failed Clearing

The opposite failure is protection that does not clear a fault when and as it should. A Failure to Trip or a Slow Trip during a Fault means the fault stays on longer than planning and operating models assumed. Longer clearing times stress equipment thermally, depress voltages, and push the system toward instability. They also pull other protection into the event. By the Glossary's own terms, a Slow Trip is a Misoperation precisely when its delay caused another Element's protection to operate. Each added operation widens the disturbance and raises the odds of a cascade.

4.3 Eroded Study Assumptions

Misoperations add uncertainty to every analysis that depends on protection. Planning studies, operating limits, operating procedures and guides, and post-disturbance analysis all assume that protection clears faults selectively and on time. Unexpected or erratic operation undercuts those assumptions. The uncertainty does not stay in real time; it reaches back into the studies that set the limits the control room runs on.

4.4 Conditions at the Time

The impact of a misoperation depends on the state of the grid when it happens. The same misoperation that causes little trouble at light load with healthy margins can cause much more under heavy load, low margin, or an outage already in place. Reliability analysis judges a misoperation against the circumstances of the event, and asks what it would have done under worse ones.

4.5 Situational Awareness

Misoperations also cost the operator situational awareness. An operator's understanding of the system is built on expected behavior. Operators are expected to understand why an alarm came in, why the system state changed, and what sequence of events is unfolding. Unexpected protection actions break that understanding, especially during a disturbance when events move in real time and the operator has to respond quickly. The loss of awareness is a separate source of risk, on top of the physical effect of the misoperation.

4.6 Propagation Across Boundaries

Because the BES is interconnected, the risk is magnified. A protection operation at one point can disturb neighboring systems across geographic and ownership boundaries. A misoperation in one place can propagate, challenge relays elsewhere, and raise the chance of secondary misoperations or interactions between schemes. Misoperations have to be judged in the context of the whole system's reliability.

4.7 Misoperations as Risk Indicators

NERC does not assume every misoperation leads to harm. It treats misoperations as indicators of exposure. Recurring misoperations can point to a system vulnerability and can be an early warning that a more severe event is possible under different conditions. That probabilistic view fits risk-based oversight, which focuses on the conditions that can produce rare, high-consequence events.

NERC makes this concrete with its misoperation impact score, which estimates the impact of each misoperation on the BES by summing weighted values for facility voltage class, equipment type, cause, and category. The score runs from a minimum of 0.3034 to a maximum of 1.0. In the 2026 State of Reliability report, NERC found a statistically significant increase in the average impact score for 2025, both NERC-wide and in the Texas RE region, compared with the prior four years.

End-of-Chapter Summary

Protection system misoperations create reliability risk by changing system configuration, by extending the time a fault stays on the system, and by departing from the behavior the system was planned around. They raise vulnerability under stressed conditions by reducing margin and adding uncertainty, and they degrade operator situational awareness.

Reliability oversight looks at misoperations in their operating and system context, and at consequences that may not be obvious at first. That is why misoperation data is a focal point of reliability monitoring even when the direct consequences of most individual events are small.

5 Oversight, Analysis, and Industry Learning from Misoperations

5.1 What the Data Shows

NERC's oversight of misoperations runs on aggregated data, technical analysis, and lessons drawn from events. It does not require prescribing designs. It requires seeing system performance and the patterns that point to new or systemic issues.

NERC's 2026 State of Reliability report, published June 24, 2026, gives the current picture. Across all Regional Entities, misoperations fell from 1,172 in 2021 to 1,153 in 2022, 1,118 in 2023, 1,089 in 2024, and 1,087 in 2025, against 17,454, 17,804, 17,871, 19,325, and 18,397 Protection System operations in those years.

The 2025 count was the lowest in five years. NERC found a statistically significant decreasing trend in the misoperation rate for MRO, and no statistically significant trend for the other Regional Entities or for the ERO as a whole. Incorrect settings and relay failures/malfunctions remained the most common causes. Human performance accounted for 42 percent of 2025 misoperations: 22 percent Incorrect Settings, 11 percent As-Left Personnel Error, 5 percent Logic Errors, and 4 percent Design Errors. The report also noted a relative rise in Unknown/Unexplainable causes from 2024 to 2025, and observed that this category historically shrinks as investigations continue and corrective action plans address the underlying conditions.

5.2 Misoperations in Analyzed Events

The same report looked at events reported through the ERO Event Analysis Process. Of 51 transmission-related events in 2025, 32, or 63 percent, involved misoperations. In 2024, 34 of 60 transmission-related events, or 57 percent, did. The share went up while the total counts went down, and NERC said the reduction is likely attributable in part to ERO Enterprise and industry efforts through task forces, workshops, and analysis. NERC cautions that Event Analysis and MIDAS data are different datasets and should not be read as one series.

5.3 Patterns Over Single Events

A single misoperation can look unimportant. Viewed as a pattern, misoperations tie back to assumptions built into protection schemes, to system changes made since those schemes were set, and to interactions between facilities. Taken together they reveal far more about risk than any single event review.

Oversight analysis focuses on frequency, incidence, and circumstances more than on the technical cause of each event. It looks for conditions that justify a closer look: rising counts of a particular misoperation type, repeat misoperations at the same facility, or similar misoperations across entities and areas. That analysis can show the extent and nature of a risk before a

significant disturbance makes it obvious. The Texas RE impact-score finding discussed in Chapter 7 is an example.

5.4 Industry Learning

Industry learning is one of the main products of oversight. Misoperation findings show up in State of Reliability reports, technical reports, lessons learned, workshops, and industry discussion. These products inform; a lessons learned document is not a Reliability Standard. They raise awareness of observed trends and give owners context. The framework supports voluntary, industry-wide improvement alongside the mandatory requirements.

5.5 Consistency and Candor in Reporting

Oversight depends on a shared understanding of what a Misoperation is and how it is reported. Inconsistent classification distorts the data and hides real trends, so oversight puts a premium on clarity, consistency, and transparency. In my view, the reliability of misoperation data is its greatest value for learning and risk identification.

How misoperations are treated also shapes how they get reported. In my view, an organization that sees every misoperation as a potential penalty will be tempted to classify borderline events out of the data. That is a mistake. The definitions decide what is a Misoperation, not the owner's comfort level, and a misoperation classified out of the data is one that never gets a CAP.

5.6 A System in Motion

The BES is changing quickly: the resource mix, the share of power electronics, system configuration, and operating practices. As it changes, monitoring and learning matter more. Misoperation analysis is one of the earliest tools for seeing how those changes stress protection, and an early indicator of reliability issues that may be coming. Chapter 7 takes up that theme directly.

End-of-Chapter Summary

NERC uses aggregated misoperation data to find trends and issues that individual events do not show. The current data show about 1,100 misoperations a year across roughly 17,500 to 19,300 Protection System operations, with incorrect settings and relay failures leading the causes and human performance behind about four in ten.

Industry learning from that analysis builds a common awareness of protection risk across transmission and generation, while keeping each function's responsibilities clear.

6 Boundaries Between Protection Engineering, Operations, and Reliability Oversight

6.1 Three Functions, One Event

Protection system misoperations happen at the interfaces between several functions: protection engineering, real-time operations, maintenance, and reliability monitoring. Defining those interfaces clearly is necessary for identifying misoperations correctly and for making sure the reliability framework tracks the right things. When the interfaces blur, engineering decisions get mistaken for reliability criteria, and reliability monitoring gets used for things it was never meant to do.

6.2 Protection Engineering

Protection engineering covers the design, application, and performance of protection systems: protection philosophy, relay settings, and coordination assumptions. It is highly technical, involves a large measure of engineering judgment, and depends on the physical characteristics of the equipment and the network. Under the reliability framework, the design and the settings values remain the owner's responsibility.

The standards do reach the engineering function, but through process. PRC-027-1 requires each Transmission Owner, Generator Owner, and Distribution Provider to establish a process for developing new and revised settings so that Protection Systems operate in the intended sequence during Faults, including a review and update of short-circuit model data and a review of the developed settings. It does not tell the engineer what the settings should be.

6.3 Real-Time Operations

Operations covers the real-time work of keeping the system stable under normal and abnormal conditions. Protection acts as an automatic barrier that responds faster than any operator could. In most cases the operator has no influence over what protection does during an event. What the operator does inherit is the result. Misoperations can put the system into a state the operator did not expect, has to understand quickly, and has to control under high uncertainty.

6.4 Reliability Oversight

Reliability oversight is neither design nor operations. It asks how protection behaved from a system reliability perspective and whether that behavior supported reliability. It does not ask whether the scheme was designed well or whether a different design would have prevented the misoperation. It asks what actually happened and what it meant for the BES.

Keeping these roles separate protects the integrity of each. The reaction to a misoperation often starts with a search for the technical cause and someone to blame. Technology is essential to engineering and asset management, but reliability assurance is a pattern, trend, and risk function, not a technical exercise. Looking back at a misoperation should not prejudice a fair assessment of its impact.

6.5 Where the Boundaries Meet in PRC-004

PRC-004-6 is where the three functions meet on paper. Engineering usually finds the cause. Operations and the event record supply the sequence of events, the relay targets, and the disturbance records. Compliance owns the clock, the notification to co-owners, and the dated evidence. The CAP belongs to whoever owns the components that caused the Misoperation, and its evaluation of other Protection Systems and locations usually needs engineering and asset management together.

The handoffs between those groups are where the clock is most exposed. In my view, a clear, written assignment of who decides, who documents, and who notifies, with dates, is worth more than any spreadsheet.

6.6 A Shared Vocabulary

Clear boundaries make communication between departments work. Describing misoperations in reliability terms lets people separate design improvement discussions from discussions of system risk. It also lets audits and regulatory reviews be seen as additive to engineering and operations work rather than as a constraint on it.

The standards and guidance focus on what must be recorded and analyzed, not on how protection is designed or operated, and Chapter 11 takes that point up in full.

End-of-Chapter Summary

Protection system misoperations occur where engineering, operations, and reliability meet, and clear boundaries are needed to analyze them objectively. Engineering owns design and settings. Operations owns real-time response to what protection does. Reliability oversight owns the system-wide view of what misoperations mean for risk.

The framework reaches engineering through process requirements such as PRC-027-1 and PRC-004-6, and clear boundaries between the functions make learning, interpretation, and balanced risk management possible.

7 Evolving System Conditions and Emerging Misoperation Risk

7.1 A Moving Target

The reliability risk of protection system misoperations is not static. Advances in technology and changes on the BES create operating conditions that can invalidate the assumptions behind protection philosophies and lead to unexpected protection behavior. Overseeing reliability on a changing system requires understanding how those changes affect misoperation risk.

7.2 The Changing Resource Mix

The change in generation connected to the BES is one of the largest forces acting on protection. Changes in the resource mix, operating conditions, and fault characteristics change how the system behaves during faults. Much existing protection was specified and coordinated against the system as it used to be. When the changes show up in an actual disturbance, protection meets conditions its original coordination did not anticipate.

The standards now reflect that change in several places. PRC-029-2 and PRC-030-1 took effect on October 1, 2026, setting ride-through requirements for inverter-based resources and requiring Generator Owners to identify, analyze, and mitigate unexpected changes in IBR output. PRC-030-1 is worth a careful read alongside PRC-004-6. Its Requirement R1 excludes from the PRC-030 process any Real Power reduction due solely to a Protection System Misoperation being analyzed and corrected under PRC-004. An IBR owner therefore has to decide, event by event, which standard's process the event belongs in, and has to be able to show why.

The 2026 State of Reliability report traced the Texas RE region's higher misoperation impact score primarily to more misoperations reported by new Generator Owners, more misoperations on 345 kV equipment, and use of the "unknown" cause code. My read is that new entrants bring new protection, new commissioning practices, and in many cases their first experience with PRC-004 and MIDAS.

7.3 Topology and Temporary Configurations

Changes in system topology also move misoperation risk. New transmission projects, replacement of aging lines and transformers, and temporary configurations for maintenance all change fault currents, impedances, and loading, which are the quantities protection is designed around. PRC-027-1 builds this into its periodic requirement: an owner may either perform a coordination study at least every six calendar years, or compare present fault currents against a baseline and perform a study when the comparison shows a deviation of 15 percent or more,

within the same six-year limit. The 15 percent trigger exists because fault current changes break coordination.

Temporary configurations add stress to design assumptions. MIDAS reporting reaches BES Composite Protection Systems in temporary non-BES configurations for the same reason. When protection performance becomes more variable under unusual configurations, problems can start to show up beyond a single facility.

7.4 Complexity

Modern protection systems have more communication interfaces, more sophisticated algorithms, and more interdependent elements. Added sophistication can improve performance, but it also creates interactions that nobody anticipated, and some of those interactions surface as misoperations. Misoperations can reveal interactions that design reviews did not catch. The MIDAS cause and sub-cause codes reflect this, with categories for communication failures, user-programmed logic errors, and failure to update firmware.

7.5 Operating Practices

Operating practices also affect misoperation risk. Changes in dispatch, in the direction of power flow, and in contingency handling all change the conditions protection operates in. Operators do not cause protection to act, but their decisions shape the environment protection sees. Reliability oversight therefore considers operating conditions when it reads misoperation trends.

7.6 Reading the Flags

Emerging risks are often first seen in individual events, but the underlying signal is usually a change in misoperation characteristics: more occurrences of a particular type, a change in the circumstances in which they occur, or similar misoperations appearing at other entities. Those changes can mean that the assumptions behind correct protection performance no longer hold. Oversight uses these flags to raise awareness and prompt investigation, not to assign root cause or liability on the spot.

A changing system makes a risk-based approach to misoperations more important, not less. Misoperations are a dynamic proxy for how protection will behave on a system that keeps changing, and the framework has to adapt as technologies and operating practices do.

End-of-Chapter Summary

The evolving BES is changing misoperation risk by undermining assumptions about generation, configuration, and fault behavior, and by adding complexity. New IBR standards effective October 1, 2026 and the arrival of new Generator Owners make the interaction between protection and the rest of the plant a live compliance question as well as a reliability one.

NERC and the Regional Entities watch grid performance and use misoperation trends to spot new risks as the system develops.

8 Systemic Risk, Pattern Recognition, and Reliability Context

8.1 From Events to Patterns

Systemic risk is one of the main things misoperation data can reveal. One misoperation on one piece of equipment may look minor. A series of them over time can reveal vulnerabilities in the BES. This side of reliability monitoring depends on detecting patterns and understanding context, so that each misoperation is read for what it says about the larger system.

Systemic risk shows up when similar misoperations occur in many places and times, across locations, systems, owners, or regions, or cluster under similar system conditions. That suggests causes rooted in broad assumptions, system characteristics, or common practices rather than in a single component or design. A single failure tells you little. The pattern can tell you a great deal.

8.2 PRC-004 Already Asks the Systemic Question

PRC-004-6 builds pattern thinking into the requirement. A CAP under R5 must come with an evaluation of its applicability to the entity's other Protection Systems, including other locations. That is an extent-of-condition review. If an incorrect setting came from a template, the template is in other relays. If a commissioning step was missed, it was probably missed at the next site too. In my view, an evaluation that says "not applicable" without showing the search is the weakest thing a CAP package can contain.

8.3 Consistent Data Makes Patterns Visible

Pattern recognition depends on consistent classification and reporting. Without uniform definitions and outcome-based categories, nobody can tell whether an event is an anomaly or part of a trend. Oversight uses consistent data to find whether certain types of misoperations are increasing, whether they occur under particular conditions, whether they relate to changes in design or operations, and whether they signal reliability stress.

8.4 Context

Several misoperations during unusual system conditions, heavy load, or extreme events may show sensitivity to those conditions rather than a general performance problem. Misoperations spread across a range of normal conditions point to a different kind of problem. The circumstances of repeated misoperations have to be part of any oversight analysis.

Systemic analysis also looks at interactions between protection and other reliability functions. Misoperations that occur when situational awareness is degraded or margins are thin have a larger effect on reliability. A misoperation can trigger or contribute to a larger disturbance even

when the Element that misoperated did not itself lose much load. Those interactions have to be understood to judge what a misoperation means.

8.5 Patterns Are Warnings, Not Verdicts

Patterns in reliability data do not prove cause and effect. They are warning signs that may warrant investigation, discussion, or industry awareness. Treating them with appropriate caution lets them educate without prejudging technical or procedural failure.

Industry-wide visibility gives everyone a common dataset to test observations against. It can confirm or challenge what one entity sees in its own system, and it reveals trends that are hard to see from any single piece. The interconnected nature of the system is the reason that system-wide view matters.

End-of-Chapter Summary

Systemic reliability risk from protection system misoperations is mostly a matter of patterns and relationships that individual event reviews miss. Aggregated data lets reliability managers find clusters of misoperations and relationships with system conditions that point to broader risk. PRC-004-6's requirement to evaluate each CAP against other Protection Systems and locations puts that same discipline inside each owner's program.

Read in their operating and system context, misoperation patterns surface reliability concerns as they develop, and do so in a way that stays distinct from prescriptive controls.

9 Reliability Objectives, Expectations, and Performance Perspective

9.1 Judged Against Objectives

Analysts judge a misoperation against defined reliability objectives, not against an absolute standard of right and wrong. The BES does not require perfect protection performance in every conceivable circumstance. Reliability analysis asks whether protection performance supports the system's reliability objectives.

9.2 Selective, Fast Fault Isolation

The first objective is rapid, selective fault isolation. Protection must remove faulted components quickly enough that the system stays stable after the fault, while disconnecting as little as possible. Misoperations, whether an unnecessary trip or a faulted Element left connected too long, cut directly against that objective. Protection performance is judged by how well its behavior under real fault conditions meets it.

9.3 Predictability

The second objective is predictability. Reliable operation requires system behavior predictable enough to match the assumptions used in design, planning, and operating studies. Protection in particular should act in line with those assumptions. Misoperations introduce unpredictability that complicates operations during disturbances and complicates analysis afterward. Unpredictability is a risk in its own right, even when the consequences of a given misoperation are short-lived.

9.4 Coordination

The third objective is coordination. Protection operates as a coordinated system in which many devices and schemes work together to isolate faulted sections selectively. A misoperation can be the symptom of a coordination assumption that failed under a particular operating condition, a configuration change, or the complexity of overlapping relay functions. Reliability analysis looks at the effect on coordinated system behavior rather than at the coordination criteria or methods themselves. PRC-027-1 is where the standards address the coordination process.

9.5 Performance in Context

From a reliability perspective, performance is outcome-oriented and depends on the situation. Protection performance is not measured against perfection. It is measured against specific reliability objectives under the conditions the system was actually in. A misoperation during an

abnormal situation is not viewed the same way as one during normal operation. Judging performance in context gives a balanced view and avoids broad conclusions drawn from a few unusual events.

Protection is one layer among many in the reliability picture, and a misoperation on its own does not mean a site's overall reliability posture has failed. What deserves attention is a series of events at important locations, or similar events at different times, that suggest one layer of defense-in-depth is weakening. Oversight is about spotting those anomalies and early indicators and analyzing what they mean for reliability.

9.6 Expectations Evolve With the System

Performance expectations change as the system changes. As operating, technological, and system conditions change, protection performance has to be confirmed against current operating experience to be sure it still meets current reliability needs. The October 1, 2026 effective dates for PRC-024-4, PRC-029-2, and PRC-030-1 are a reminder that the expectations themselves move. Misoperations provide direct operating experience that either confirms current expectations or shows where they no longer fit.

End-of-Chapter Summary

Protection system misoperations are evaluated against three reliability objectives: selective, fast fault isolation; predictability; and coordination. Reliability monitoring uses an outcome-oriented, context-dependent assessment rather than a demand for perfect performance at all times.

Seen against the system's state when it occurred, a misoperation shows how well protection served as a layer of reliability defense, and how much the system's reliability objectives were put at risk.

10 Misoperations in the Context of Reliability Events and Disturbances

10.1 Part of the Sequence

A misoperation gets its closest scrutiny when it occurs during a reliability event or disturbance. There it can shape how the event begins, how far it spreads, and how fast the system recovers. Reliability analysis treats a misoperation as part of the sequence of events, not as an isolated occurrence.

Protection performance during disturbances is presumed to match the assumptions in contingency analysis, operating limits, and emergency plans. A misoperation can prove those assumptions wrong and leave the system in a state nobody studied. That is a material deviation, because it happens during the most stressful part of system operations.

10.2 Initiating and Secondary Misoperations

Misoperations can enter a disturbance at different points. They can help initiate an event by removing equipment unnecessarily or by failing to isolate a fault properly. Or they can occur after the initiating event, as secondary misoperations, when the system is already vulnerable. Event analysts read them in sequence and consider how timing and system conditions shaped the consequences and the risk.

A clarification is needed here, because the term is often used loosely after an event. In NERC usage, a Misoperation is a protection outcome: the failure of a Composite Protection System to operate as intended. It is not a label for an operator's decision or for a control action that turned out badly in hindsight. And the on-site work exclusion in Chapter 2 still requires the event record to explain the operation.

10.3 How Misoperations Feed a Cascade

As Chapter 2 defines it, Cascading is the uncontrolled successive loss of System Elements triggered by an incident at any location. Some removals during a disturbance are intended, such as the operation of a Remedial Action Scheme or other planned control actions. Others are not. Misoperations can hasten Cascading or worsen its consequences in several ways:

- They can increase current on the lines that remain in service and contribute to further trips.
- They can reduce the number of paths available to carry power as more Elements are lost.
- They can remove additional lines from service when the system is already unstable.
- They add uncertainty and instability at each step, increasing the likelihood that more Elements fail.

10.4 Restoration

Event analysis also looks at how misoperations affect recovery. Unexpected protection actions can cause additional outages that slow restoration, either by obscuring where the initial fault was or by changing the configuration in ways that require more corrective action. From an oversight perspective, these restoration problems are a continuation of the misoperation's risk beyond the initial disturbance.

10.5 Materiality

Not every misoperation during an event changed its outcome, and timing alone does not establish cause. To decide whether a misoperation was material, the analysis asks whether it changed the system's response, the available margin, or the actions operators had to take. Event analysis places misoperations in the context of the event so that protection behavior under stress can be judged properly. Findings are discussed in terms of system resilience, defense-in-depth, and the interaction between protection and other reliability controls. That discussion stays at the level of what happened and why it mattered.

For entities subject to PRC-004-6, the event review and the R1 identification are the same facts viewed twice. An event report that calls an operation a misoperation and a PRC-004 record that says otherwise, or the reverse, is a finding waiting to be written.

End-of-Chapter Summary

Protection system misoperations can affect how reliability events start, develop, and end. How much they matter depends on timing, system conditions, and interaction with other protection and control actions.

Reliability oversight reviews abnormal events as sequences, to determine how each element of the sequence affected risk without automatically concluding that a given misoperation caused the event. Contextual event analysis is what establishes a misoperation's real reliability consequence.

11 Reliability Oversight Without Design Prescription

11.1 What the Framework Does Not Prescribe

A central principle of the reliability framework for protection is that it does not dictate technology or design. Protection involves countless technical judgments by engineers, and the framework is built to measure system performance without second-guessing each of them, so that owners keep the flexibility to design for their own equipment and system. Reliability oversight focuses on outcomes and their consequences for reliability. There are many acceptable ways to design and set protection for a given piece of equipment, depending on its design, condition, and operating history. Oversight asks whether the resulting performance meets reliability objectives.

In my view, leaving design out is the right call: design prescriptions would be overtaken by technology and changing system conditions, and they would lock entities out of innovative or more efficient approaches suited to their circumstances. An outcome-oriented, technology-neutral approach accommodates the diversity of system designs.

11.2 What the Framework Does Prescribe

The original edition of this reference stopped there, and that leaves a reader with the wrong impression. The protection standards are non-prescriptive about design. They are quite prescriptive about process, timing, and certain outcomes:

- **PRC-004-6** requires identification within 120 calendar days, a CAP or declaration within 60 calendar days of identifying a cause, an evaluation of each CAP against other Protection Systems and locations, and implementation until complete.
- **PRC-005-6** requires documented maintenance programs for Protection Systems, Automatic Reclosing, and Sudden Pressure Relaying, implemented so those systems are kept in working order.
- **PRC-027-1** requires a settings development process and periodic coordination studies, with a six-calendar-year outer limit and a 15 percent fault current trigger option.
- **PRC-023-6** requires that protective relay settings not limit transmission loadability, while still reliably detecting fault conditions.

These requirements are enforced. NERC's annual report named PRC-005 first among the most frequently reported operations and planning noncompliance in 2025, and one of the three serious-risk violations filed that year was a PRC-023-4 R1 violation involving a relay on a 500 kV circuit whose trip limit was not set above 150 percent of the circuit's highest seasonal Facility Rating. The correct way to describe the framework is this: it prescribes process and outcome, and it leaves design to the engineer.

11.3 Learning Before Mandates

Within that structure, the framework's response to new misoperation patterns is usually learning first. When misoperation data point to an emerging risk, the typical first response is closer analysis, information exchange among reliability organizations, and industry discussion through reports, workshops, and guidance. That gives the industry time to learn from each other's experience before anyone decides a new mandate is needed. When the learning shows that guidance is not enough, the standards change. PRC-004's current form came out of that path: its technical basis cites NERC's 2011 risk assessment and the 2014 State of Reliability report, which identified Protection System Misoperations as a significant contributor to transmission outage severity and recommended completing the revised standard.

11.4 Objectivity

Keeping design judgments out of oversight also protects objectivity. By not ruling on the merits of particular designs after the fact, the oversight function avoids the hindsight bias that colors many risk judgments. That objectivity is important to public and industry confidence in how misoperations are found and reported.

The separation between observation and instruction is visible in NERC's analytical products. They describe observed performance, the context, and the reliability implications, and they are meant for education and analysis. As systems grow more complex, this outcome-based approach becomes more important. New technology, changing system dynamics, and new operating models cannot all be anticipated and specified in advance. An outcome-based framework can adapt by learning from real system performance instead of trying to cover every case with detailed prescriptions.

End-of-Chapter Summary

Reliability oversight of protection is performance-based and does not prescribe design. Protecting room for engineering judgment matters, but not more than making sure performance does not create reliability risk for the system. That balance keeps innovation from being constrained by the hindsight of the last event.

It is not a framework without obligations. PRC-004-6, PRC-005-6, PRC-027-1, and PRC-023-6 prescribe process, timing, and specific outcomes, and they are enforced. Misoperations are used to improve understanding and drive correction through the owner's own CAP, with industry learning shaping whether further requirements are needed.

12 Synthesis and Reliability Perspective on Protection System Misoperations

12.1 What Misoperations Are

A misoperation is the clearest record the industry has of protection doing something other than what it was set to do. Misoperations are neither purely an engineering problem nor an inevitable cost of operating a complex system. They are observable outcomes of protection operating in a complex, changing, and risk-prone environment. This chapter brings together the main ideas of the reference.

Misoperations matter because protection takes automatic, high-consequence actions across a wide range of abnormal conditions. Those fast, automatic actions are essential to reliability, and when they go wrong the consequences can be quick and severe. Reliability monitoring treats misoperations as one of the richest sources of information about how protection performs.

12.2 Outcome-Based Measurement

Current misoperation metrics are technology neutral and outcome-based. They record what happened, when, and where, along with its actual or potential impact on reliability. A technology-neutral approach allows for different technologies and designs without passing judgment on them; design and operating practice remain the province of the owner's experts. It also provides a uniform basis for combining and comparing data across regions, owners, and years. That is what the NERC Glossary definition, the MIDAS cause codes, and the misoperation impact score provide.

12.3 Context and Shared Risk

Context is now a standard part of judging a misoperation's significance. System conditions, configuration, operating mode, and the sequence of the disturbance all frame it. Oversight does not give every event the same weight; it evaluates each in the context in which it occurred. That balance avoids overstating an isolated incident while still catching trends that point to developing vulnerability.

Because the BES is interconnected, the risk is shared. A misoperation at one facility can affect reliability at facilities owned by many other companies. Misoperations are an industry-wide risk that calls for industry-wide awareness, consistent reporting, and a way for the industry to learn. PRC-004-6's co-owner notification requirement and MIDAS reporting are the formal mechanisms for exactly that.

12.4 Learning and Correction

The framework separates learning from design prescription. Industry analysis uses misoperations to understand risk, while each owner's PRC-004 program uses them to correct the specific cause and check whether it exists elsewhere. That combination keeps the framework current as technologies, resources, and operating practices change, without freezing in place requirements that would soon be out of date.

Taken together, misoperations show the relationships among design assumptions, operating practices, and system development. They show how the system responds to disturbances and signal developing conditions that can affect reliability. They are not a tool for assigning blame. They are a tool for understanding and reducing risk.

12.5 What an Audit Team Will Look For

For a registered entity, the synthesis has a practical edge. On PRC-004-6, an audit team will typically want to see the population of BES interrupting device operations for the period, the dated R1 determination for each, notifications to co-owners where they apply, and for each Misoperation the CAP or declaration with its date, the evaluation of other Protection Systems and locations, and the implementation record with revision history. NERC publishes a Reliability Standard Audit Worksheet for PRC-004-6. A program that can produce that package from its normal records, without a scramble, is a program that is learning from its misoperations rather than just filing them.

> **From the Field**
>
> In my view, misoperation rates track program maturity. A program that closes every CAP and checks the next substation for the same problem gives the same cause fewer chances to repeat. Industry-wide misoperation trends drive standards revisions. Reading the trends tells you what's coming.

End-of-Chapter Summary

Protection system misoperations are outcome-based indicators of reliability, resilience, and future risk. They show how protection behaves on an increasingly dynamic grid with more interconnection, new resources, and new owners.

Through context, aggregation, and learning, reliability oversight uses misoperations to support an objective and adaptive framework for the BES, while PRC-004-6 holds each owner to finding, fixing, and extending the fix within defined deadlines.

Glossary

The definitions below are quoted from the NERC Glossary of Terms as published on nerc.com on October 25, 2026, except where an entry says otherwise. The Glossary is updated as standards change; refer to the current official version for the governing language.

Term	Meaning in this paper
Bulk Electric System (BES)	Unless modified by the lists shown below, all Transmission Elements operated at 100 kV or higher and Real Power and Reactive Power resources connected at 100 kV or higher. This does not include facilities used in the local distribution of electric energy. (The Glossary definition continues with Inclusions I1 through I5 and Exclusions E1 through E4.)
Cascading	The uncontrolled successive loss of System Elements triggered by an incident at any location. Cascading results in widespread electric service interruption that cannot be restrained from sequentially spreading beyond an area predetermined by studies.
Composite Protection System	The total complement of Protection System(s) that function collectively to protect an Element. Backup protection provided by a different Element's Protection System(s) is excluded.
Corrective Action Plan	A list of actions and an associated timetable for implementation to remedy a specific problem.
Distribution Provider	Provides and operates the "wires" between the transmission system and the end-use customer. For those end-use customers who are served at transmission voltages, the Transmission Owner also serves as the Distribution Provider. Thus, the Distribution Provider is not defined by a specific voltage, but rather as performing the distribution function at any voltage.
Element	Any electrical device with terminals that may be connected to other electrical devices such as a generator, transformer, circuit breaker, bus section, or transmission line. An Element may be comprised of one or more components.
Fault	An event occurring on an electric system such as a short circuit, a broken wire, or an intermittent connection.
MIDAS	Misoperation Information Data Analysis System, NERC's application for quarterly reporting of Protection System operation and Misoperation data under a Section 1600 data request. (Not a NERC Glossary term; description from NERC's 2026 MIDAS Data Reporting Instructions.)

Term	Meaning in this paper
Misoperation	The failure of a Composite Protection System to operate as intended for protection purposes. The Glossary lists six types: Failure to Trip and Slow Trip, each During Fault and Other Than Fault, and Unnecessary Trip, During Fault and Other Than Fault. Under the sixth type, Unnecessary Trip, Other Than Fault (an unnecessary Composite Protection System operation for a non-Fault condition), a Composite Protection System operation that is caused by personnel during on-site maintenance, testing, inspection, construction, or commissioning activities is not a Misoperation. (Summarized from the Glossary definition.)
Protection System	Protective relays which respond to electrical quantities; communications systems necessary for correct operation of protective functions; voltage and current sensing devices providing inputs to protective relays; station dc supply associated with protective functions (including station batteries, battery chargers, and non-battery-based dc supply); and control circuitry associated with protective functions through the trip coil(s) of the circuit breakers or other interrupting devices.
Protection System Maintenance Program (PSMP)	An ongoing program by which Protection System, Automatic Reclosing, and Sudden Pressure Relaying Components are kept in working order and proper operation of malfunctioning Components is restored. (The Glossary definition continues with the activities verify, monitor, test, inspect, and calibrate.)
Reliability Coordinator (RC)	The entity that is the highest level of authority who is responsible for the Reliable Operation of the Bulk Electric System, has the Wide Area view of the Bulk Electric System, and has the operating tools, processes and procedures, including the authority to prevent or mitigate emergency operating situations in both next-day analysis and real-time operations. The Reliability Coordinator has the purview that is broad enough to enable the calculation of Interconnection Reliability Operating Limits, which may be based on the operating parameters of transmission systems beyond any Transmission Operator's vision.
Transmission Operator (TOP)	The entity responsible for the reliability of its "local" transmission system, and that operates or directs the operations of the transmission Facilities.
Transmission Owner (TO)	The entity that owns and maintains transmission Facilities.

How Energy Compliance Can Help

PRC-004 and protection program reviews

A regulator-perspective program review tests whether your Misoperation records, CAPs, and extent-of-condition evaluations would survive real audit questions. EC also provides reliability governance and program assessments, compliance program design and improvement, mitigation planning and Self-Report development when a PRC-004 or PRC-005 clock has already been missed, and registration and applicability analysis for owners sorting out what falls inside PRC-004 and PRC-030.

Audit defense and audit preparation

EC provides audit and enforcement support (non-advocacy), audit defense with Notice of Penalty response and settlement posture, NERC compliance program support, interpretation, and audit preparation, RSAW production, and data request strategy.

Senior advisory across engineering and operations

EC offers NERC reliability and compliance advisory support, senior advisory with direct engagement on complex reliability questions, operational and engineering reliability alignment between protection engineering, operations, and compliance, training and executive briefings on reliability frameworks, and industry engagement in standards development and working-group participation. Each engagement is scoped to the entity's role, function, and bulk system impact.

WattOps Compliance

A 120-day clock is an evidence problem before it is an audit problem. WattOps Compliance is EC's NERC compliance evidence platform (wattopscompliance.com). EC will run one standard at one facility through WattOps at no cost (CIP standards excluded).

RenewOps

For renewable and storage owners, the question of whether a trip belongs under PRC-004 or PRC-030 starts in the operations data. RenewOps is EC's renewable operations monitoring and analytics platform, with a Data Center module.

Pull your last four quarters of BES breaker operations and check each against a dated R1 determination. If any are missing, call us.

Website: energycomplianceinc.com · Email: rsmith@complianceforenergy.com

Phone: 763.438.4427

About the Author

Rob Smith is the Founder and Principal of Energy Compliance, Inc., with more than thirty years in the industry on every side of the system. He began in control-room operations as a Reliability Coordinator, Transmission Operator, and Power System Operator across RTO/ISO and utility control centers. On the regulator side, he was a senior compliance auditor and subject matter expert for NERC Reliability Standards. He audited grid facilities, evaluated mitigation adequacy, participated in risk-based oversight of utility mitigation activities, and supported the development of violation notifications and settlements in FERC-directed enforcement actions. He conducted a regulatory audit in the Sultanate of Oman against the Sultanate's Sector Law and Grid Code.

He founded Energy Compliance, Inc. to deliver senior regulator-side compliance authority without the layered staffing and billable-hour overhead of larger firms.

Education:

- MBA, Energy Management, University of Mary
- MSL, Compliance Law, Fordham Law University
- BAS, Energy Management, Bismarck State College
- BAS, Mechanical Engineering, Metallurgy minor, University of Florida
- BAS, Criminology, St. Petersburg College (State Law Enforcement Certification)
- AAS, Power Plant Technology, Bismarck State College
- AAS, Electrical Transmission System Technology, Bismarck State College

Certifications: NERC Lead Auditor training; previously NERC-certified at the Reliability Coordinator level; 1st Class A Boiler Engineer License, Minnesota.

About Energy Compliance, Inc.

Energy Compliance, Inc. is an independent consulting and advisory firm based in Bloomington, Minnesota, focused exclusively on electric reliability, cybersecurity reliability, and regulatory compliance for organizations connected to the North American Bulk Electric System.

We support registered entities, including Generator Owners and Operators, Transmission Owners and Operators, Reliability Coordinators, Balancing Authorities, and Distribution Providers. Our work spans NERC Reliability Standards, FERC orders, RTO/ISO market participation rules, Regional Entity oversight, and state regulatory frameworks.

We do this work differently than larger consulting firms. A senior practitioner with regulator-side experience oversees every engagement. We staff for outcomes, not billable hours. Our deliverables are written to be operationally executable and audit-defensible, structured for the auditor's question rather than the consultant's binder. Where automation can replace manual work, we build the automation. Where senior judgment is required, the senior is in the room.

Energy Compliance is not affiliated with, sponsored by, or endorsed by the North American Electric Reliability Corporation, the Federal Energy Regulatory Commission, or any Regional Entity.

Learn more at energycomplianceinc.com.

Sources and Authorities

- North American Electric Reliability Corporation, Glossary of Terms Used in NERC Reliability Standards (web version, retrieved October 25, 2026): Bulk Electric System, Cascading, Composite Protection System, Corrective Action Plan, Distribution Provider, Element, Fault, Misoperation, Protection System, Protection System Maintenance Program, Reliability Coordinator, Transmission Operator, Transmission Owner. https://www.nerc.com/glossary-of-terms
- North American Electric Reliability Corporation, Reliability Standard PRC-004-6, Protection System Misoperation Identification and Correction (effective April 1, 2021), Applicability, Requirements R1 through R6, Measures M1 through M6, Evidence Retention, Violation Severity Levels, Version History, and Guidelines and Technical Basis. https://www.nerc.com/globalassets/standards/reliability-standards/prc/prc-004-6.pdf
- North American Electric Reliability Corporation, Reliability Standard Audit Worksheet, PRC-004-6 (2021, v1). https://www.nerc.com/globalassets/programs/compliance/rsaws/rsaw-prc-004-6_2021_v1.docx
- North American Electric Reliability Corporation, Reliability Standard PRC-005-6, Protection System, Automatic Reclosing, and Sudden Pressure Relaying Maintenance (effective January 1, 2016), Purpose and Applicability. https://www.nerc.com/globalassets/standards/reliability-standards/prc/prc-005-6.pdf
- North American Electric Reliability Corporation, Reliability Standard PRC-023-6, Transmission Relay Loadability (effective April 1, 2024), Purpose. https://www.nerc.com/globalassets/standards/reliability-standards/prc/prc-023-6.pdf
- North American Electric Reliability Corporation, Reliability Standard PRC-027-1, Coordination of Protection Systems for Performance During Faults (effective April 1, 2021), Requirements R1 and R2. https://www.nerc.com/globalassets/standards/reliability-standards/prc/prc-027-1.pdf
- North American Electric Reliability Corporation, Reliability Standard PRC-029-2, Frequency and Voltage Ride-through Requirements for Inverter-Based Resources (effective October 1, 2026, following FERC approval). https://www.nerc.com/globalassets/standards/reliability-standards/prc/prc-029-2.pdf
- North American Electric Reliability Corporation, Reliability Standard PRC-030-1, Unexpected Inverter-Based Resource Event Mitigation (effective October 1, 2026), Purpose, Applicability, and Requirement R1. https://www.nerc.com/globalassets/standards/reliability-standards/prc/prc-030-1.pdf

- North American Electric Reliability Corporation, PRC Reliability Standards listing, status and effective dates (retrieved October 26, 2026). https://www.nerc.com/standards/reliability-standards/prc
- North American Electric Reliability Corporation, MIDAS Data Reporting Instructions (effective January 1, 2026), Introduction and Chapter 1, and Cause of Misoperation definitions. https://www.nerc.com/globalassets/programs/rapa/midas/midas_dri_2026.pdf
- North American Electric Reliability Corporation, Misoperation Information Data Analysis System (MIDAS) page, Deadlines for Data Submission into MIDAS (retrieved October 26, 2026). https://www.nerc.com/programs/reliability-assessment--performance-analysis/misoperation-information--data-analysis-system-midas
- North American Electric Reliability Corporation, Rules of Procedure, Section 1600, Requests for Data or Information, Section 1601. https://www.nerc.com/globalassets/who-we-are/rules-of-procedure/nerc-rop.pdf
- North American Electric Reliability Corporation, 2026 State of Reliability: Technical Assessment of 2025 Bulk Power System Performance (June 24, 2026), Chapter 3, Protection System Misoperation Trends, Leading Causes of Misoperations, Misoperation Impact Score, Event-Related Misoperations, and Protection System Misoperations (human performance). https://www.nerc.com/globalassets/programs/rapa/pa/nerc_sor_2026_technical_assessment.pdf
- North American Electric Reliability Corporation, ORCP and CMEP Annual Report (February 11, 2026), Chapter 5, Top 10 O&P Noncompliance Reported in 2025 and Top 10 Serious and Moderate Risk Noncompliance Filed in 2025. https://www.nerc.com/globalassets/programs/enforcement/cmep-and-vegetation-reports/2025-orcp-and-cmep-annual-report.pdf

© Energy Compliance, Inc. · EC-WP-306 · October 2026