

# Important Considerations for Testing and Commissioning Digital Protective Relays

The proven advantages of digital technology for power system protective relays are now commonplace in the power producing and delivery industry. Digital relays provide unsurpassed reliability and extended capabilities at an economical cost. Keeping pace with the testing and commissioning requirements of these devices has proven to be a challenge for both protective relay engineers and technicians. Although testing procedures have been well defined for single-function electromechanical (EM) protection devices, modern relay test procedures have been left to the utility to develop, creating possible shortcuts that may compromise the protection system operation.

Extended options and settings, complex trip logic equations, and advanced communication options can lead to overwhelming difficulties in ensuring that a multifunction intelligent electronic device (IED) is properly tested. Observations from within the industry indicate that a common reason for potential errors is the implementation of shortcuts, primarily for simplifying the process and meeting regulatory recordkeeping requirements. Some of these testing shortcut practices include setting and logic changes that accommodate easy testing, creating test values based on single-element settings rather than the actual applications, and failing to test the entire enabled capabilities of the protection system.

This article presents examples of common mistakes typically observed during testing and commissioning as well as ways to avoid them with simple-to-understand guidelines. The importance of testing protection systems, rather than single, protective elements that avoid protective relay misoperations once in service, is also discussed.

## Testing Procedures

The process of testing multifunction digital protective relays brings new challenges for many reasons. First, we must understand the focus of testing these devices as compared with that of EM or single-function relays. The main purpose of testing EM relays was to ensure proper calibration. Calibration and testing procedures were widely available from the manufacturer and relatively easy to understand. Although modern digital technology provides many advantages, finding appropriate guidance for proper testing can be very difficult. This article offers suggestions for simplifying the testing process without compromising proper testing procedures.

## Adequate Test Equipment

For the proper testing of multiphase IEDs, it is essential to provide a multiphase source of voltage and current. Testing a multiphase protective element with a single-phase source can lead to false assessment. Some calculations of fault values rely on measured values from a nonfaulted phase. Typically, all possible faults should be simulated for each protective element. All utilized CT and PT inputs must be taken into consideration during the testing process. Additionally, all binary inputs and outputs utilized by the IED must be accounted

for in the test equipment because it is equally important to test all logic associated with the IED's operation.

## Understanding Different Types of Tests

The different types of testing procedures are defined as follows:

1. *Evaluation testing* determines whether a protective relay is suitable for use on a particular protection application(s) within a power system; this is also recognized as a process to evaluate and validate published specifications by the relay manufacturer.
2. *Commission testing* ensures correct functionality of the relay when first installed and activated within the power system.
3. *Periodic or maintenance testing* routinely checks and validates the correct operation of an already installed and active protective relay.

For the purposes of this article, we refer mainly to the commissioning of digital protective relays, although the discussion can also be relevant to the other testing processes as well [1].

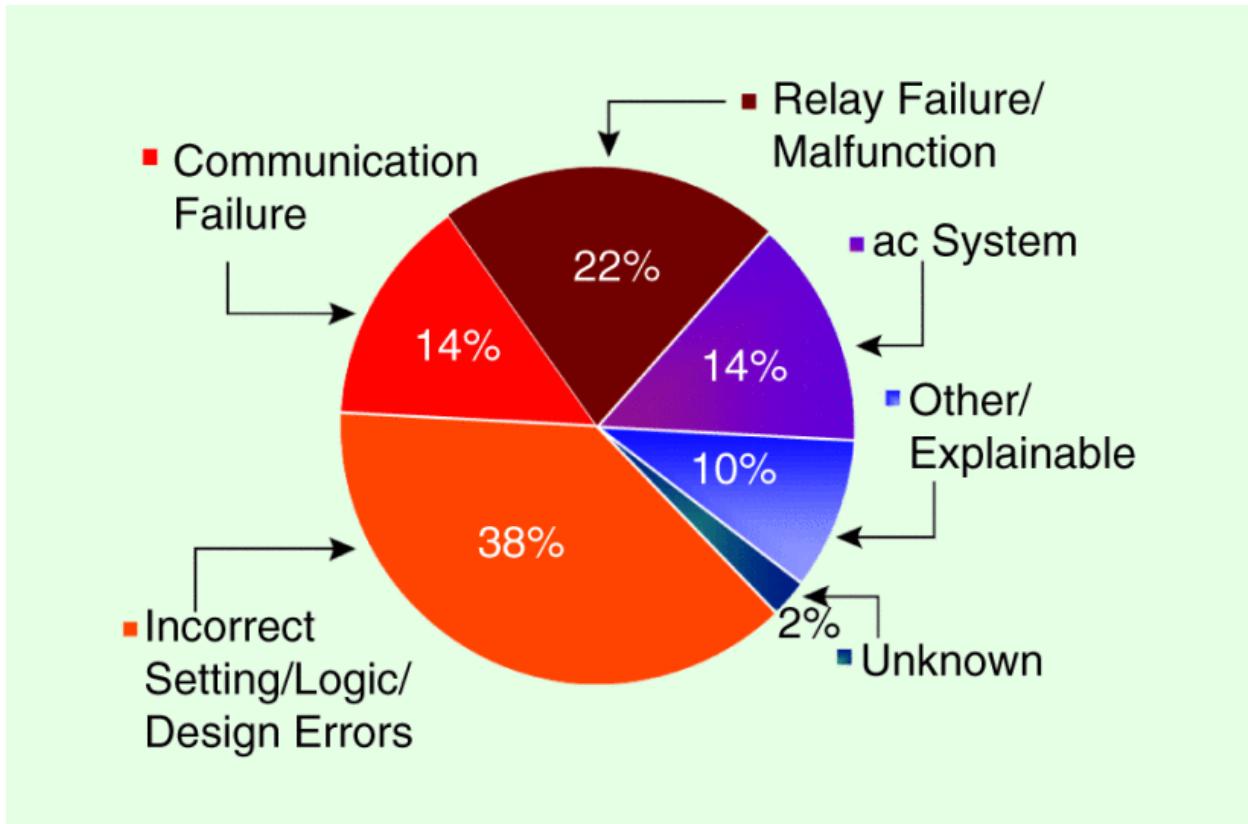
## First Consideration: Why Do We Test?

For EM technology, the main purpose of testing was to ensure proper calibration of the device. Over long periods of time, contacts, springs, potentiometers, and coils tend to require recalibration, cleaning, or adjustments to ensure proper operation. The term *silent sentinel* was often used to describe this type of technology because there were no self-diagnostics present to determine whether or not the relay would function properly in the event of a fault. With no such calibration required for digital technology, as well as the ability to rely on certain self-diagnostics, why is the commission process still required?

In 2013, the North American Electric Reliability Corporation (NERC) released a report that claimed a dramatic rise in the annual number of mis operations due, in large part, to the complexity of programming and testing digital protection relays.

As shown in Figure 1, mis operations primarily occurred because of the following reasons:

- incorrect setting/logic/design errors
- communication failures
- relay failure or malfunctions.



**Figure 1.**  
The 2012 NERC mis operations graph.

These events include human error during testing and maintenance activities. This human error, resulting in protection system activation, has contributed to large disturbance events.

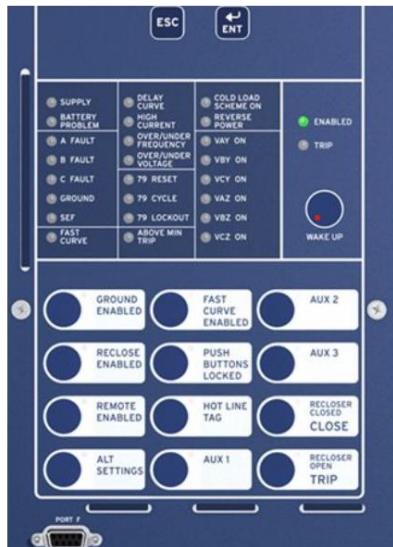
Proper testing is just as important for multifunction digital IEDs as it is for older EM technology, but the focus has changed significantly. It is true that the IED self-diagnostics can alert operations of an internal failure and remove itself from service, but only through proper testing procedures can it be determined that the protection system is properly configured.

Complex logic configurations, multiple setting groups, communication-based protection schemes, and a large number of protective elements in a single IED add significant challenges to proper commissioning. Much of this complexity has led to recognized shortcuts within the testing process, which can ultimately lead to mis operation [1].

## Second Consideration: What Do We Test?

At first glance, this may appear to be a simple question, but when faced with the complexity of a modern protection IED, it is anything but. The components tested are as follows:

1. *Test each protection element:* Each protection element must be tested to ensure that it has been set properly. This may seem unnecessary because there is no calibration, but relay engineers and technicians are quite capable of human error in setting each device. A misplaced decimal point, forgotten time delay, or even forgetting to enable an element are all possible and can lead to misoperations.
2. *Associated logic:* This important factor is often overlooked. The complexity associated with some logic equations adds to a large majority of mis operations. For example, when protective element supervision from a breaker contact is required, breaker simulation during the testing process is essential. Many protection IEDs also have programmable human–machine interface controls, some of which invoke safety-related commands such as Hot Line Tag (Figure 2). If the controls are not programmed and tested properly, extreme hazards could be present [2].
3. *Communication-based protection schemes:* These are most often seen in transmission line protection and, in the majority of cases, are the basis for end-to-end testing. However, these types of tests are time-consuming and often difficult to achieve. Nonetheless, in this critical test for a transmission line, the protection engineer can verify the delay time of the teleprotection signals (i.e., the delay time between sending signal transmissions recorded on the first end and the received signal recorded on the other end) immediately after executing the shot, as shown in Figure 3 [3].



**Figure 2.**  
A feeder relay with human–machine interface control.



**Figure 3.**

The delay time of teleprotection signals.

### Third Consideration: How Do We Test?

These test procedures should be avoided:

- testing a protection IED based on factory settings
- changing, altering, or disabling the associated logic with each protective element to validate settings

- changing, altering, or disabling the components of a protective element to validate settings
- testing the IED by relying only on the settings that lie within the relay
- closing the relay trip circuit without the metering validation of a nontrip state [1].

These procedures should be followed:

- ensure that the settings coincide with those pertaining to the application and not factory or predefined “test settings”
- test the device with associated logic enabled, considering both sides of a logic equation for proper validation
- test the element without changing settings such as pick up, dropout, or time delays and using proper fault values for fault simulations.
- use relay software to validate proper secondary CT and PT wiring prior to enabling the trip circuit, as shown in Figure 4 [2].



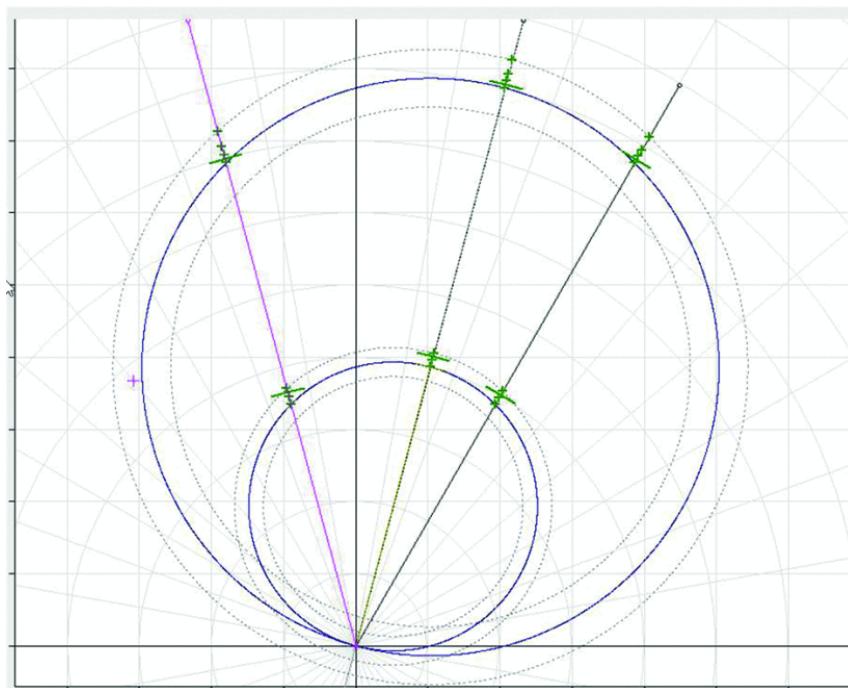
**Figure 4.**

An example of relay-metering software.

The proper test sequences that account for associated logic are as follows:

1. Begin each test with a proper prefault condition: “Be the relay.” This should include, but not be limited to, the proper simulation of breaker contacts and the application of prefault analog values (nominal) that are maintained long enough for lockouts to reset (feeder management relays). Doing so will mitigate logic interference such as “switch on to fault,” “cold load pickup,” and so on.

2. Maintain a proper calculated fault value until the element picks up, allowing for the validation of trip times and thresholds.
3. Follow up with a proper post-fault state, including breaker open logic, and faulted values that would be eliminated in a normal trip state condition. Doing so removes interference from associated breaker failure conditions.
4. Ensure that calculated test values coincide with published tolerances provided by the relay manufacturer. Most modern testing software allows for automated test sequences and assessment (Figure 5).



**Figure 5.**  
The automated tests from a test set.

## Fourth Consideration: When Do We Test?

### NERC Testing Intervals

As shown in Figure 6, the System Protection and Controls Task Force of the NERC Planning Committee publishes maximum testing intervals by equipment category [4]. Figure 7 illustrates published recommendations of relay testing intervals, according to International Electrical Testing Association (NETA) standards.

Maximum Allowable Testing Intervals by Equipment Category						
Category	Component	Maximum Verification Interval			Verification Activities	
Reference Figure 1		Un-monitored	Partial Monitoring Note 1	Thorough Monitoring Note 2	Full Monitoring Note 3	
1	Testing and calibration of protective relays, per Note 7	Five years	Seven years (Notes 1a, 1e, 1f)	10 years (Note 2a)	Continuous Monitoring and Verification	Test the functioning of relays with simulated inputs, including calibration per Note 7. Verify that settings are as specified. See Section 12 for a discussion of verifying settings.
2	Verification of instrument transformer outputs and correctness of connections to protection system	Seven years	Seven years (Notes 1a, 1f)	10 years (Note 2a)	Continuous Monitoring and Verification	Verify the current and voltage signals to the protection system and instrument transformer circuit grounding.
3	Verification of protection system tripping including circuit breaker tripping, auxiliary tripping relays and devices, lockout relays, telecommunications-assisted tripping schemes, and circuit breaker status indication required for correct operation of protection system	Five years	Seven years (Notes 1a, 1b, 1d, 1e, 1f)	10 years (Note 2b)	Continuous Monitoring and Verification	Perform trip tests for the whole system at once and/or component operating tests with overlapping of component verifications as explained in Section 10. Every operating circuit path must be fully verified, although one check of any path is sufficient. A breaker only needs to be tripped once per trip coil within the specified time interval. Telecommunications-assisted line protection systems may be verified either by end-to-end tests or by simulating internal or external faults with forced channel signals.
4	Station battery supply (Note 12)	One month	Seven years (Notes 1b, 1d, 1f)	Continuous Verification (Notes 2b, 2d)	Continuous Monitoring and Verification	Verify voltage of the station battery once a month if not monitored.

**Figure 6.**  
NERC testing intervals.

Section	Description	Visual	Visual and Mechanical	Visual and Mechanical and Electrical
7.9	Protective Relays			
7.9.1	EM and Solid State	1	12	12
7.9.2	Microprocessor Based	1	12	12
7.10	Instrument Transformers	12	12	36
7.11	Metering Devices			
7.11.1	EM and Solid State	12	12	36
7.11.2	Microprocessor Based	12	12	36

**Figure 7.**

Relay testing intervals in months per the NETA.

Additional considerations for testing intervals are

- environmental conditions
- criticality of the protected asset
- redundancy of protection
- historical performance.

The final considerations for when to test are

- setting changes after commissioning
- relaying firmware updates
- rewiring in the trip circuit or secondary CTs or PTs.

## Conclusion

When considering digital protection relays, it is important to understand the impact that self-diagnostics play in the testing process. Although self-diagnostics will detect the failures of certain components, such as power supplies, microprocessors, and circuit board parts, we must also understand what it will not detect, such as relay output contacts. Most importantly, self-diagnostics will not alarm when there is human error in setting the protective elements or logic correctly. While digital technology adds greater reliability within the protection system, this does not eliminate the need for proper testing; rather, this technology necessitates refocusing of the testing process.

## Drew S. Welton

Vice President of Sales



### Biography

Drew Welton (IEEE Senior) is Vice President of Sales for Intellirent, division of Electrorent, providing strategic leadership to the sales team and creating new business development for the industrial testing, power producing industries. Welton was previously the North American Regional Manager for OMICRON, starting in 1997. Prior to his career with OMICRON, Welton was a Regional Sales Manager with Beckwith Electric. He also served as National Sales Director for Substation Automation with AREVA T&D. Welton has written numerous articles on substation maintenance testing and has conducted training sessions for substation technicians and engineers at utilities and universities across North America. He is a 20-year Senior Member of IEEE-PES, IAS, and an active member of the Transformers Committee. He has been a contributor on a number of PSRC working groups and presented at many industry conferences specific to power system protection and control. He has a bachelor's degree in Business Administration from Fort Lewis College, Durango, Colorado.

### References

1. D. Welton, "Avoiding potentially dangerous testing practices for digital relays", *Proc. Georgia Tech Protective Relay Conf.*, pp. 1-4, 2008.
2. D. Welton, "Testing advanced digital relay systems", *Electric Energy Mag.*, May/June 2004.
3. F. Steinhauser, "Network simulation on the PC—New options for protection testing", *Proc. IPTS*, 2004.

**4.** *Protection system maintenance: A technical reference*, 2007, [online] Available: [https://www.nerc.com/pa/RAPA/PA/Performance%20Analysis%20DL/NERC\\_2018\\_SOR\\_06202018\\_Final.pdf](https://www.nerc.com/pa/RAPA/PA/Performance%20Analysis%20DL/NERC_2018_SOR_06202018_Final.pdf).

**5.** D. Welton, W. Knapek, "Important considerations for testing and commissioning digital protection relays", *Proc. IEEE REPC Conf. Rec*, pp. 12-16, 2017.