



IEEE Guide for Power System Protection Testing

IEEE Power & Energy Society

Sponsored by the
Power System Relaying Committee

IEEE
3 Park Avenue
New York, NY 10016-5997, USA

11 December 2009

IEEE Std C37.233™-2009

IEEE Guide for Power System Protection Testing

Sponsor

IEEE Power System Relaying Committee

of the

IEEE Power & Energy Society

Approved 11 September 2009

IEEE-SA Standards Board

Abstract: Test approaches and procedures for the components and the overall protection and control system functions are presented. Test of equipment in the system protection scheme, associated communications equipment, auxiliary power supplies, and the control of power apparatus are addressed. Much of the testing emphasizes a bottom-up approach, in which the basic behavior of scheme components are verified first, followed by testing of interconnected components in a function-oriented assembly.

Keywords: application testing, commissioning testing, design testing, maintenance testing, performance assessment

The Institute of Electrical and Electronics Engineers, Inc.
3 Park Avenue, New York, NY 10016-5997, USA

Copyright © 2009 by the Institute of Electrical and Electronics Engineers, Inc.
All rights reserved. Published 11 December 2009. Printed in the United States of America.

IEEE is a registered trademark in the U.S. Patent & Trademark Office, owned by the Institute of Electrical and Electronics Engineers, Incorporated.

PDF: ISBN 978-0-7381-6080-1 STD95978
Print: ISBN 978-0-7381-6081-8 STDPD95978

No part of this publication may be reproduced in any form, in an electronic retrieval system or otherwise, without the prior written permission of the publisher.

IEEE Standards documents are developed within the IEEE Societies and the Standards Coordinating Committees of the IEEE Standards Association (IEEE-SA) Standards Board. The IEEE develops its standards through a consensus development process, approved by the American National Standards Institute, which brings together volunteers representing varied viewpoints and interests to achieve the final product. Volunteers are not necessarily members of the Institute and serve without compensation. While the IEEE administers the process and establishes rules to promote fairness in the consensus development process, the IEEE does not independently evaluate, test, or verify the accuracy of any of the information or the soundness of any judgments contained in its standards.

Use of an IEEE Standard is wholly voluntary. The IEEE disclaims liability for any personal injury, property or other damage, of any nature whatsoever, whether special, indirect, consequential, or compensatory, directly or indirectly resulting from the publication, use of, or reliance upon this, or any other IEEE Standard document.

The IEEE does not warrant or represent the accuracy or content of the material contained herein, and expressly disclaims any express or implied warranty, including any implied warranty of merchantability or fitness for a specific purpose, or that the use of the material contained herein is free from patent infringement. IEEE Standards documents are supplied “**AS IS**.”

The existence of an IEEE Standard does not imply that there are no other ways to produce, test, measure, purchase, market, or provide other goods and services related to the scope of the IEEE Standard. Furthermore, the viewpoint expressed at the time a standard is approved and issued is subject to change brought about through developments in the state of the art and comments received from users of the standard. Every IEEE Standard is subjected to review at least every five years for revision or reaffirmation. When a document is more than five years old and has not been reaffirmed, it is reasonable to conclude that its contents, although still of some value, do not wholly reflect the present state of the art. Users are cautioned to check to determine that they have the latest edition of any IEEE Standard.

In publishing and making this document available, the IEEE is not suggesting or rendering professional or other services for, or on behalf of, any person or entity. Nor is the IEEE undertaking to perform any duty owed by any other person or entity to another. Any person utilizing this, and any other IEEE Standards document, should rely upon his or her independent judgment in the exercise of reasonable care in any given circumstances or, as appropriate, seek the advice of a competent professional in determining the appropriateness of a given IEEE standard.

Interpretations: Occasionally questions may arise regarding the meaning of portions of standards as they relate to specific applications. When the need for interpretations is brought to the attention of IEEE, the Institute will initiate action to prepare appropriate responses. Since IEEE Standards represent a consensus of concerned interests, it is important to ensure that any interpretation has also received the concurrence of a balance of interests. For this reason, IEEE and the members of its societies and Standards Coordinating Committees are not able to provide an instant response to interpretation requests except in those cases where the matter has previously received formal consideration. A statement, written or oral, that is not processed in accordance with the IEEE-SA Standards Board Operations Manual shall not be considered the official position of IEEE or any of its committees and shall not be considered to be, nor be relied upon as, a formal interpretation of the IEEE. At lectures, symposia, seminars, or educational courses, an individual presenting information on IEEE standards shall make it clear that his or her views should be considered the personal views of that individual rather than the formal position, explanation, or interpretation of the IEEE.

Comments for revision of IEEE Standards are welcome from any interested party, regardless of membership affiliation with IEEE. Suggestions for changes in documents should be in the form of a proposed change of text, together with appropriate supporting comments. Comments on standards and requests for interpretations should be submitted to the following address:

Secretary, IEEE-SA Standards Board
445 Hoes Lane
Piscataway, NJ 08854
USA

Authorization to photocopy portions of any individual standard for internal or personal use is granted by The Institute of Electrical and Electronics Engineers, Inc., provided that the appropriate fee is paid to Copyright Clearance Center. To arrange for payment of licensing fee, please contact Copyright Clearance Center, Customer Service, 222 Rosewood Drive, Danvers, MA 01923 USA; +1 978 750 8400. Permission to photocopy portions of any individual standard for educational classroom use can also be obtained through the Copyright Clearance Center.

Introduction

This introduction is not part of IEEE Std C37.233-2009, IEEE Guide for Power System Protection Testing.

This guide focuses on the general approach and specific procedures for testing protective relaying systems that include multiple interacting relay components, auxiliary devices, and power apparatus. In the most critical applications, these system devices may interact over an extended physical or geographic area and use communications systems. The procedures focus separately on design testing, commissioning testing, routine maintenance testing, and ongoing performance assessment with a discussion of what each of these test categories aims to accomplish.

Notice to users

Laws and regulations

Users of these documents should consult all applicable laws and regulations. Compliance with the provisions of this standard does not imply compliance to any applicable regulatory requirements. Implementers of the standard are responsible for observing or referring to the applicable regulatory requirements. IEEE does not, by the publication of its standards, intend to urge action that is not in compliance with applicable laws, and these documents may not be construed as doing so.

Copyrights

This document is copyrighted by the IEEE. It is made available for a wide variety of both public and private uses. These include both use, by reference, in laws and regulations, and use in private self-regulation, standardization, and the promotion of engineering practices and methods. By making this document available for use and adoption by public authorities and private users, the IEEE does not waive any rights in copyright to this document.

Updating of IEEE documents

Users of IEEE standards should be aware that these documents may be superseded at any time by the issuance of new editions or may be amended from time to time through the issuance of amendments, corrigenda, or errata. An official IEEE document at any point in time consists of the current edition of the document together with any amendments, corrigenda, or errata then in effect. In order to determine whether a given document is the current edition and whether it has been amended through the issuance of amendments, corrigenda, or errata, visit the IEEE Standards Association Web site at <http://ieeexplore.ieee.org/xpl/standards.jsp>, or contact the IEEE at the address listed previously.

For more information about the IEEE Standards Association or the IEEE standards development process, visit the IEEE-SA Web site at <http://standards.ieee.org>.

Errata

Errata, if any, for this and all other standards can be accessed at the following URL: <http://standards.ieee.org/reading/ieee/updates/errata/index.html>. Users are encouraged to check this URL for errata periodically.

Interpretations

Current interpretations can be accessed at the following URL: <http://standards.ieee.org/reading/ieee/interp/index.html>.

Patents

Attention is called to the possibility that implementation of this guide may require use of subject matter covered by patent rights. By publication of this guide, no position is taken with respect to the existence or validity of any patent rights in connection therewith. The IEEE is not responsible for identifying Essential Patent Claims for which a license may be required, for conducting inquiries into the legal validity or scope of Patents Claims or determining whether any licensing terms or conditions provided in connection with submission of a Letter of Assurance, if any, or in any licensing agreements are reasonable or non-discriminatory. Users of this guide are expressly advised that determination of the validity of any patent rights, and the risk of infringement of such rights, is entirely their own responsibility. Further information may be obtained from the IEEE Standards Association.

Participants

At the time this guide was submitted to the IEEE-SA Standards Board for approval, the Power System Protection Testing Working Group had the following membership:

Vahid Madani, *Chair*
Hyder DoCarmo, *Vice Chair*

Marc Achterkamp
Mark Adamiak
Mike Agudo
Alexander Apostolov
James Ariza
Miroslav Begovic
Robert Beresh
Gustavo Brunello
Dac-Phouc Bui
Sean Chilcote
Guy Colpron

Ratan Das
Kelly Gardner
Daniel Goodrich
Anthony Giuliente
Gene Henneberg
Rich Hunt
Bogdan Kasztenny
Tim Kern
Mladen Kezunovic
Gary L. Kobet
Peter McLaren
Michael Mendik

Kalyan Mustaphi
Damir Novosel
Farnoosh Rahmatian
André Santos
Tony Seegers
Jon Sykes
Eric Udren
Alfredo Vaccaro
Benton A. Vandiver
Jun Verzosa
Ilia Voloh

The following members of the individual balloting committee voted on this guide. Balloters may have voted for approval, disapproval, or abstention.

William J. Ackerman	Roger Hedding	Joe Nims
Steven Alexanderson	Charles Henville	Gary Nissen
Alexander Apostolov	Lee Herron	Allan St. Peter
Stan Arnot	Gary Heuston	Craig Preuss
Ali Al Awazi	Scott Hietpas	Iulian Profir
Thomas Barnes	Jerry Hohn	Farnoosh Rahmatian
G. Bartok	Dennis Holstein	Madan Rana
David Basset	David Horvath	R. Rebbapragada
Thomas Basso	James Huddleston III	Michael Roberts
Robert Beresh	James Ingleson	Charles Rogers
Martin Best	Gerald Johnson	M. Sachdev
Steven Bezner	James Jones	Miriam Sanders
Wallace Binder	Innocent Kamwa	Steven Sano
Kenneth Birt	Bogdan Kasztenny	Daniel Sauer
William Bloethe	Gael Kennedy	Bartien Sayogo
Chris Brooks	Mladen Kezunovic	Thomas Schossig
Gustavo Brunello	Tanuj Khandelwal	Sam Sciacca
Hyder DoCarmo	Yuri Khersonsky	Tony Seegers
Arvind K. Chaudhary	Chad Kiger	Douglas Seely
Stephen Conrad	James Kinney	Gregory Sessler
Tommy Cooper	Gary L. Kobet	Devki Sharma
Jerry Corkran	Joseph L. Koepfinger	Gil Shultz
James Cornelison	David W. Krause	Tarlochan Sidhu
Ratan Das	Jim Kulchisky	David Smith
Alla Deronja	Saumen Kundu	James E. Smith
Gary L. Donner	Chung-Yiu Lam	Jerry Smith
Ernest Duckworth	Raluca Lascu	Kevin Stephan
Donald Dunn	Debra Longtin	Charles Sufana
Douglas J. Edwards	Federico Lopez	Richard Taylor
Gearold O. H. Eidhin	William Lowe	John Tengdin
Gary Engmann	Bruce Mackie	David Tepen
Keith Flowers	Vahid Madani	Demetrios Tziouvaras
Fredric Friend	O. Malik	Joe Uchiyama
Jeffrey Gilbert	Omar Mazzoni	Eric Udren
Anthony Giuliante	Gary Michel	Benton A. Vandiver
Jalal Gohari	Georges Montillet	John Vergis
Stephen Grier	Charles Morse	Jane Verner
Randall Groves	Jerry Murphy	Solveig Ward
Ajit Gwal	Dennis Nietzel	Kenneth White
	Michael S. Newman	

When the IEEE-SA Standards Board approved this guide on 11 September 2009, it had the following membership:

Robert M. Grow, *Chair*
Thomas Prevost, *Vice Chair*
Steve M. Mills, *Past Chair*
Judith Gorman, *Secretary*

John Barr	Alexander Gelman	David J. Law
Karen Bartleson	Jim Hughes	Ted Olsen
Victor Berman	Richard H. Hulett	Glenn Parsons
Ted Burse	Young Kyun Kim	Ronald C. Petersen
Richard DeBlasio	Joseph L. Koepfinger*	Narayanan Ramachandran
Andy Drozd	John Kulick	Jon Walter Rosdahl
Mark Epstein		Sam Sciacca

*Member Emeritus

Also included are the following nonvoting IEEE-SA Standards Board liaisons:

Howard L. Wolfman, *TAB Representative*

Michael Janezic, *NIST Representative*

Satish K. Aggarwal, *NRC Representative*

Lorraine Patsco

IEEE Standards Program Manager, Document Development

Soo Kim

IEEE Standards Program Manager, Technical Program Development

Contents

1. Overview	1
1.1 Scope	1
1.2 Purpose	1
1.3 General	2
1.4 Types of applications	2
1.5 Types of tests	3
1.6 Applications for systems, schemes, and multistation testing	5
1.7 Considerations for testing and scheme self-monitoring	7
2. Normative references	10
3. Definitions, acronyms, and abbreviations	11
3.1 Definitions	11
3.2 Acronyms and abbreviations	11
4. Types of tests	12
4.1 Certification tests	12
4.2 Application tests	13
4.3 Commissioning tests	14
4.4 Maintenance tests	15
4.5 Example of test setup configurations and equipment (end-to-end testing)	18
4.6 Methods for generating test modules and cases	21
4.7 Analyses and retention of test results	26
5. Benefits and justification for different types of tests	30
6. Description of types of relay schemes and testing requirements	31
6.1 Introduction	31
6.2 Line protection	32
6.3 Transformer protection	43
6.4 Distribution protection	49
6.5 Shunt capacitor protection	56
6.6 Bus protection	58
6.7 Breaker failure protection and control	59
6.8 Reactor protection	67
6.9 Generator protection	68
6.10 Trip circuit logic scheme	70
7. Protection system communication testing	74
7.1 Power-line carrier testing	74
7.2 Functional testing of IEC 61850-based substation automation systems	77
7.3 Wireless communication	82

8. SIPS test requirements	83
8.1 Proof-of-concept testing	86
8.2 Field commissioning tests	87
8.3 System-wide performance testing during maintenance intervals	87
8.4 Validation through state estimation	88
8.5 Automatic and manual periodic testing of the entire scheme	88
9. Testing protection and control systems with unconventional voltage and current sensing inputs	90
9.1 Testing inputs to relays and microprocessor-based devices with low-level analog inputs per IEEE Std C37.92™-2005 [B17]	90
9.2 Testing inputs to relays with digital interfaces per IEC 61850-9-2-2004 [B13] process bus	91
9.3 Testing outputs of unconventional sensors	94
9.4 Verification by condition-based maintenance	96
Annex A (informative) Bibliography	97
Annex B (informative) Suggested line current differential scheme testing procedure	100
Annex C (informative) Impact of high-impedance faults to protective relay performance and system testing	105
Annex D (informative) Transformer oil and winding temperature computational methods	108
Annex E (informative) Measuring and compensating for time delay after trigger for performing end-to-end testing using different relay test sets	110

IEEE Guide for Power System Protection Testing

IMPORTANT NOTICE: *This guide is not intended to ensure safety, security, health, or environmental protection in all circumstances. Implementers of the guide are responsible for determining appropriate safety, security, environmental, and health practices or regulatory requirements.*

This IEEE document is made available for use subject to important notices and legal disclaimers. These notices and disclaimers appear in all publications containing this document and may be found under the heading “Important Notice” or “Important Notices and Disclaimers Concerning IEEE Documents.” They can also be obtained on request from IEEE or viewed at <http://standards.ieee.org/IPR/disclaimers.html>.

1. Overview

1.1 Scope

This guide covers suggested test requirements for power system protection scheme testing, system application tests, the scope and level of tests based on the application, and benefits of the overall protective schemes testing. This guide encompasses overall system testing procedures (generators, line, line reactors, transformer, capacitors, special protection schemes, end-to-end testing, distributed application within substation, etc.) and data collection requirements, as well as the test procedure definitions. This guide describes the methods, extent, and types of system tests for protection applications at various voltage levels. Control functions inherent to the protective systems are included. Importance of line testing, indirect trip applications, open/closed-loop tests, and dynamic/nonlinear tests are also covered.

1.2 Purpose

This guide is intended for power system protection professionals. It includes a reference list of type tests for protective devices as well as overall protection scheme performance tests for various types of protection schemes. The guide describes the methods, extent, and types of protection scheme tests. Interlocking and control functions inherent to the protective schemes are included.

1.3 General

Testing individual relays, or testing within the confines of one traditional protected-zone panel, is not comprehensive enough to demonstrate that the system is ready to respond to a real fault or emergency. This guide focuses on the general approach and procedures for testing protective relaying systems that include multiple interacting relay components, auxiliary devices, and power apparatus.

Many elaborate or wide area protection systems are installed to handle rare and critical events, and these systems must work as designed to avoid major system outages. Sustained operation in the field does not give the user benign opportunities to observe and correct performance issues. These systems need accurate and realistic simulation of these rare events for type testing and effective in-service maintenance tests.

This guide presents test approaches and procedures for the components of the system and the overall protection and control system functions. The testing of equipment in the system protection scheme, the associated communications equipment, the auxiliary power supplies, and the control of power apparatus are addressed. The system is tested as a functional unit when possible, but it may be necessary to test components or portions of the system in overlapping test schemes when it is not practical to test the whole system together. Much of the testing emphasizes a bottom-up approach, in which the basic behavior of scheme components is verified first, followed by testing of interconnected components in a function-oriented assembly.

The procedures focus separately on design testing, commissioning testing, routine maintenance testing, and ongoing performance assessment with a discussion of what each of these test categories aims to accomplish.

Testing recommendations in this document are intended not only to assist engineering and maintenance personnel in developing technical testing procedures, but also to help in planning testing resource requirements for discussion with utility management.

1.4 Types of applications

The three overlapping categories of system design and applications needing these specialized functional testing approaches are listed in 1.4.1 through 1.4.3.

1.4.1 Wide area special protection schemes incorporating power system measurements from multiple substations around the network

These types of schemes utilize communications systems to combine results or distribute the control action commands. The testing challenge lies in stimulating and observing the performance of the system as installed over its extended physical domain. The user needs robust verification of both security and dependability of the protection.

1.4.2 Wide or local area protection schemes based on exchange of data among relays and microprocessor-based devices on a communications data bus or local area network (LAN) or wide area network

The data communications networks perform the signal exchange previously handled by individually wired dedicated connections that the user can check with simple test instruments. The communications networks may be dedicated but are increasingly shared with other operating functions or even with the highly diverse utility information technology (IT) infrastructure. The testing challenge lies in verifying that the protection function performs with robust design margins, without imposing the need for impractical levels of expertise

in data transmission and protocols or specialized protocol analysis instruments. Testing also needs to demonstrate that no credible interference of unrelated communications traffic leaves the shared communications network unable to serve the critical protective function under test.

1.4.3 Local area protection schemes with complex wired interconnections of components, input signals, and control outputs

The objective is to verify the output or protection performance of the entire scheme over all the expected combinations or ranges of input conditions. The test can verify behavior by input stimulation and observation of the entire ensemble operating as a system. However, this may not show behavior or security margins in signals among the components, so some additional observation of these signals may be required. When a full input-to-output test requires more repetitive cases than is practical, it is sometimes acceptable to test individual components or portions of the scheme separately as long as the boundaries among the tested portions overlap. Every component or interconnection should have at least one functional test.

An example is an electromechanical transformer or generator relaying system with 10 or more relays, plus interconnecting wiring and auxiliary tripping devices such as lockout switches. Tripping and lockout operation may occur as a result of inputs to any of a number of measuring elements, each of which must be tested. In at least one case, the lockout switch should be operated and its ability to trip and lock out breakers should be confirmed. For many other test cases used to verify the relays that feed the lockout switch, the breaker tripping or the lockout switch operation can be blocked, as long as no wire or path is left untested.

1.5 Types of tests

The document addresses several testing situations in detail, as discussed in 1.5.1 through 1.5.4.

1.5.1 Application certification type tests in the factory or laboratory

The objective of application certification type tests (also known as functional tests) is to verify the engineering design and performance of the system and its components through simulation of the full range of expected operating conditions. These cases can be in the form of playback of simulation results or real-time interactive testing. Typically, the developers run such type tests only on a first production sample if more than one is to be built.

In the case of playback of simulated cases, the tests rely on power system or apparatus modeling, simulation, and tools to demonstrate the security and dependability of the scheme before shipping to the site. Features include comprehensive modeling of the application, standardized test cases, large variety of test cases to exercise design, and simulation of communications and environmental challenges of a field installation. The test personnel document the test cases and results in some detail. For a specialized protection system or critical application, representatives of the end user may witness some or all of the type testing process to learn the system and gain confidence.

In general, component devices of a system under test have been or should be type-tested according to relevant standards for the physical and electrical environment. For example, protective relays are tested according to specified revisions of IEEE Std C37.90™ as well as IEEE Std C37.90.1™, IEEE Std C37.90.2™, and IEEE Std C37.90.3™; such test results are documented separately. These well-defined product type tests are not discussed further in this document.

1.5.2 Commissioning tests (at installation site)

The objectives are to determine whether equipment was damaged or changed during shipping and field installation, to ensure that equipment is installed and wired properly, to verify that installers entered appropriate settings and option selections, and to observe interaction with the power apparatus. The test focus shifts from verification of design to verification that the system is working as designed.

The commissioning test objectives are as follows:

- a) Install and integrate the system components with the site current transformers (CTs), voltage transformer (VTs), sensors, communications systems, wiring, and auxiliary power supplies.
- b) To verify that factory-supplied connections are correct and complete.
- c) To ensure each component performs in accordance with vendor specifications and type testing for that component.
- d) Test interactions, and overall system performance, with a sampling of test cases across the spectrum of possibilities but not a comprehensive suite as is used for factory type tests.
- e) Test the overall scheme by simulating power system events that cannot be generated on demand, using techniques described in this guide. Examples include transient simulation, tests for abnormal conditions, end-to-end testing, and functional testing of applications using IEC 61850.
- f) Operate other power apparatus or secondary control systems in the vicinity to show that the system is secure and/or dependable in the face of spurious environmental influences or communications traffic.
- g) Verify proper mapping and operation of the protective device with other data/control systems to which it is interconnected.

1.5.3 Periodic maintenance tests

The objective is to detect in-service failures of components, wiring, interfaces, communications, or unwanted changes of setting or configuration.

- a) Assume the design requires no additional verification.
- b) Test for correctness of wiring or switching configuration that could conceivably have been changed by maintenance elsewhere in the substation, including polarity or phase rotation, and instrument transformer or other interface grounding/earthing.

Periodic testing should focus on carrying out steps that detect most in-service hardware failures and avoid additional testing that tends to reverify the design, software behavior, or the fundamental installation correctness that were already confirmed. Excessive testing risks accidental introduction of problems and work errors that leave the system unable to protect after the test is complete and the technicians have left the site. This is especially true for invasive testing that calls for taking systems out of service, disconnecting circuits, changing settings, or opening unit cases.

Note that for electromechanical relays, as well as solid-state and microprocessor-based devices, users have been accustomed to reverifying pickup characteristics during each periodic test because some internal failures can change these characteristics. Relay technicians open test switches and apply a large set of boundary tests from a computer-operated test set.

For microprocessor-based devices with self-monitoring and diagnostics, internal failures have different effects, most of which can be observed during normal operation via data communications or front-panel data checking. For example, metered nonfault trip data that the processor communicates or displays can show any measurement error that could influence trip characteristics. Although settings could be incorrect, they

can also be checked via data communications or the panel. The only element of the tripping chain that might need an overt periodic test is the trip contact and circuit to the breaker, and that can sometimes be tested via communications or the relay front panel. Periodic maintenance tests can thus be minimally invasive, and the risk of problems caused by maintenance activity is reduced. If the scheme is designed and installed with this opportunity in mind, the user may be then able to carry out some or all of the periodic checking without entering the substation.

In making efforts to detect every possible failure, the user should balance the risk from a missed element of low failure probability versus the maintenance risk of introducing a disruptive step to check it.

1.5.4 Troubleshooting tests following operations

It is important to emphasize the value of verifying overall system performance following correct as well as incorrect operations by retrieving and analyzing sequence-of-events and oscillographic records captured from various devices and recorders for nearby disturbances. It is also suggested that correct operations also be studied to verify security and quantify nearness to trip. Some key steps in reviewing performance of relay systems after operation include the following:

- a) Periodically review the application in light of power system evolution and protection and control system changes.
- b) Analyze relay or digital fault recorder (DFR) data from disturbances for which the protection system did or did not operate.
- c) Consider correctness of logic, characteristics, and set points.
- d) When problems appear, carry out commissioning-like tests to demonstrate continuing suitability or to verify needed changes.
- e) Make and verify needed changes to the periodic test procedures.

1.6 Applications for systems, schemes, and multistation testing

The document discusses examples of protection schemes and testing approaches for the following applications. In some applications, references are provided to other IEEE guides or standards where specific aspects of testing are covered.

Line protection

- Transmission
- Directional comparison pilot protection
- Multiterminal
- Tapped line configuration
- Line switching equipment integration
- Series compensated
- Shunt compensated
- Current differential or comparison
- Integrated relaying communications monitoring
- Conductor heating/sag

- Distribution circuits, including interaction with reclosers, switches, capacitor banks, monitors, load control systems, and other circuit equipment
- Integrated automatic reclosing and voltage/synch check
- Conditional single-pole tripping and reclosing

Transformer protection

- Multiwinding
- Phase shifting
- Tap changing
- Overload protection with distributed thermal inputs
- Distributed winding measurement or data acquisition systems
- Integrated load, life, and condition monitoring systems
- Predictive, acoustic, or partial discharge detection systems

Bus protection

- Low impedance
- Medium impedance
- High impedance
- Distributed measurement and control
- Configuration dependent protection zones and switching
- Postfault closing lockout
- Automatic reclosing

Shunt capacitor protection

Breaker failure protection and control

Reactor protection

- Voltage control
- Line reactors
- Current-limiting reactors

Wide area special protection schemes

- Generator or tie outage reconfiguration or load shedding
- Plant load or tie rejection
- Voltage collapse protection and restoration
- Out of step, synchrophasor-triggered, or phasor measurement unit (PMU)-based protection

Distributed load shedding schemes

- Frequency or voltage-based load shedding that is dependent on centralized system conditions or remote event triggers

There are many other power system apparatus, such as static VAR compensators, harmonic filters, and automatic transfer schemes, which in most cases are application specific and are not covered in this guide.

1.7 Considerations for testing and scheme self-monitoring

One important aspect of testing any scheme is the documentation. This documentation includes the procedures and results, verifying that tests have been conducted and schemes are performing within design and acceptable parameters. The procedures and test setups also ensure consistency in testing. Schemes can be simple, and the documentation may also be simple. When schemes are complicated and involve multiple owners and devices at sites, detailed documentation describing the steps necessary to accomplish this testing will make sure that these schemes are tested the same way each time to provide repeatability and comparison of test results. The procedures need to include test setups, equipment required, and procedures to isolate the system to be tested. When testing is conducted in an energized environment, additional steps are needed to ensure that all elements of the electric system are protected while testing is progress. Documentation of test procedures are usually retained to track performance history and for future maintenance purposes, and it is available as needed for demonstrating methods used for testing.

1.7.1 Built-in checks for internal or system problem identification

A critical aspect of testing is to develop an approach that can detect when the normal evolutionary changes in the power system or protective and communications systems surrounding the scheme under test threaten its ability to perform as designed. As the industry develops such adaptive testing approaches, the designers of components and systems should focus on incorporating the sensing and logic needed to look for impending trouble and make the system robust in the face of such gradual change.

For example, a system integrity protection scheme (SIPS), also known as a special protection system (SPS), might use an ON-OFF power-line carrier (PLC) channel to transmit a single critical status report between two substations. Many PLC channels are typically multiplexed through symmetric or skewed hybrids, line tuners, and capacitance coupled voltage transformers (CCVTs) and are dependent on tuned line traps and on the modal carrier propagation characteristics of the transmission line itself. For this example, the SPS is thoroughly tested during commissioning and a simplified maintenance test is periodically or automatically carried out after that. The PLC monitoring may include automatic check-back testing.

In subsequent years, several transformer taps are installed to serve new customers along the line. Additional PLC channels may be multiplexed with those that were operating at commissioning time, both on the line in question and on adjacent lines. At some point, the expanded combination of frequencies and signal levels combines with the multiplexing schemes and line propagation modes such that the simultaneous operation of two carrier sets not associated with the SPS will cancel the SPS carrier signal. If this circumstance occurs only during a fault, the SPS maintenance testing may show all is well until the SPS really must do its job. For a particular fault situation, the carrier state is not received and the SPS fails.

Although there are no convenient checklists to protect against all future changes, the designers and their testing approaches should include scheme verification in the face of routine surrounding events and changes that do not call for operation of the scheme under test or for restraint of the scheme. In the example above, using a frequency-shift carrier or continuously observable channel can combine with SPS carrier dropout monitoring that can point to trouble on the horizon.

In most cases, checks for nonfault behavior of components can passively monitor critical signals without adding links to the critical protective chain. In hard-coded or programmable logic of microprocessor-based devices, monitored critical signals can be posted as events or alarms to be checked by the user without disrupting the tripping chain. These signals can be supervised by independently programmed logic that filters the alarm cases without having any effect on tripping. The scheme designers should integrate this monitoring logic so that it is subjected to the full range of type and commissioning tests.

1.7.2 Drive for scheme and test simplicity

In designing for robustness, engineers often consider the effectiveness and complexity of the scheme and how it can be tested. During the engineering and design stage, consider the following factors and their impact on testing:

- Supervising elements, their setpoints, and how the elements have been optimized.
- Whether the design includes use of redundant elements, applied in parallel formation, and the impact on security/dependability of the application.
- Whether the scheme is voting or vetoing, and the impact of security/dependability of the application.
- Redundant systems may offer flexibility for testing of elements without removing protection from service during tests.
- Impact on scheme complexity: Complex systems have sometimes failed to perform adequately because of difficulty to test and/or identify fundamental design or application flaws.
- Test procedures and verification to return equipment to normal conditions after tests. Test switches and testing equipment present opportunities for test personnel to leave protective devices or systems in a nonfunctioning state.

1.7.3 Test from the bottom up

For all of type testing, commissioning testing, and maintenance testing, start with verification of the smallest elements to be verified. Determine what is assumed or known—for example, environmental tests have been performed on a numerical (microprocessor-based) device to be type tested in an SPS scheme; firmware design is assumed to be solid in a maintenance test. Check the points to be verified on these smallest units and then proceed to check the joint behavior of the next level of interconnected units. Continue until the highest overall system test is completed.

1.7.4 Overlap zones of testing

It is important to design the system and its maintenance test program for segmented testing or self-monitoring of the links in the protective chain. Maintenance verification by testing or observing segments is effective as long as the segments overlap. In other words, the interface between segments or links must be verified by observations during the test of the adjacent elements.

For example, a relay input may be isolated and a test signal applied to check for trip output via contact closure. Separately, the breaker may be tested by a manual trip. This pair of tests does not check the ability of the relay trip contact to trip the breaker—an undetected cold solder joint in the relay could pass an ohmmeter test and open up when a real trip is initiated. The overlapping test would be to apply inputs and check relay response as before and then to test breaker tripping by using the front-panel or data communications trip function to operate the breaker.

Also, there may be power system effects that need to be fed into all segments as a result of a specific segment action. Therefore, segmented testing should consider a scheme purpose and incorporate sufficient levels of overlapping to prove adequacy for overall scheme performance.

1.7.5 Make use of in-service experience

In many cases, faults or system events are used to validate performance of parts or whole protection systems. Events and oscillographic records are used to verify recently exercised elements of the scheme. If a relay in a scheme under test also tripped correctly for a routine fault, the trip output and trip circuit are probably working and can be left alone.

1.7.6 Use continuous performance checks for schemes using communications messaging

Many new protection schemes make use of control messaging or status and value reporting among multifunction relays, over an Ethernet LAN or other data communications media. The messages may be based on IEC 61850 generic object-oriented substation event (GOOSE) or generic substation state event (GSSE), modbus transmission control protocol (TCP), DNP3/TCP, or any of a number of other standard control protocols or vendor-specific protocols. Serial data links or networks such as RS422 or RS485 are also widely used for critical protection and control.

For Ethernet LANs and IEC 61850 GOOSE/GSSE applications in particular, IEEE Std C37.115™ provides reference background on the analysis of normal and transient levels of message traffic on the LAN. At the time that IEEE Std C37.115 was written, there was concern over the risk of performance degradation or lost messages due to collisions or LAN capacity during a data storm triggered by a multiple-contingency relaying situation at the substation. While system designers still need to pay attention to these possibilities, the newest LAN implementations are not vulnerable to these shortcomings. Managed Ethernet switches direct the message traffic and eliminate any opportunity for collision and message loss. Network links between microprocessor-based devices and their dedicated Ethernet switch ports operate at speeds between 10 MB/s and 1 GB/s, where a properly designed LAN will not introduce any rational level of message traffic with insignificant delays that could impact protection performance. Refer to IEEE Std 1615™ for the recommended practice for designing Ethernet networks in substations and to IEEE Std 1613™ for environmental and testing requirements.

Additionally, if the protection scheme includes application of cyber security communication links (i.e., routable protocols), it is important to verify the performance of the scheme, as well as test data communications channel integrity on a continuous basis. Refer to IEEE Std 1686™ for cyber security standards associated with devices used at substations. In such cases, communication link monitoring requires the following:

- For continuously streamed data, such as analog measurements or status reports, establish a predictable maximum time interval between messages in the never-ending transmission stream. The receiving microprocessor-based protection device with integrated communications interface then watches for the critical messages and raises an alarm if valid messages are not received in the expected time frame. This presumes that the integrity of the message is also confirmed via parity, cyclic redundancy check (CRC), or other message bit error detection methods available in the applied communications protocol. In such cases, corrupted messages can be alarmed along with missing messages.
- For transient control messages, such as a control command, it is important to define a companion nontrip monitoring message that is sent as a streaming message and used for monitoring the messaging path as explained above. The monitoring message must use the same data communications hardware, transmission path, and protocol and be as close as practical yet clearly distinguished from the rarely used control command. IEC 61850 GOOSE and GSSE messages used for control inherently offer this capability. The messages are time-tagged and constantly streamed in their quiescent state at a designer-set time interval when the station has no protection events in progress. All the relays that subscribe to a GOOSE message from a particular publishing relay watch for the stream of messages, and each can alarm if it is not receiving the stream of no-operate messages at the expected time intervals. Channel problems are thus caught when they occur as opposed to waiting for a mishandled fault to point to a

communications failure. The monitoring is complete from relay processor to relay processor, so periodic testing by personnel is neither necessary nor advisable. When a state change, such as a fault, occurs, IEC 61850 GOOSE defines a temporary acceleration of the messaging rate to ensure that all the subscribing relays have multiple opportunities to receive the critical tripping message without significant time delay.

GPS time tagging or sequential numbering of the messages can improve the quality and precision of the monitoring but is not always necessary. IEC 61850 GOOSE/GSSE includes this message identification feature by which subscribing relays can report the times of missing or corrupted messages.

2. Normative references

The following referenced documents are indispensable for the application of this document (i.e., they must be understood and used, so each referenced document is cited in text and its relationship to this document is explained). For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments or corrigenda) applies.

IEEE Std C37.90TM, IEEE Standard for Relays and Relay Systems Associated with Electric Power Apparatus.^{1,2}

IEEE Std C37.90.1TM, IEEE Standard for Surge Withstand Capability (SWC) Tests for Relays and Relay Systems.

IEEE Std C37.90.2TM, IEEE Standard for Withstand Capability of Relay Systems to Radiated Electromagnetic Interference from Transceivers.

IEEE Std C37.90.3TM, IEEE Standard for Electrostatic Discharge Tests for Protective Relays.

IEEE Std C37.99TM, IEEE Guide for the Protection of Shunt Capacitor Banks.

IEEE Std C37.116TM, IEEE Guide for Protective Relay Application to Transmission-Line Series Capacitor Banks.

IEEE Std C37.119TM, IEEE Guide for Breaker Failure Protection of Power Circuit Breakers.

IEEE Std C57.91TM, IEEE Guide for Loading Mineral-Oil-Immersed Transformers.

IEEE Std 643TM, IEEE Guide for Power-Line Carrier Applications.

IEEE Std 1613TM, IEEE Standard Environmental and Testing Requirements for Communications Networking Devices Installed in Electric Power Substations.

IEEE Std 1615TM, IEEE Recommended Practice for Network Communication in Electric Power Substations.

IEEE Std 1686TM, IEEE Standard for Substation Intelligent Electronic Devices (IEDs) Cyber Security Capabilities.

¹ IEEE publications are available from the Institute of Electrical and Electronics Engineers, 445 Hoes Lane, Piscataway, NJ 08854, USA (<http://standards.ieee.org/>).

² The IEEE standards or products referred to in this clause are trademarks of the Institute of Electrical and Electronics Engineers, Inc.

3. Definitions, acronyms, and abbreviations

3.1 Definitions

For the purposes of this document, *The IEEE Standards Dictionary: Glossary of Terms & Definitions*³ should be referenced.

3.2 Acronyms and abbreviations

ATP	Alternative Transient Program
BER	bit error ratio
BF	breaker failure
BFR	breaker failure relaying
CBM	condition-based maintenance
CCVT	capacitive coupled voltage transformer
CT	current transformer
DCB	directional comparison blocking
DFR	digital fault recorder
DNP	data network protocol
DTT	direct transfer trip
DUT	device under test
DUTT	direct underreaching transfer trip
EMTP	Electromagnetic Transients Program
EHV	extra high voltage
FSK	frequency-shift keying
GOOSE	generic object-oriented substation event
GPS	global positioning satellite
GSSE	generic substation state event
GSU	generator step-up
HV	high voltage
ICT	information and communication technology
IED	intelligent electronic device
IOU	input/output unit
LAN	local area network
LD	logical device
LN	logical node
MOV	metal-oxide varistor
MU	merging unit
OOS	out of step
PLC	power line carrier
PMU	phasor measurement unit
POTT	permissive overreaching transfer trip
PSTN	public switched telephone network
PUTT	permissive underreaching transfer trip
RAS	remedial action scheme
RF	reflected frequency
RUT	relay under test
SAS	substation automation system
SCADA	supervisory control and data acquisition

³ *The IEEE Standards Dictionary: Glossary of Terms & Definitions* is available at <http://shop.ieee.org/>.

SCL	substation configuration language
SDH	synchronous digital hierarchy
SER	sequence of events recorder
SIPS	special integrity protection scheme
SONET	synchronous optical network
SPS	special protection system
SWC	surge withstand capability
SWR	standing wave ratio
TMU	test merging unit
TCP	transmission control protocol
TOC	time overcurrent
TRV	transient recovery voltage
VLF	very low frequency
VT	voltage transformer

4. Types of tests

In this clause, different types of tests are described. Some of the tests are device specific, and others are application oriented.

4.1 Certification tests

Type tests are certification tests performed by a certification organization or application tests on demand of a user. Certification tests are objective and can be accepted by a wide range of users. Certification tests are normalized tests under normalized procedures and with normalized equipment. For numerical protection devices, type tests cover hardware as well as software. Each hardware or software version can be a different type. The results of these tests are acceptable to a wide range of users, independent of the application.

Certification tests consist of conformance tests and performance tests.

4.1.1 Conformance tests

The goal of conformance testing is to verify the performance of the protective device or protection system against a set of predefined specifications.

- *Functional conformance tests:* Functional conformance tests verify whether the functionality of a protective function is as expected. Tests are focused on verifying the general characteristics against specification by means of signals without transients and direct current (dc) components. Functional conformance tests are generally steady-state accuracy tests.
- *Technological conformance tests:* Technological conformance tests verify the response of the protective function to external disturbances and internal failures. Technological tests cover the verification of the hardware quality, a reliability assessment, and an evaluation of the self-supervision. The verification of the hardware quality includes insulation properties and environmental conditions (electromagnetic compatibility, mechanical, and climatic).

4.1.2 Performance tests

A performance test (also referred to as acceptance or type testing) is a type of certification test that describes the limits of performance of protective relays used in a specific application. The testing is a generic way to rate the performance of a specific relay. The test results clearly describe the ability of the relay to perform according to its specifications and the performance of the relay during certain types of common performance requirements and fault conditions. Test conditions are generally derived from testing

models based on a simple power system model. These types of tests are typically performed when evaluating a new relay for use on a specific power system, or, in some cases, when evaluating new firmware. See IEEE Std C37.231TM-2006 [B28]⁴ for additional information regarding firmware revision control. The severity of firmware changes can be used to determine whether a new suite of tests is needed. The general results from certification tests include operating speed, consistency and repeatability of performance, boundary conditions for optimal performance, understanding of settings methodology, and the suitability of this relay for typical applications. As an example, certification tests of a distance relay will illustrate operating speed of the distance element and the reliability of the distance element for zone boundary faults and during CCVT transients. These tests, therefore, determine the general suitability of a distance relay for extra high voltage (EHV) and high voltage (HV) protection applications.

The goal of performance testing is to verify the behavior of the protection under realizable network conditions. It includes aspects like dc offset, source-to-impedance ratio, fault resistance, various types of faults, and so on. In contrast to conformance testing, performance tests do not focus on how a certain function is performed within the protection but on what is to be expected from a function under certain power system conditions. In case of multifunctional protection, distinction can be made between function tests and scheme tests.

- *Functional performance tests:* At functional performance testing, each function is tested and evaluated separately. The performance of an individual protective function is examined in detail.
- *Scheme performance tests:* Scheme performance testing verifies the performance of a protective function under various conditions. Because numerical protection contains a large number of functionality combinations, it will be impossible to test them all. Scheme performance tests are therefore limited to a number of practical protection applications, with the protection schemes configured as applicable.

Software (firmware) upgrade of a protective function should be treated as testing a new protection type. Due to the interval of software upgrades, full replication of all tests may not be cost effective. Therefore, a limited program can be performed if, in an earlier stage, a complete type test is performed. The limited program should consist of the following:

- Tests to verify that the new or changed function works correctly.
- Tests to verify that no other functions are declining. This is more complicated because of the number of functions and possible combinations.

Some probabilistic analysis may help to determine which elements or hardware components need retesting.

4.2 Application tests

Application tests are driven by the user and are mostly subjective. Application tests are specific tests to determine the suitability of a relay for a specific protection system design application or location. Application tests are based on a detailed model of the power system and include performance testing against a wide variety of possible fault conditions. This type of testing typically uses transient simulation to replicate more accurately the behavior of the power system. The goal is to ensure a specific relay will perform for a specific application or location before actual installation. Although certification tests focus on specific relays, which are the basic building blocks, application tests may also be used to verify the entire protection scheme. Application tests are typically performed during the evaluation and design phases. The benefits of application testing are numerous. The application tests document that a specific relay, algorithm, or protection scheme is the correct choice for a certain set of power system conditions or criteria. It is typical, for example, to use a transient model of the specific power system, using multiple fault conditions, to determine the suitability of a distance relay. System integrity protection schemes require significant

⁴ The numbers in brackets correspond to those of the bibliography in Annex A.

application testing as transient system modeling is inherently used to design the scheme and specify the scheme response to power system events.

A second benefit of application testing can be the determination of, and documentation of, appropriate settings. Application testing verifies the performance of a protection system in total response and will highlight the failure or overlap of specific elements of the scheme. The operating settings of these elements can then be modified based on the results of the application testing.

The following application tests are based on the use of transients for testing protective relays in order to simulate the behavior of the network during faulted conditions:

- Fault resistance
- Current transformer saturation
- Potential transformer transients

Commonly practiced methods of creating test files for transient testing include use of transient signals obtained from fault recorders (COMTRADE format), generating test files using simulation programs in combination with playback, or closed-loop test equipment such as real-time simulators. Refer to IEEE Std C37.111™-1999 [B25] for information related to the COMTRADE file formatting and standard.

4.3 Commissioning tests

Commissioning tests are intended to ensure the protection system will operate as designed after field installation. These tests verify the individual components, interactions between components, communications system, and scheme redundancy along with wiring and installation. These basic tests must be performed for any new installation or significant modification to an existing installation and are typically combinations of certification and application tests. The certification tests performed during commissioning verify that elements perform in a field installation in a manner consistent with laboratory results. This step is important for equipment with performance that varies due to environmental conditions or age of components such as electromechanical relays. Application tests performed during commissioning verify that the total installed scheme works as designed and intended, especially in regard to installation accuracy and interaction between various protection and control system components.

Commission testing is vitally important, as these tests prove that the actual installed system will work as designed. Commissioning tests can become very advanced. End-to-end testing of transmission lines is one advanced method, ensuring that units at both ends operate correctly. The most important benefit of commissioning tests is verifying that the protection and control system works in the field as it was designed. A second benefit is documentation of field performance as a benchmark for verifying performance for future tests.

For the elements or features that have been set on a device, the tests normally follow the functional hierarchy of the protection system in the following order:

- Check the available system parameters measurements and make sure that they meet the technical specifications.
- Test the enabled and configured protection elements.
- Test the built-in protection schemes.
- Test the multirelay protection schemes.

Commission testing of an entire system is also intended to verify the hard-wired or communication-based interfaces between the multiple microprocessor-based devices included in a protection scheme, or other

distributed applications. The interface with the auxiliary contacts of the breaker and its trip coils are generally included as part of the tests.

Commissioning tests may require the use of multiple synchronized test devices in order to verify the performance of protection schemes or other distributed applications. Proper simulation of abnormal conditions for each of the devices in a scheme is essential for the testing.

In summary, commission testing is used to make sure the protection system is properly installed and working as expected in a substation.

4.4 Maintenance tests

Maintenance tests are specific tests to validate that the protection and control system is operating correctly after a period of time of field installation. Some of these tests are calibration tests to confirm that individual components are still operating within desirable performance parameters. This type of test is especially vital for the components susceptible to degraded or changing characteristic due to aging and wear. Another type of test is application tests. Application tests are performed to verify that the total protection system works, from measurement of power system values, to properly identifying fault characteristics, to the operation of the interrupting device and associated interlocking with automatic or manual restoration devices and schemes. One form of maintenance testing involves performing forced outage of protective equipment when performance of the respective scheme is identified as questionable and immediate attention to servicing the relay or the scheme is needed.

There are different philosophies concerning when it is appropriate to perform maintenance tests in an attempt to best balance assurance that the protection system will perform correctly versus the costs involved in maintaining the system. Aside from forced outage testing, there are two basic methodologies in use that are time-based maintenance and condition-based maintenance practices.

Periodic maintenance testing is performed to ensure that the protection and control system is operating correctly after a period of time of field installation. These tests may be used to ensure that individual components are still operating within acceptable performance parameters—this type of test is needed for components susceptible to degraded or changing characteristics due to aging and wear. Full system performance tests may be used to confirm that the total protection system functions from measurement of power system values, to properly identifying fault characteristics, to the operation of the interrupting device and associated interlocking with automatic or manual restoration devices and schemes.

Time-based maintenance is based on scheduled intervals for review and maintenance of the system, to demonstrate that routine testing of the system and system components are performed. Test schedules are generally determined by operating experience with a system or device, manufacturer's recommendations, and the availability of resources to perform the testing. Periodic testing may include a review of the recent power system activities on the particular terminal and whether the entire protective system has operated correctly since the last scheduled interval. If it is determined that a protection system and scheme has performed correctly, the interval may be adjusted based on most recent operational experience on the respective terminal. Similar to performance-based maintenance, condition-based maintenance includes examination of the relay system, history of specific systems and devices, and operating experience to perform maintenance only when necessary to ensure adequate performance of the protection system.

Intelligent electronic devices, such as microprocessor-based protective relays, add an additional form of maintenance testing, which is the ability to perform continuous self-monitoring for correct performance of the device. Self-monitoring capabilities vary between devices and may include the ability to monitor the incoming analog measuring circuits, the device output contacts, time synchronization signals, communications signals, internal hardware (including battery status and system board voltages), nonvolatile erasable programmable read-only memory, and the internal software algorithms. Failure of a self-test routine typically generates an alarm available through supervisory control and data acquisition

(SCADA) communications and output contacts. Certain self-test alarms may disable the functioning of the device.

Troubleshooting operating problems, from a protection system testing perspective, is generally a combination of commissioning tests and calibration tests, designed to identify specific components or specific parts of the protection system design that do not provide the desired operation results. Troubleshooting always involves good engineering practices and experience to identify the cause of operating problems.

4.4.1 Maintenance practices

Maintenance and test programs that often incorporate the following types of maintenance practices:

- a) *Time-based maintenance (TBM)*—Externally prescribed maximum maintenance or testing intervals are applied for components or groups of components. The intervals may have been developed from prior experience or manufacturers' recommendations. The TBM verification interval is based on a variety of factors, including experience of the particular asset owner, collective experiences of several asset owners who are members of a country or regional council, and so on. The maintenance intervals are fixed and may range in number of months or in years.

TBM can include review of recent power system events near the particular terminal. Operating records may prove that some portion of the protection system has operated correctly since the last test occurred. If specific protection scheme components have demonstrated correct performance within specifications, the maintenance test time clock is reset for those components.
- b) *Performance-based maintenance (PBM)*—Maintenance intervals are established based on analytical or historical results of TBM failure rates on a statistically significant population of similar components. Some level of TBM is generally followed to justify continued use of PBM-developed extended intervals for low occurrence of test failures or in-service failures.
- c) *Condition-based maintenance (CBM)*—Continuously or frequently reported results from nondisruptive self-monitoring of components demonstrate operational status as those components remain in service. Whatever is verified by CBM does not require manual testing, but taking advantage of this requires precise technical focus on exactly what parts are included as part of the self-diagnostics. Microprocessor-based protective relays that perform continuous self-monitoring to verify correct operation of most components within the device. Self-monitoring capabilities may include the alternating current (ac) signal inputs, analog measuring circuits, processors and memory for measurement, protection, data communications, trip circuit monitoring, and protection or data communications signals. For those conditions, failure of a self-monitoring routine generates an alarm and may inhibit operation to avoid false trips. When internal components, such as critical output relay contacts, are not equipped with self-monitoring, they can be manually tested. Method of testing may be local or remote, or through inherent performance of the scheme during a system event.

The TBM is the overarching maintenance process of which the other types are subsets. Unlike TBM, PBM intervals are adjusted based on good or bad experiences. The CBM verification intervals can be hours or even milliseconds between nondisruptive self-monitoring checks within or around components as they remain in service.

TBM, PBM, and CBM can be combined for individual components, or within a complete protection system. Figure 1 illustrates the relationship between various types of maintenance practices described in this section. In the Venn diagram, the overlapping regions show the relationship of TBM with PBM historical information and the inherent continuous monitoring offered through CBM. This figure shows:

- *Region 1:* The TBM intervals that are increased based on known reported operational condition of individual components that are monitoring themselves.
- *Region 2:* The TBM intervals that are adjusted up or down based on results of analysis of maintenance history of a statistically significant population of similar products that have been subject to TBM.
- *Region 3:* Optimal TBM intervals based on regions 1 and 2.

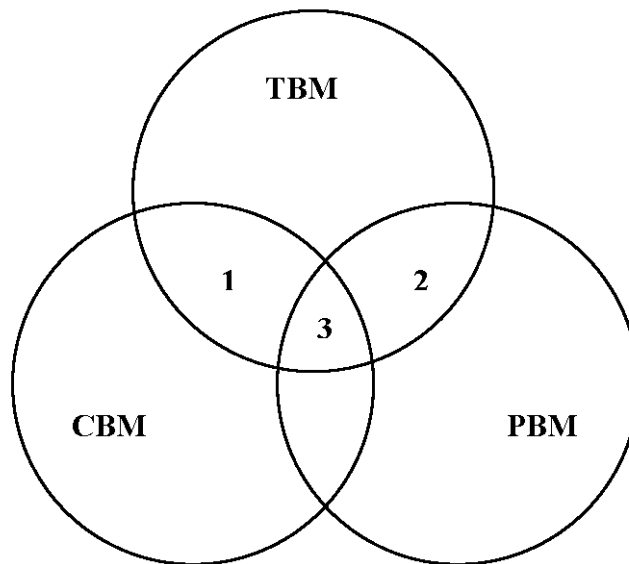


Figure 1—Relationship of time-based maintenance types

4.4.2 Regulatory considerations

It is important to the reliability of the electric system that protection and control systems function properly. Malfunctioning systems can contribute to major power system outages and widespread cascading events. Maintenance programs have demonstrated benefits in uncovering problems and allowing the problems to be addressed under a controlled power system environment. It is important to follow prudent maintenance programs to uncover problems and hidden failures in advance.

The effectiveness of a maintenance program is often tracked and determined by the asset owner. These tracking mechanisms allow the owner to optimize the program based on the application. However, when the performance of a protective device or system has a greater impact to the overall power system, the proper performance of the protective system will benefit the entire electrical grid, which may be composed of several interconnected power systems, or in some cases possibly part of a regulatory controlled electric system. In some countries or electrical grid systems, the regulatory agency may require evidence that the asset owners each have established a prudent maintenance program that meets a minimum level of standards and practices established by the regulatory body. Furthermore, the regulatory agency may require evidence that the owner is performing maintenance based on the program. Depending on the level of regulatory oversight, the asset owners may be asked periodically to either voluntarily, or through a cohesive and collective established audit process, or both, demonstrate that they have met their obligations to maintain the protection and control system.

In a regulatory system, the owner may be asked to certify that he or she can perform the following tasks:

- Demonstrate and submit detailed maintenance records and that asset owners are cognizant that regulatory agencies may require verification of the maintenance program, including evidence that protection systems and components are being maintained and tested per the owner's program.
- Submit a program documenting the methodology or philosophy behind the owner's program.
- Show a tracking mechanism and archiving system for the maintenance records related to the protection and control equipment and systems.

An example of a regulatory agency that establishes reliability standards and compliance measures is the North American Electric Reliability Corporation (NERC). NERC has established some standards and requirements (see NERC [B33]) of a Protection System Maintenance Program and a technical document that describes maintenance program options (NERC [B34]).

NERC and its regional reliability organizations (RROs) audit asset owning organizations across North America for compliance with these maintenance standards. Organizations found to be deficient in compliance with these standards are subject to serious fines, depending on the severity of the infraction, and they must also carry out a corrective action program.

For example, the NERC Standard for Protection System Maintenance and Testing is enforced for the bulk electric system. This standard does not impose specific test or maintenance procedures, or time intervals. Rather, it requires the asset owner to establish its own maintenance practices and include the following:

- A documented maintenance program.
- A documented basis for that program.
- Documentation that tracks the program and proves that it is being carried out as described, consistently and completely.

Note that the NERC definition of a protection system includes all of the following:

- Protective relays.
- Instrument transformers and sensors of electrical quantities needed for fault protection.
- Communications systems needed for relaying or protective tripping.
- DC station batteries supplying the protection system.
- Breaker tripping and control circuits, including auxiliary tripping and lockout relays, and primary equipment status indications required for correct relaying operation.

Similar programs are established in other interconnected electrical systems and countries.

4.5 Example of test setup configurations and equipment (end-to-end testing)

To perform end-to-end testing, some basic equipment is needed at both ends of the line under test. In this subclause, a list of recommended equipment is provided for reference purposes. This listing can be used in conjunction with the established testing practices of the owner of the protection equipment. The following description applies specifically to two terminal lines but can be extrapolated to three or more terminals by including additional sets of equipment and the necessary personnel.

This list of recommended equipment is based on having qualified personnel and equipment at both ends of the transmission line for which the protection is being tested. There are techniques for having personnel at one terminal only and remotely controlling the activities at the opposing terminal. Refer to Schreiner and Kunter [B35] for more information.

The following equipment is recommended for use in the end-to-end testing of transmission lines.

a) *Test equipment*

- 1) Interface to microprocessor-based device: A computer with appropriate manufacturer-specific software is often used in order to communicate with the microprocessor-based device under test to monitor performance, view/retrieve data, and possibly modify settings and application logic.
- 2) Test equipment: To test the devices, test equipment capable of being time synchronized and to provide three-phase voltages and currents are often used. In some cases, such as line differential, three-phase voltages may not be essential but are useful for testing the performance of ancillary or backup functions.
- 3) Fault simulation software: Software is needed that can generate fault sequences. The output from this software is used by the primary injection equipment and provides the sequence information and waveforms necessary for the test. This software may be associated with the specific primary injection equipment or may be some third-party software that has output data format compatibility with the primary injection test equipment.
- 4) Fault recorders: To monitor all the requisite test points, the use of a fault recorder at each site may be needed to capture information that is not already recorded by the microprocessor-based device.
- 5) Time coordination: Time coordination at both terminals of the transmission line is essential in performing end-to-end tests. A global positioning satellite (GPS) receiver that provides an accuracy of 10 μ s (which is equivalent to an angle of 0.216° at 60 Hz) or better should be used. A suitable GPS receiver is required at both ends of the transmission line.

NOTE—Existing GPS receivers at the test sites may be loaded to their maximum output capability, and it would be prudent to check that enough signal strength is available prior to commencing the test. An oscilloscope can be used to measure the voltage level of the GPS signal, and this can be compared with manufacturer specifications. The GPS signal is connected to both the microprocessor-based device under test and the test equipment. This time synchronization is used to coordinate the start of the test cycle at both ends of the transmission line and to time-stamp the data accurately. Signal strength at the receiving end should be verified prior to testing.⁵

- 6) Miscellaneous equipment: In addition to the above equipment, standard miscellaneous devices and components such as multimeters, connector cables from the microprocessor-based device to the laptop, jumpers, tools, and test leads may also be required for testing purposes.

b) *Communication equipment*

- 1) Data: Many multiterminal protections (for example, line differential relays) pass such data as voltage, current, trip signals, and time stamps among each other over existing communication channels in the normal course of operation. Additional data transmission requirements for testing purposes may not be necessary in these cases. For protection schemes where power system data is not normally passed from one terminal to the other (for example, distance protections where only a permissive signal may be sent), some additional method may be required such as a modem connection. However, this data transmission requirement may not be necessary in most cases as coordinated testing schemes from test equipment can be used and data can be retrieved from the test equipment and microprocessor-based devices at each site after the tests are completed. In the planning stages of the test, determine what data are required at both ends during the test and how to obtain that data.

⁵Notes in text, tables, and figures of a standard are given for information only and do not contain requirements needed to implement this standard.

- 2) Voice: A voice channel is necessary for staff to communicate with each other and system control operators. This channel can be anything that is convenient and reliable such as a cell phone or microwave/fiber channel.

The configuration in Figure 2 can be used to perform end-to-end testing of a two-terminal transmission line. The test equipment injects required three-phase voltages and currents into the protection under test. The test equipment also monitors the trip output, breaker failure initiate, transfer trip receive, and transfer trip send signals from the protection. GPS satellite receiver clock synchronization is used in order to allow comparison of data between the two terminals. More detailed description of end-to-end testing is available in the line protection section.

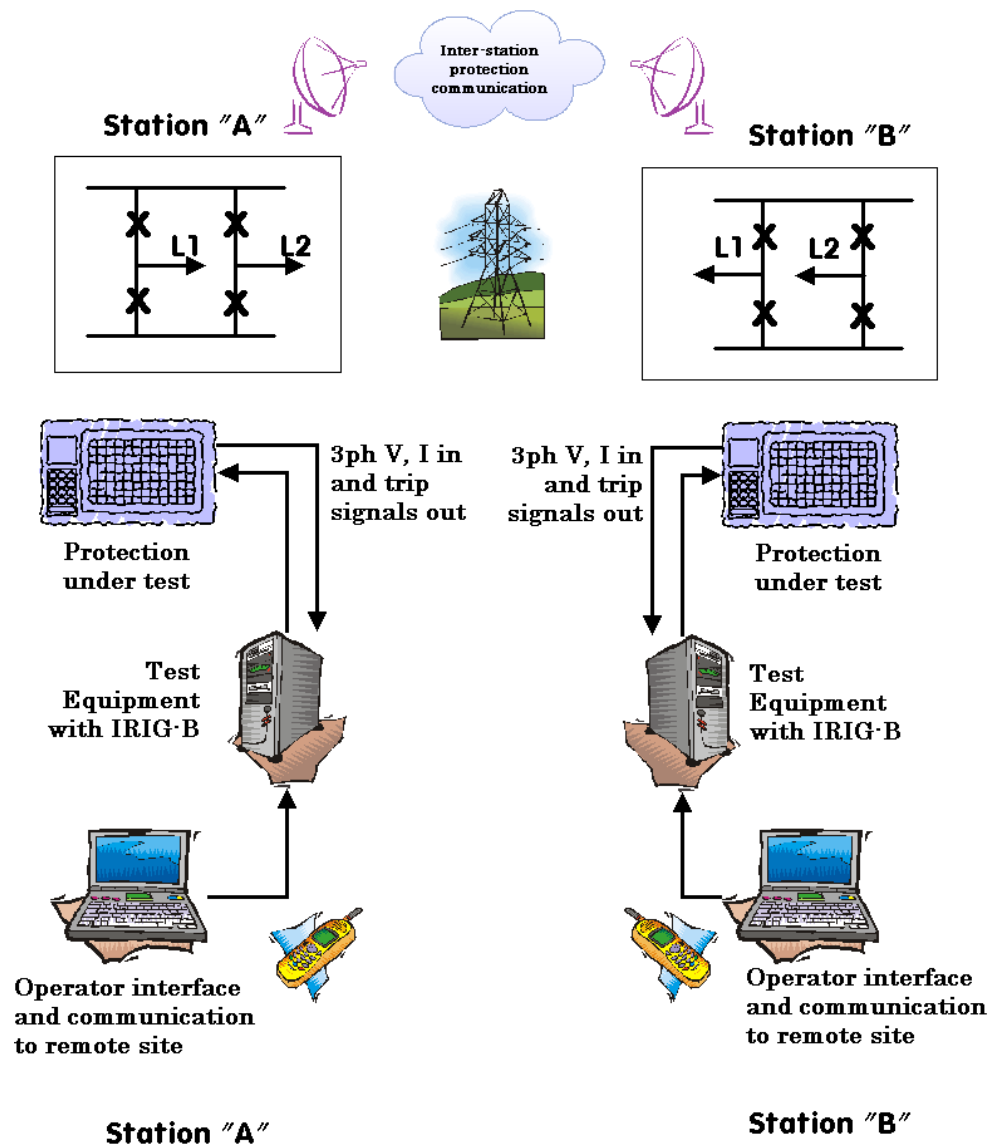


Figure 2—Example setup for transmission line end-to-end testing using GPS

4.6 Methods for generating test modules and cases

4.6.1 Fault studies

A test module comprises currents and voltages with/without external logic inputs (for example, digital signals for fault inception point or reclosing command) that need to be applied to a protection device or system. In order to generate test modules, specific fault studies need to be conducted and analyzed. One has to make sure that a specific test set can handle these quantities. Otherwise, some compromise or adjustment has to be made for accommodating the test set.

- In general, there are 11 types of faults: ABC, ABCG, ABG, BCG, CAG, AB, BC, CA, AG, BG, and CG. However, there are variations in the way these faults occur.
- Simultaneous faults (unusual). There can be simultaneous faults of two types mentioned above at the same or different location. For example, BC and AG fault at the same time. Or AG and BG demonstrate fault resistances at the same time. Also, a conductor can break and fault to ground, causing open phase with line-to-ground fault.
- Sequential faults (unusual). There can be more than one fault in power system, particularly during bad weather conditions. This will test relays that can experience external faults or external faults followed by an internal fault.
- Intercircuit/cross-country faults. A fault can occur between two lines operating at same voltages (intercircuit) or different voltages (cross-country) but located on the same tower. For example, phase A of a 230 KV line can be faulted to phase B of another 230 KV or 69 KV circuit on the same tower or sharing the same right of way.
- Evolving faults. A fault may start with one phase and evolve into other phases within a time period. Here, the speed of the relay may be slower because of phase-selection logic. For example, the fault can start with AG for one cycle followed by AB or ABG for three cycles.
- Fault locations. When deriving the test currents and voltages from fault studies, faults should be created on the line at different points. Usually, a close-in fault, middle of the line, end of the line, and in the reverse direction close to the bus will be adequate. If there are parallel lines, a fault on the parallel line should be created to see the effect of zero sequence mutual coupling. When applicable, the effect of sequential clearing on the adjacent line is tested.
- Fault duration. Fault duration can be anywhere between 0.5 cycles and a few seconds to test various aspects of a protective systems logic. A self-clearing fault may last 0.5 to 1 cycle.
- Faults through reclosing cycles. This is an extension of fault duration. Here, the fault currents and voltages may change after reclosing. If it is high-speed reclosing from both ends, the fault current reversal can occur within a cycle or more that can be experienced by a parallel line as an external fault.
- Varying fault impedance helps determine protection sensitivity, phase selection, and time coordination.
- Varying fault inception angles. For example, simulating different fault types with 15° or 30° intervals helps verify protection performance under various dc offset conditions.

4.6.2 Fault data assembly

Compilation of fault data usually consists of gathering the prefault, fault, and postfault quantities. Three-phase voltages are needed. Depending on the type of test, single or three-phase currents may be needed.

- *Prefault.* Prior to a fault, the line can be loaded between minimum and maximum. If the fault is sequential, i.e., an external fault with a subsequent internal fault, then prefault can be external fault quantity. The prefault time can be set from a few cycles to many seconds.
- *Fault.* Fault quantities that are derived from fault studies or selected may last for three cycles to a few seconds, which should be determined by the user.
- *Lines with automatic reclosing.* For lines with automatic reclosing, two sets of fault quantities may be needed to simulate reclosing interval. One set is for the initial fault, followed by dead time/band (open breaker) before reclosing with another set of test quantities. For external fault simulations adjacent to the line position under test, the impact of automatic reclosing on the adjacent line should be considered as part of the test. For example, changes in line loading characteristics after the initial fault may need to be considered as part of the automatic reclosing. Other examples include voltage and current oscillations after the initial fault.

4.6.3 Transient simulation

Protection systems or relays are exposed to transient currents and voltages in various circumstances as pointed out below. This transient situation can best be simulated using time-domain simulation programs described more in depth in later sections of this guide. The outputs from these programs can be downloaded to an active test set that can be activated for testing. Transient simulation tools assist in preparing test cases that may include the following:

- *DC offset.* The fault current may include dc offset, based on factors such as X/R ratio and point-on-wave incidence. The dc offset may have influence on the performance of a relay. The relay can overreach/underreach unless the relay filters the dc. The speed of the relay may be affected, too. The offset current can be simulated by transient simulation programs.
- *Power swing simulations.*
- *CT saturation modeling.* A heavy fault current or presence of dc offset current can saturate a CT, causing a distorted secondary current waveform. Relay performance can be degraded due to this distorted waveform.
- *CCVT subsidence transients and high-frequency ring behavior.* A CCVT contains capacitors, inductors, and a voltage transformer. Any change in power system voltage results in transient energy adjustment within these components that causes nonfundamental frequency to appear in the voltage waveforms, which affects the performance of equipment.
- *Subsynchronous fault current.* A subsynchronous fault current can occur in a power system having series compensation. This subsynchronous current can degrade the performance of the distance function.
- *Line energization.* Line energization transients can contain harmonic currents and voltages. For long lines, sometimes line reactors are used to control the voltages. Line capacitance and reactor impedance can produce resonant currents. Relays can be affected by these harmonic transients, which may last for few to several seconds.
- *Transformer (local and remote end) energization.* Sometimes, a transformer is part of a line zone of protection. This transformer can be energized by a breaker or a disconnect switch. During transformer energization, current containing harmonics can last many seconds. Because of the saturation effect of the transformer, harmonic resonance can occur. Relays can be affected by these transient currents and voltages.

- *Voltage source location (i.e., CCVT).* Location of voltage source has impact on distance measuring elements, for example, on series compensated lines.
- *Fault location and characteristics.* Variations in fault location and characteristics such as incipient angles, fault impedance, and so on, have an impact on the performance of the protective device.
- *Current differential protection.*

4.6.4 Power swing abnormal conditions

Transmission line relays are designed with “out-of-step” (OOS) elements (i.e., out-of-step tripping or power swing blocking) by measuring the impedance locus. Examples include time delay between two impedance characteristics, one encompassing the other. The applied voltage, current, and phase angle can be manipulated in a dynamic test simulator to move the impedance trajectory from the outside characteristic to inside characteristic beyond a set time. This method is generally used for blocking function. Similarly, tripping functions are designed by moving the trajectory from outside to inside to outside within a time frame.

It has been observed by some power system engineers that the traditional testing methods for microprocessor distance elements may not work on OOS elements, considering that out-of-step swings are three-phase phenomena and are more slow-moving and gradual than faults. As with other protective elements, it is crucial that the functions are adequately tested prior to placing them in-service.

It should be noted that it is generally inaccurate to test OOS elements by examining the results of the stability program and the R-X impedance swing locus, picking out several states of a swing condition and playing those states through the relay, trying to make the transition as smooth as possible. The reason is the step change between states does not accurately reflect the actual impedance transitions the relay will experience. Figure 3 illustrates stable and unstable swings as generated by a transient stability program, using 0.25 cycle steps, superimposed on line protection and out-of-step characteristics.

It has been proven that it is possible to take the raw positive-sequence voltage and R-X output from a dynamic stability program (using power system load flow modeling), calculate balanced three-phase quantities for each time step, and then translate this data into COMTRADE waveforms that can then be imported into modern relay test software that can play the waveforms through a relay. Figure 4 and Figure 5 illustrate an impedance trajectory generated by a stability program and the resulting COMTRADE waveforms in a relay testing program.

One challenge for out-of-step relays is the case of a fault that occurs during a power swing when the distance function has been already blocked. Again, the testing of these functions requires a simulation as close as possible to the real system conditions and at the same time needs to take into consideration the capabilities of the test equipment. Because testing tools normally generate the simulated current and voltage signals based on built-in modules or replay of COMTRADE files, it is clear that the following two approaches are possible: 1) use of a testing tool designed to simulate power swing conditions (synchronous or asynchronous) and faults that occur during a power swing, and 2) play COMTRADE files for power swing conditions (synchronous or asynchronous) and faults that occur during a power swing. Such files can be generated using off-the-shelf transient simulation programs or can be produced from disturbance recorders capturing real events.

Figure 6 and Figure 7 show an asynchronous power swing and asynchronous power swing with a single phase to ground fault that can be used for testing the power swing blocking function of distance relays.

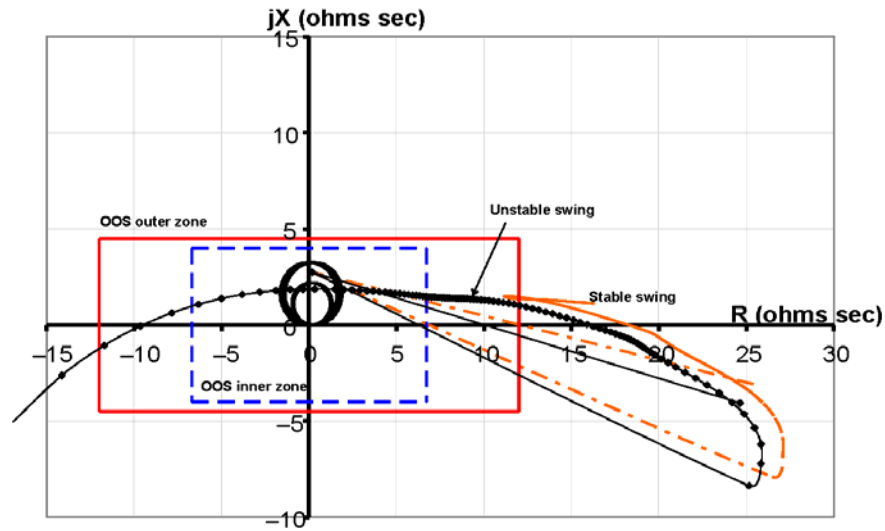


Figure 3—OOS impedance trajectory from dynamic simulation using transient stability program

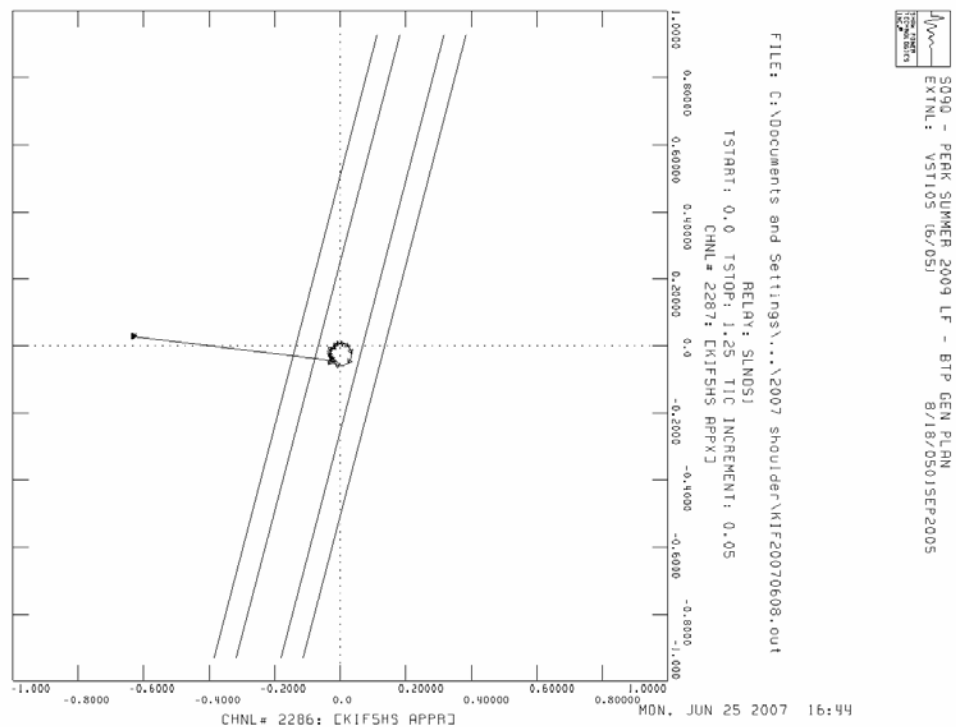


Figure 4—OOS impedance trajectory from dynamic simulation using transient stability program

IEEE Std C37.233-2009
IEEE Guide for Power System Protection Testing

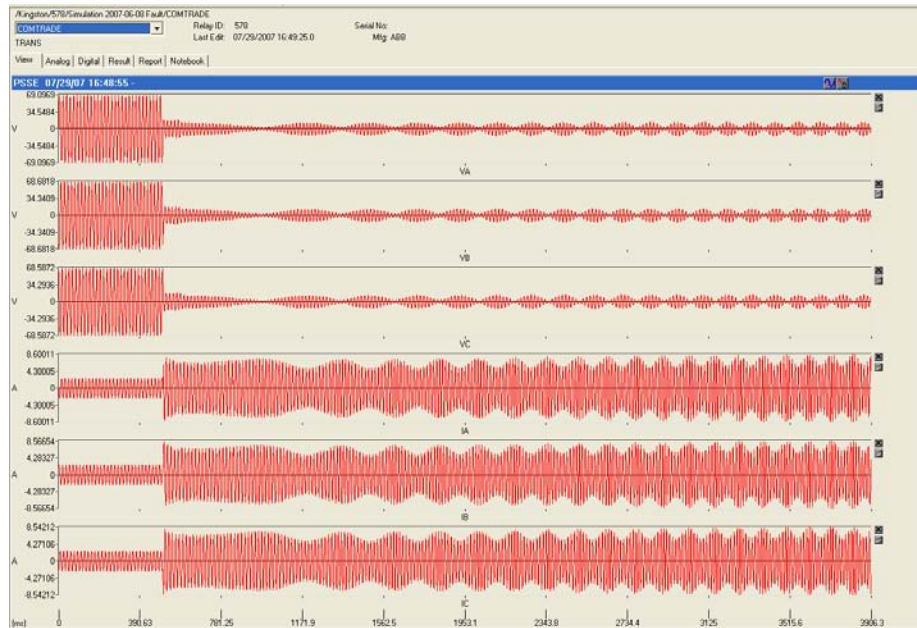


Figure 5—Resulting three-phase voltages and currents

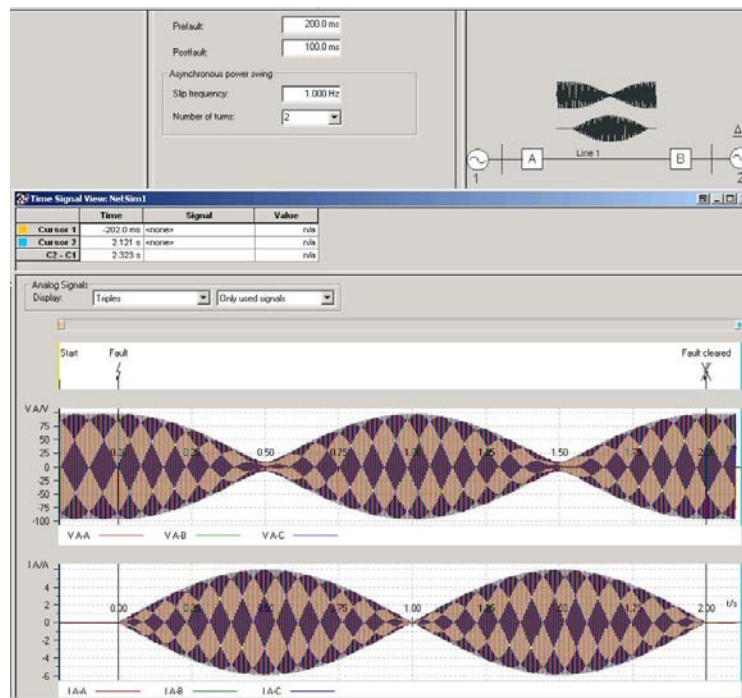


Figure 6—Asynchronous power swing simulation

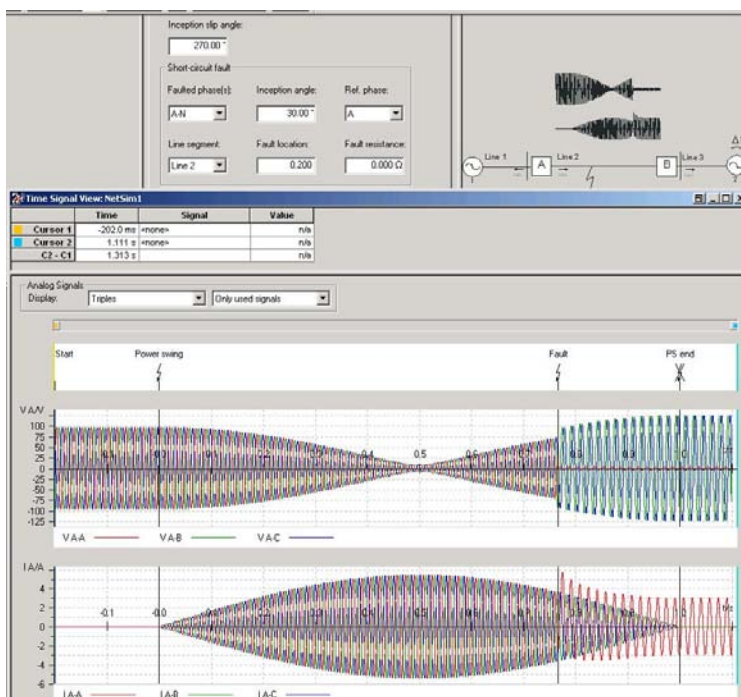


Figure 7—Asynchronous power swing with single-phase-to-ground fault simulation

4.6.5 Real-time simulation for transmission line relay performance evaluation

Power system simulations for relay performance evaluations are often conducted by users as well as by manufacturers to verify the performance of a newly developed relaying system or to verify the performance of an existing product in some special situations. Real-time simulation testing is covered in detail in the line protection section.

Power system simulation has been used for the relay performance evaluation for many years. The simulation tool should be easy to configure, should be able to simulate all power system contingencies, and provide means to analyze test cases automatically. The simulator should operate in a closed-loop mode with relays tripping and reclosing circuit breakers within the simulator. Performance evaluation of relays may take anywhere between 2 days and 2 weeks in most applications, depending on the complexity of the relaying system. Simulation tools such as real-time simulators can also provide means for testing of back-up elements, sympathy trips, voltage collapse, and other slow events that require interactive testing.

4.7 Analyses and retention of test results

The goal of analyzing test results is to determine the performance of relay systems. This analysis may determine whether the scheme operated correctly or whether the scheme has any subtle and/or noncritical problems. It may help establish a historical reference that will help in determining degradation of the system over time, and the analysis can even help determine component failure.

Systems are tested initially from the component level to the overall system. For example, a line relaying system may have each individual relay tested for specific calibration, but fault simulation tests will be applied at all terminals of the line to determine how the entire line relaying system functions. Frequently, routine testing no longer involves component testing and will consist of an overall system test. Component testing is only performed during initial commissioning of a system or after major or significant changes.