



IEEE Guide for Power System Circuit Breaker Failure Protection

IEEE Power and Energy Society

Developed by the
Power System Relaying and Control Committee

IEEE Std C37.119™-2025
(Revision of IEEE Std C37.119-2016)

STANDARDS

IEEE Guide for Power System Circuit Breaker Failure Protection

Developed by the

Power System Relaying and Control Committee
of the
IEEE Power and Energy Society

Approved 10 September 2025

IEEE SA Standards Board

Abstract: Methods to protect a power system from faults that are not cleared because of failure of a power circuit breaker to operate or interrupt when called upon by a protective relay are described in this guide. The intent is to provide the reader with a guide on how to detect when a circuit breaker has failed to clear a fault and how to electrically isolate the fault after the circuit breaker has failed to clear it. Additionally, schemes that provide primary protection of the power system from performance failures of the power circuit breaker other than fault clearing failures such as failure to operate, either tripping or closing, manual or automatic, are also described. Such schemes, when applied, are typically integrated as a part of the overall breaker failure protection scheme. Also covered are recent practices that take advantage of new technologies.

Keywords: BFP, breaker failure, breaker failure protection, circuit breaker, fault, IEEE C37.119™, power system

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

Copyright © 2026 by The Institute of Electrical and Electronics Engineers, Inc. All rights reserved.
Published 30 January 2026. 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 979-8-8557-3021-0 STD28572
Print: ISBN 979-8-8557-3022-7 STDPD28572

IEEE prohibits discrimination, harassment, and bullying.

For more information, visit <https://www.ieee.org/about/corporate/governance/p9-26.html>.

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.

Important Notices and Disclaimers Concerning IEEE Standards Documents

IEEE Standards documents are made available for use subject to important notices and legal disclaimers. These notices and disclaimers, or a reference to this page (<https://standards.ieee.org/ipr/disclaimers.html>), appear in all standards and may be found under the heading “Important Notices and Disclaimers Concerning IEEE Standards Documents.”

Notice and Disclaimer of Liability Concerning the Use of IEEE Standards Documents

IEEE Standards documents are developed within the IEEE Societies and the Standards Coordinating Committees of the IEEE Standards Association (IEEE SA) Standards Board. IEEE develops its standards through an accredited consensus development process, which brings together volunteers representing varied viewpoints and interests to achieve the final product. IEEE Standards are documents developed by volunteers with scientific, academic, and industry-based expertise in technical working groups. Volunteers are not necessarily members of IEEE or IEEE SA, and participate without compensation from IEEE. While IEEE administers the process and establishes rules to promote fairness in the consensus development process, 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.

IEEE makes no warranties or representations concerning its standards, and expressly disclaims all warranties, express or implied, concerning this standard, including but not limited to the warranties of merchantability, fitness for a particular purpose and non-infringement. In addition, IEEE does not warrant or represent that the use of the material contained in its standards is free from patent infringement. IEEE standards documents are supplied “AS IS” and “WITH ALL FAULTS.”

Use of an IEEE standard is wholly voluntary. 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.

In publishing and making its standards available, IEEE is not suggesting or rendering professional or other services for, or on behalf of, any person or entity, nor is IEEE undertaking to perform any duty owed by any other person or entity to another. Any person utilizing any IEEE Standards document, should rely upon his or her own 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.

IN NO EVENT SHALL IEEE BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO: THE NEED TO PROCURE SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE PUBLICATION, USE OF, OR RELIANCE UPON ANY STANDARD, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE AND REGARDLESS OF WHETHER SUCH DAMAGE WAS FORESEEABLE.

Translations

The IEEE consensus development process involves the review of documents in English only. In the event that an IEEE standard is translated, only the English version published by IEEE is the approved IEEE standard.

Official statements

A statement, written or oral, that is not processed in accordance with the IEEE SA Standards Board Operations Manual shall not be considered or inferred to be the official position of IEEE or any of its committees and shall not be considered to be, nor be relied upon as, a formal position of IEEE. At lectures, symposia, seminars, or educational courses, an individual presenting information on IEEE standards shall make it clear that the presenter's views should be considered the personal views of that individual rather than the formal position of IEEE, IEEE SA, the Standards Committee, or the Working Group.

Comments on standards

Comments for revision of IEEE Standards documents are welcome from any interested party, regardless of membership affiliation with IEEE or IEEE SA. However, **IEEE does not provide interpretations, consulting information, or advice pertaining to IEEE Standards documents.**

Suggestions for changes in documents should be in the form of a proposed change of text, together with appropriate supporting comments. Since IEEE standards represent a consensus of concerned interests, it is important that any responses to comments and questions also receive 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 comments, or questions except in those cases where the matter has previously been addressed. For the same reason, IEEE does not respond to interpretation requests. Any person who would like to participate in evaluating comments or in revisions to an IEEE standard is welcome to join the relevant IEEE working group. You can indicate interest in a working group using the Interests tab in the Manage Profile and Interests area of the [IEEE SA myProject system](#).¹ An IEEE Account is needed to access the application.

Comments on standards should be submitted using the [Contact Us](#) form.²

Laws and regulations

Users of IEEE Standards documents should consult all applicable laws and regulations. Compliance with the provisions of any IEEE Standards document does not constitute 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.

Data privacy

Users of IEEE Standards documents should evaluate the standards for considerations of data privacy and data ownership in the context of assessing and using the standards in compliance with applicable laws and regulations.

Copyrights

IEEE draft and approved standards are copyrighted by IEEE under US and international copyright laws. They are made available by IEEE and are adopted 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 these documents available for use and adoption by public authorities and private users, IEEE does not waive any rights in copyright to the documents.

¹ Available at: <https://development.standards.ieee.org/myproject-web/public/view.html#landing>.

² Available at: <https://standards.ieee.org/content/ieee-standards/en/about/contact/index.html>.

Photocopies

Subject to payment of the appropriate licensing fees, IEEE will grant users a limited, non-exclusive license to photocopy portions of any individual standard for company or organizational internal use or individual, non-commercial use only. To arrange for payment of licensing fees, please contact Copyright Clearance Center, Customer Service, 222 Rosewood Drive, Danvers, MA 01923 USA; +1 978 750 8400; <https://www.copyright.com/>. Permission to photocopy portions of any individual standard for educational classroom use can also be obtained through the Copyright Clearance Center.

Updating of IEEE Standards documents

Users of IEEE Standards documents 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.

Every IEEE standard is subjected to review at least every 10 years. When a document is more than 10 years old and has not undergone a revision process, 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 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 [IEEE Xplore](#) or [contact IEEE](#).³ For more information about the IEEE SA or IEEE's standards development process, visit the IEEE SA Website.

Errata

Errata, if any, for all IEEE standards can be accessed on the [IEEE SA Website](#).⁴ Search for standard number and year of approval to access the web page of the published standard. Errata links are located under the Additional Resources Details section. Errata are also available in [IEEE Xplore](#). Users are encouraged to periodically check for errata.

Patents

IEEE Standards are developed in compliance with the [IEEE SA Patent Policy](#).⁵

Attention is called to the possibility that implementation of this standard may require use of subject matter covered by patent rights. By publication of this standard, no position is taken by the IEEE with respect to the existence or validity of any patent rights in connection therewith. If a patent holder or patent applicant has filed a statement of assurance via an Accepted Letter of Assurance, then the statement is listed on the IEEE SA Website at <https://standards.ieee.org/about/sasb/patcom/patents.html>. Letters of Assurance may indicate whether the Submitter is willing or unwilling to grant licenses under patent rights without compensation or under reasonable rates, with reasonable terms and conditions that are demonstrably free of any unfair discrimination to applicants desiring to obtain such licenses.

Essential Patent Claims may exist for which a Letter of Assurance has not been received. 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

³ Available at: <https://ieeexplore.ieee.org/browse/standards/collection/ieee>.

⁴ Available at: <https://standards.ieee.org/standard/index.html>.

⁵ Available at: <https://standards.ieee.org/about/sasb/patcom/materials.html>.

reasonable or non-discriminatory. Users of this standard 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.

IMPORTANT NOTICE

IEEE Standards do not guarantee or ensure safety, security, health, or environmental protection, or ensure against interference with or from other devices or networks. IEEE Standards development activities consider research and information presented to the standards development group in developing any safety recommendations. Other information about safety practices, changes in technology or technology implementation, or impact by peripheral systems also may be pertinent to safety considerations during implementation of the standard. Implementers and users of IEEE Standards documents are responsible for determining and complying with all appropriate safety, security, environmental, health, and interference protection practices and all applicable laws and regulations.

Participants

At the time this guide was completed, the K31 Working Group had the following membership:

Vahid Madani, Chair
Brandon Davies, Vice Chair

Abu Bapary
Jeffrey Barsch
Arunodai Chanda
Alla Deronja
Jason Eruneo
Kamal Garg
Gene Henneberg
Binaya Joshi

Steve Klecker
Hillmon Ladner-Garcia
Don Lukach
Bernard Matta
Alexis Mezco
Adi Mulawarman
Claire Patti

Shivam Prabhakar
Taylor Raffield
Satish Samineni
Michael Thompson
Chris Walker
Don Ware
Roger Whittaker
Yujie Yin

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

Abu Bapary
Thomas Barnes
Jeffrey Barsch
David Beach
Tony Bell
Martin Best
Steven Bezner
Sebastien Billaut
Brian Boysen
Laurel Brandt
Gustavo Brunello
Paul Cardinal
Sharmeela Chenniappan
Ritwik Chowdhury
Brian Clement
Stephen Conrad
Timothy Coyle
Brandon Davies
Robert Dempsey
Alla Deronja
Michael Dood
Douglas J. Edwards
Paul Elkin
William English
Keith Flowers
Carl Fredericks
Fredric Friend
Kamal Garg
Shubhanker Garg
Abel Gonzalez
Prasanth
Gopalakrishnan
Stephen Grier

Randy Hamilton
Gene Henneberg
Marshall Hilgemann
Werner Hoelzl
Robert Hoerauf
Yi Hu
Richard Jackson
Jonathan Jenkins
Erin Jessup
Jack Jester
Andrew Jones
Nathanael Kamm
John Kay
Peter Kelly
Yuri Khersonsky
James Kinney
Gary Kobet
Andrew Kunze
Hillmon Ladner-Garcia
Mikhail Lagoda
Karl Lai
Chung-Yiu Lam
Joshua Lamb
Raluca Lascu
Chase Lockhart
Don Lukach
Greg Luri
Bruce Mackie
Vahid Madani
Muthu Madhu
Todd Martin
Bernard Matta
Mark Mcchesney
Daleep Mohla

Adi Mulawarman
Bruce Muschlitz
Vicente Alonso Navarro
Valencia
Arthur Neubauer
Joe Nims
James O'Brien
Sivaraman P.
Lorraine Padden
Manish Patel
Pathik Patel
Subhash Patel
Claire Patti
Farnoosh Rahmatian
Antonio Richmond
Charles Rogers
Ryandi Ryandi
Daniel Sabin
Bartien Sayogo
Kris Sommerstad
Fenghai Sui
Eric Thibodeau
Michael Thompson
Eric Udren
Benton Vandiver
John Vergis
Quintin Verzosa
Austin Wade
Christopher Walker
John Wang
Don Ware
Keith Waters
Kenneth White

When the IEEE SA Standards Board approved this guide on 10 September 2025, it had the following membership:

Lei Wang, *Chair*
Jon Walter Rosdahl, *Vice Chair*
David J. Law, *Past Chair*
Alpesh Shah, *Secretary*

Edward Au
Ted Burse
Xiaofeng (Alfred) Chen
Doug Edwards
Nehad El-Sherif
J. Travis Griffith
Deborah R. Hagar

Guido R. Hiertz
Ronald W. Hotchkiss
Tyler L. Jaynes
Thomas Koshy
Howard Li
Xiaohui Liu
Kevin W. Lu
Hiroshi Mano

Daleep C. Mohla
Annette D. Reilly
Robby Robson
Daniel Sabin
F. Keith Waters
Sha Wei
Luyang (Eric) Zhang

Introduction

This introduction is not part of IEEE Std C37.119-2025, IEEE Guide for Power System Circuit Breaker Failure Protection.

This guide is a revision to IEEE Std C37.119-2016. Several new clauses have been included to address changes in the power system. Several sections have been updated, and further details, figures, and diagrams are included to assist the reader. There are other additions that are described further in this introduction section.

The scope of breaker failure protection schemes has been broadened to provide a more comprehensive description of breaker failure protection for circuit breakers applied to generation, distribution, and transmission systems.

In addition to the breaker failure schemes described in the earlier versions of this guide, additional examples of interconnect control power to redundant protective relay systems for breaker failure functionality are provided [B18]. Breaker failure modes have been expanded to present circuit breaker phase discrepancy and status discrepancy monitoring. Circuit breaker condition monitoring schemes, such as low insulating gas, have been enhanced. Likewise, breaker failure protection with redundant electro-mechanical or static primary relays has been described in more detail. The fault detector pickup setting description section has been expanded. Practical considerations are now included that describe the application of breaker failure protection to legacy equipment and microprocessor relays, and that describe the interaction of the breaker failure protection scheme with local and remote controls, including automatic reclosing, lockout, and restoration functions.

Another addition to the guide is the description of low-level fault current situations. Information included for inverter-based sources, breaker failure protection for system integrity protection schemes (SIPS), and tandem circuit breaker protection is expanded. Failure to close has been added to include applications where a bypass circuit breaker is applied to help absorb high-energy current. These protection functions are typically applied as part of the overall breaker failure protection scheme.

Contents

1. Overview	14
1.1 General	14
1.2 Scope	15
1.3 Purpose	15
1.4 Word usage	15
2. Normative references	16
3. Definitions, acronyms, and abbreviations	16
3.1 Definitions	16
3.2 Acronyms and abbreviations	16
4. Need for breaker failure protection	17
5. Circuit breaker failure modes	20
6. Breaker failure protection schemes	22
6.1 General	22
6.2 Basic breaker failure scheme	23
6.3 Breaker failure re-trip function	26
6.4 Breaker failure scheme for multiple circuit breaker arrangements	27
6.5 Breaker failure scheme based on 50BF pickup time	28
6.6 Breaker failure scheme with two-step timing arrangement	29
6.7 Breaker failure initiate seal-in	30
6.8 Breaker failure minimal or no current scheme	31
6.9 Dual timer breaker failure scheme with fast circuit breaker auxiliary contact and current detector reset check	34
6.10 Triple timer breaker failure scheme	35
6.11 Single-phase tripping, breaker failure, and re-trip logic	36
6.12 Circuit breaker condition monitoring schemes	38
6.13 Circuit breaker current differential protection	41
6.14 Column ground fault breaker failure	41
6.15 Series (tandem) circuit breakers	42
6.16 Breaker failure protection for generator applications	44
6.17 Breaker failure considerations for systems with IBRs	52
6.18 Breaker failure related to System Integrity Protection Schemes (SIPS)	53
6.19 Failure to close bypass circuit breaker in series capacitor bank applications	53
6.20 Stuck BFI security timer	54
7. Breaker failure design considerations	55
7.1 General considerations	55
7.2 Breaker failure current supervision (50BF)	57
7.3 Breaker failure as an element of protection and control devices	58
7.4 Breaker failure initiation	60
7.5 Breaker failure actions	61
7.6 Practical considerations, applying breaker failure protection to redundant control circuits	62
8. Factors influencing breaker failure protection settings	72
8.1 General factors	72
8.2 50BF detector pickup	72
8.3 Total clearing time	73
9. Communications-based breaker failure protection	73

9.1 Teleprotection in conventional breaker failure protection	73
9.2 High-speed peer-to-peer communications on substation LAN or system WAN	74
10. Breaker failure protection scheme testing	75
10.1 General	75
10.2 BFP scheme testing guidelines and awareness	75
10.3 Overall system testing	77
Annex A (informative) Bibliography	79
Annex B (informative) Breaker failure setting examples	82

List of Figures

Figure 1—Local and remote circuit breaker clearing	18
Figure 2—Circuit breaker phase discrepancy protection logic	21
Figure 3—Circuit breaker status discrepancy monitoring logic	22
Figure 4—Basic breaker failure scheme.....	23
Figure 5—Breaker failure sensing options	24
Figure 6—Fault clearing timing chart	25
Figure 7—Breaker failure re-trip.....	27
Figure 8—Timer without 50BF supervision.....	28
Figure 9—Logic diagram for BF scheme without 50BF reset time	29
Figure 10—BF scheme timing chart without 50BF reset time.....	29
Figure 11—Two step timing arrangement	30
Figure 12—Breaker failure seal-in	30
Figure 13—Minimum or no fault current seal-in scheme	31
Figure 14—BFI seal-in with 86 supervision of 52a	31
Figure 15—Basic minimal or no current scheme	32
Figure 16—Minimal or no current scheme with segregated BFI.....	33
Figure 17—Minimal or no current scheme with segregated BFI and separate timers.....	33
Figure 18—Dual timer with 52aa and 50BF reset	34
Figure 19—Triple timer with 52aa, 50BF, and 52a reset	35
Figure 20—Single-phase BFI with re-trip. The re-trip signals may be directed to a single set of trip coils, or alternately, to both sets of trip coils using additional outputs	37
Figure 21—Single- or three-phase BFI with re-trip only for trips originating from devices other than the single-phase tripping relays	38
Figure 22—Circuit breaker trip circuit design example for no-trip on low gas.....	39
Figure 23—Breaker failure timer bypass scheme logic.....	40
Figure 24—Relay connection example for breaker failure timer bypass scheme	40
Figure 25—Circuit breaker differential protection	41
Figure 26—Column ground fault protection	42
Figure 27—Series circuit breaker scheme to avoid tripping of two critical system components for single BF event.....	43
Figure 28—Series circuit breaker scheme to achieve faster total clear time.....	44

Figure 29—Example of CT location for BFP applications with generator circuit breaker	46
Figure 30—Modified breaker failure logic for circuit breaker flashover	47
Figure 31—Unit-connected generator directly connected.....	48
Figure 32—Unit-connected generator, ring bus configuration	48
Figure 33—Modified breaker failure scheme for dual circuit breaker applications.....	49
Figure 34—Generator low-side circuit breaker	50
Figure 35—Generator synchronizing circuit breaker dc schematic close circuit.....	51
Figure 36—Synchronizing circuit breaker failure to close tripping logic.....	52
Figure 37—Midline series capacitor installation with high-speed bypass circuit breaker	54
Figure 38—Addition of control timer.....	55
Figure 39—Possible allocations of BFP functions among multiple devices.....	59
Figure 40—Power circuit breaker common to circuit elements X and Y	62
Figure 41—Methods to initiate BF for circuits X and Y on each side of a power circuit breaker.....	63
Figure 42—Continuation of Figure 41	64
Figure 43—Breaker-and-a-half BFP scheme using electro-mechanical/static relays.....	67
Figure 44—Simplified protective relay dc trip circuit for line #1 of Figure 43	67
Figure 45—Simplified trip coil circuits for circuit breaker BKR#2 of Figure 43	68
Figure 46—Breaker failure dc circuit, circuit breaker BKR#2 of Figure 43	68
Figure 47—Breaker failure scheme implemented externally of relays.....	69
Figure 48—Breaker failure scheme implemented internally in relays.....	69
Figure 49—Example system diagram – BFI on BF trip.....	71
Figure 50—Distributed breaker failure protection	74
Figure B.1—Setting example timing chart.....	82
Figure B.2—One line representation of radial IBR application with possible current and voltage sensing locations	86
Figure B.3—Inverter-based resource BF logic example	87
Figure B.4—One-line diagram non-radial IBR application	87

IEEE Guide for Power System Circuit Breaker Failure Protection

1. Overview

1.1 General

The most common form of breaker failure protection (BFP) covers failure to clear a fault when called upon to do so by a protective relay. The BFP scheme acts to isolate the fault from the protected power system by removing from service power circuit elements located electrically adjacent to the failed power circuit breaker.

Backup relay protection has been used on power systems for many years. All parts of the protection system, including relays, voltage and current transformers, circuit breakers, and control power source, are vulnerable to failure. All these components need to work properly to effectively clear a fault. To improve protection system reliability, components such as protective relays, power sources, and instrument transformers are often duplicated. Duplicate or redundant systems are designed to operate independently to increase protection system functionality during failures. Because it is usually too costly to install a duplicate circuit breaker and the need for additional field space, breaker failure schemes are specifically employed to provide backup protection in the event that a circuit breaker fails to operate properly during fault clearing.

Protection for power circuit breaker performance failures, other than fault-clearing failures, is sometimes added to breaker failure schemes. These include failure to operate, either tripping or closing, manual or automatic. Where applied, this protection typically exists as an addition to, and as a part of, the same overall scheme as the breaker failure backup protection.

The choice and successful application of any BFP scheme depend upon factors such as the local circuit breaker arrangement and the relative criticality of protected power circuit elements. There is a delicate balance between the risk of damage to unprotected equipment versus the impact of removing adjacent power circuit elements when the scheme operates.

This guide reviews generally accepted breaker failure schemes used on utility transmission and generation systems. Many of the characteristics of these schemes also apply to the use of breaker failure on utility distribution systems. Schemes are carefully examined so that advantages as well as disadvantages can be compared. Application examples and testing practices are also included.

This guide has been revised to reflect changes in the power system. Since its last revision in 2016, there have been many power system changes, such as the proliferation of inverter-based resources (IBR), the broader use of system integrity protection schemes (SIPS), and the transition from discrete to integrated breaker failure schemes. In addition, this guide describes consequences that may include interruption or outage of other sources (or feeds) connected to the bus that is shared with the failed circuit breaker, multiple circuit outages

caused by operation of the remote backup protection, increased equipment damage and outages, or loss of stability and widespread blackouts.

This guide covers BFP for many types of equipment protection. However, there may be other power system components where BFP may not be explicitly covered by this guide. In those instances, it may be helpful to refer to both this guide and applicable IEEE standards associated with the primary protection of the respective equipment.

For example, breaker failure considerations for shunt reactors are discussed in IEEE Std C37.109™ [B15] and reactor switching and circuit breaker specification considerations are discussed in IEEE Std C37.015™ [B12], both providing relevant considerations to the application of BFP for a shunt reactor.⁶

This guide discusses BFP for power circuit breakers. There are other types of power circuit interrupters, such as motor-operated circuit switches and switchgears. The industry practices for failure of these types of interrupters may be application-specific and are not addressed in this guide.

The guide is prepared for engineers who have a working knowledge of power system protection and are seeking information on industry practices and a better understanding of breaker failure applications. This guide may also be used as an evaluation tool when comparing alternative breaker failure options.

1.2 Scope

This guide describes methods to protect a power system and its components from consequences resulting from a circuit breaker failure to operate (open or close) when called upon by protection or control systems. The guide explains how to detect a breaker that has failed to operate and the actions to address the failure.

1.3 Purpose

This guide assists relay engineers with the application of power system breaker failure protection.

1.4 Word usage

The word *shall* indicates mandatory requirements strictly to be followed in order to conform to the standard and from which no deviation is permitted (*shall* equals *is required to*).^{7,8}

The word *should* indicates that among several possibilities one is recommended as particularly suitable, without mentioning or excluding others; or that a certain course of action is preferred but not necessarily required (*should* equals *is recommended that*).

The word *may* is used to indicate a course of action permissible within the limits of the standard (*may* equals *is permitted to*).

The word *can* is used for statements of possibility and capability, whether material, physical, or causal (*can* equals *is able to*).

⁶ The numbers in brackets correspond to those of the bibliography in [Annex A](#).

⁷ The use of the word *must* is deprecated and cannot be used when stating mandatory requirements; *must* is used only to describe unavoidable situations.

⁸ The use of *will* is deprecated and cannot be used when stating mandatory requirements; *will* is only used in statements of fact.

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.

There are no normative references in this document.

3. Definitions, acronyms, and abbreviations

3.1 Definitions

For the purposes of this document, the following terms and definitions apply. The *IEEE Standards Dictionary Online* should be consulted for terms not defined in this clause.⁹

backup protection: A protection scheme for the same zone of protection as the primary protection but may be slower and removes the same or additional equipment from service. Backup protection may be installed locally, i.e., in the same substation as the primary protection, or remotely.

breaker failure protection (BFP): A form of protection that is designed to detect the failure of a circuit breaker to operate or to interrupt a fault. Upon detection of a breaker failure during a fault condition, the scheme is designed to take appropriate action to clear the fault. Upon detection of a breaker failure during a non-fault condition, the scheme may take other appropriate action.

common-mode failure: A multiple failure attributable to a common cause.

control timer: A timer that limits the amount of time the breaker failure scheme is active after initiation.

critical clearing time: The longest time that fault conditions may persist before system stability is lost.

local backup: A form of backup protection in which the backup protective relays are at the same station as the primary protective relays.

primary protection: The main protection system for a given zone of protection that operates in the fastest time and removes the least amount of equipment from service.

remote backup: A form of backup protection in which the protection is at a station or stations other than that which has the primary protection.

3.2 Acronyms and abbreviations

Eleven	multifunction device
50	instantaneous overcurrent element
50G	instantaneous overcurrent ground element
50P	instantaneous overcurrent phase element
50BF	instantaneous breaker failure current detector

⁹*IEEE Standards Dictionary Online* is available at: <http://dictionary.ieee.org>. An IEEE account is required for access to the dictionary, and one can be created at no charge on the dictionary sign-in page.

52a	circuit breaker auxiliary contact that is closed when the circuit breaker is closed and open when the circuit breaker is open
52b	circuit breaker auxiliary contact that is open when the circuit breaker is closed and closed when the circuit breaker is open
52aa	circuit breaker auxiliary contact that is closed when the circuit breaker is closed, and opens as soon as the circuit breaker operate mechanism begins moving from the closed to the open position
62	breaker failure timer, time delay on pickup
86BF	breaker failure auxiliary lockout relay
94	auxiliary tripping relay
BF	breaker failure
BFI	breaker failure initiate
BFP	breaker failure protection
BFR	breaker failure relay
BFS	breaker failure sensing
CT	current transformer
CTR	current transformer ratio
DCB	directional comparison blocking
DTT	direct transfer trip
DUTT	direct underreaching transfer trip
EHV	extra-high voltage
IED	intelligent electronic device
IBR	inverter-based resources
LAN	local area network
LOP	loss of potential
MOV	metal oxide varistor
POTT	permissive overreaching transfer trip
SC	series capacitor
SCADA	supervisory control and data acquisition
SIPS	system integrity protection scheme
WAN	wide area network

4. Need for breaker failure protection

Circuit breakers are strategically used in power systems to connect circuits and electrical apparatus and to isolate faulty equipment detected by protection and control systems. Protection systems are coordinated so that the circuit breaker(s) closest to the fault is tripped to isolate the affected equipment thereby minimizing power system impact.

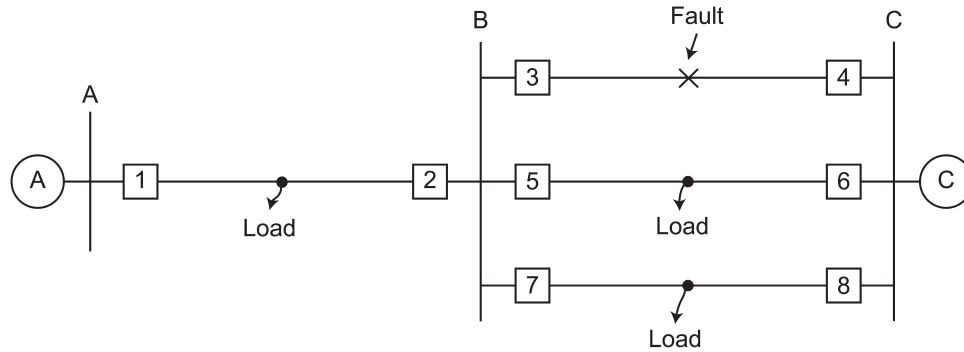


Figure 1—Local and remote circuit breaker clearing

While infrequent, circuit breakers occasionally fail to interrupt a fault. Other sources of power will continue to feed the faulted equipment if those sources are not removed by tripping the electrically adjacent circuit breakers. Referring to Figure 1, with sources at stations A and C, for a fault between circuit breakers 3 and 4, protective relays designed to detect faults on the line between these circuit breakers operate and command circuit breakers 3 and 4 to trip. In this example, circuit breaker 3 fails to interrupt the fault current. Therefore, all sources that continue to supply fault current through circuit breaker 3 need to be interrupted. Circuit breakers 2, 5, and 7 would trip by BFP. In case there is no local BFP at station B, circuit breakers 1, 6, and 8 would need to trip.

Remote backup protection for circuit breaker 3 would use overreaching elements that sense faults anywhere on the line between circuit breakers 3 and 4 and operate after a time delay. This delay allows for the local line protection on circuit breaker 3 to operate and for the circuit breaker to successfully clear the fault, recognizing that the local protective relay scheme on circuit breaker 3 may include time-delayed tripping to coordinate with other protective relays. Remote backup protection does not have the benefit of knowing exactly when the circuit breaker is commanded to open. Therefore, the remote backup protection time delay is selected to accommodate all possible tripping delays.

Remote backup, therefore, has the following considerations:

- All tapped loads between circuit breakers 1–2, 5–6, and 7–8 will be dropped, causing widespread customer outages.
- The lengthy backup clearing time will cause excessive system voltage sag duration, additional damage to faulted equipment, and possible damage to unfaulted equipment, and may lead to system instability.
- Due to infeed effects from the other lines, it may be difficult to set the remote relays at 1, 6, and 8 to detect faults on the entire length of the adjacent lines.
- The settings that provide sufficient reach to detect faults out to the remote ends of the adjacent lines may be so sensitive that the line is susceptible to tripping under heavy load during extreme disturbances, which could initiate or exacerbate a wide-area cascading outage.

The advantage of remote backup protection is that it is completely independent of protective relays, control systems, and battery supplies at the station with the failed circuit breaker.

An alternative to remote backup protection is local BFP. Using the example in Figure 1 again, and concentrating on circuit breaker 3, when the protective relay on circuit breaker 3 senses a fault on line 3–4 and issues a trip to circuit breaker 3, local BFP starts a timer. If the timer times out, and the fault is not interrupted by circuit breaker 3, then the local breaker failure scheme is activated, and a trip to adjacent circuit breakers 2, 5, and 7 is initiated. The local breaker failure scheme has several benefits over the remote backup scheme. If there are

sources at buses A and C, tapped loads between circuit breakers 1–2, 5–6, and 7–8 can still be served from the remote sources. The total clearing time for the fault is reduced substantially compared to the remote backup method. The timer setting for the local breaker failure scheme is composed of circuit breaker interrupting time plus some margin. Margins may vary depending on the critical fault clearing time. The time for the protective relay to detect and assert for the fault condition is not included in this time delay, as the local BFP timer and circuit breaker trip command are both triggered by the protective relay assertion. This timer setting is typically less than 12 cycles,¹⁰ compared to 30 cycles or greater for remote backup. This time difference could mean the difference between a stable and unstable power system for some faults and may substantially reduce damage at the fault, through fault stress on equipment, and the effect of voltage depressions on adjacent loads.

The primary disadvantage of local BFP is that it may suffer from common-mode failure. For example, a station battery failure may prevent the circuit breaker from tripping and disable the local BFP. Likewise, local protective relay malfunction may cause a failure to trip the circuit breaker and also fail to initiate the local breaker failure timer. For this reason, redundant protective relay systems [B18] for each zone are also often coupled with local BFP designed to reduce common mode failures. Otherwise, failure to detect a fault and failure to interrupt a fault are considered the same contingency, which may justify the application of backup overreaching relays tripping different circuit breakers (remote backup). The cost of adding local BFP systems, while once a major consideration, has been significantly reduced as the breaker failure function may be integrated into microprocessor-based protective relay schemes.

There are many things that may cause the failure of a circuit breaker to interrupt fault current. Many are external to the circuit breaker such as a loss of tripping power, dc battery failure, battery charger failure, dc breaker tripped or blown fuse, loose wire or shorted trip circuit, etc. If one of these is the cause for the failure, slow clearing of the fault will probably not cause further damage to the circuit breaker. However, some common internal causes for the failure to interrupt are that the circuit breaker mechanism travel is incomplete or the mechanism is slow; components needed for the interruption, resistors or capacitors, are faulty; or the dielectric material in the interrupter is out of specification (low pressure, low temperature) or contaminated. If these are the causes for the failure to interrupt, the circuit breaker needs protection to prevent further damage. By the time the remote backup protection has operated, the arcing inside the interrupter will likely cause a phase-to-ground fault internal to the circuit breaker. These internal faults may lead to explosions and fires. As a result of the slow clearing of the original fault, what could have been a minor circuit breaker repair project may now result in the replacement of the circuit breaker and possibly other equipment in close proximity to the faulty circuit breaker.

To summarize, when evaluating whether to apply local BFP or rely on remote backup protection, the three fundamental attributes of the protection system are as follows:

- Sensitivity: Can the overreaching protective relays in adjacent zones reliably detect faults in 100% of the zones to be backed up, considering infeed?
- Selectivity: Is it acceptable to trip additional power system elements and loads that may be otherwise preserved by applying a BFP system?
- Speed: Is delayed clearing from remote backup for a breaker failure event acceptable for system stability, power quality, equipment through-fault stress, and equipment fault damage?

Another factor in deciding to rely solely on remote backup is the cost and effort of the derivation of relay settings and coordination over lifecycle maintenance. Relay setting management is intensive and may include revisiting system studies to revalidate critical clearing times and assessment of relay settings and coordination. The analysis effort for an even moderately complex networked system to consider all possible system configurations and current distributions that affect infeed for all possible breaker failure scenarios is difficult. Assuming that the analysis has been performed adequately, even small changes to the network may require that this analysis effort be repeated to prove that remote backup can be relied upon.

For further information about remote backup, refer to IEEE Std C37.113 [B16].

¹⁰ Throughout this document, power system operating at 60 Hz is assumed unless otherwise described.

5. Circuit breaker failure modes

Circuit breaker failure to interrupt a fault can occur in a variety of situations, as follows:

- Failure to trip where the circuit breaker contacts do not open after the trip circuit has been energized by the protective scheme. This could be caused by an open or short in the trip circuit wiring or in the trip coil. It could also be the result of a mechanical problem in the circuit breaker that prevents the contacts from opening; this condition is also known as “stuck breaker.”
- Failure to clear where circuit breaker contacts open, but the arc is not extinguished, and current continues to flow. This could be caused by mechanical problems (incomplete opening), dielectric problems (such as contaminated oil or loss of vacuum), or loss of current zero crossings (a reduction in the ac magnitude before the dc transient has dissipated). Failure to clear is significantly different from failure to trip in that the circuit breaker auxiliary contacts (52a and 52b) will change state, which indicates mechanical opening. Because of this, an auxiliary contact position may not be a reliable indicator of satisfactory fault clearing.
- Failure to clear circuit breakers with opening resistors. A failure mode, where the resistor remains in the circuit after the main contact opens, can result in a high impedance path to current flow, reducing the current magnitude but not interrupting the flow of current.

These circuit breaker failure modes can occur during different fault or operating conditions, such as high or low current faults, abnormal operating conditions, or transfer trip from remote locations.

There are also non-fault conditions or situations during system faults where the circuit breaker is not called upon to operate that may be incorporated within the breaker failure scheme design, such as the following:

- Loss of dielectric during non-fault conditions can prevent satisfactory interruption of current if called upon, potentially leading to failure of the circuit breaker. Loss of dielectric pressure can be detected in gas (e.g., SF₆) breakers using a gas density or pressure monitor. For loss of pressure below a cutoff point, circuit breaker manufacturers typically recommend either immediately tripping or block tripping to prevent mechanical or electrical failure that may occur if the breaker is called upon to clear a fault. In the latter case, the breaker failure scheme delay timer can be bypassed so that the BFP will operate with no intentional delay if a breaker failure initiate signal is received. Refer to 6.12 for details.
- Loss of mechanism energy storage during non-fault conditions can prevent satisfactory interruption of current in circuit breakers that use stored energy for the opening stroke, if called upon, potentially leading to a true breaker failure. Loss of mechanism energy storage can be detected with pneumatic or hydraulic gauges, micro-switches, or undervoltage relays. Subclause 6.12 provides information related to breaker condition monitoring. The circuit breaker manufacturer might be consulted to verify the loss of energy storage is not a transient condition that could occur during the normal operation of the circuit breaker.
- Contact flashover in an open circuit breaker can lead to catastrophic failure. This could be caused by a re-strike of an opening breaker or a surge through an already open breaker that produces dielectric breakdown across the contacts, or when the voltages on each side of the breaker are out of phase, such as during synchronizing a generator.
- Failure of a circuit breaker to close when called upon is not traditionally defined as a breaker failure condition, since it is not associated with a protective relay trip. This can, however, have significant impact on the power system and may need to be considered in the operating scheme. Many reclosing schemes include failure-to-close logic. There are instances where a protective scheme may activate closure of a circuit breaker where BFP is applied, such as a series capacitor bypass breaker. Refer to 6.19.

- Failure of a circuit breaker to close in the expected time while attempting to connect a generator to the system can cause severe damage to the generator and turbine if the breaker eventually closes when the generator is out of phase with the system. This can occur for a number of reasons, but especially if the breaker has sat for an extended time in very low ambient temperatures. It may be desirable to isolate the breaker and operate it a few times before the synchronization is attempted. Protection schemes are also available to monitor the closing time of the breaker and trigger the breaker failure-to-close scheme if the close has not occurred within an appropriate time following the synchronism signal and the close command.
- Non-fault-related failures are also possible. An example would be failure to interrupt load current, or mechanical failure during switching operations. These failures can be addressed within more complex BFP schemes.

A consideration for circuit breakers with independently operated poles (phases) is protection against phase discrepancy or pole disagreement. This protection monitors circuit breaker auxiliary contacts, 52a and 52b, from each phase of the breaker and trips or alarms if all three poles of the breaker are not in the same position (open or closed). This is of particular interest in a single-phase trip and reclosing application; refer to 6.11.

Phase discrepancy logic may be implemented in the controls of the circuit breaker itself, configured as external wiring, or configured within logic of the equipment protective relays. For applications where this feature is desired, circuit breaker auxiliary contacts 52a and 52b are combined as shown in Figure 2. The timer output initiates a three-phase trip and may also activate BFP scheme.

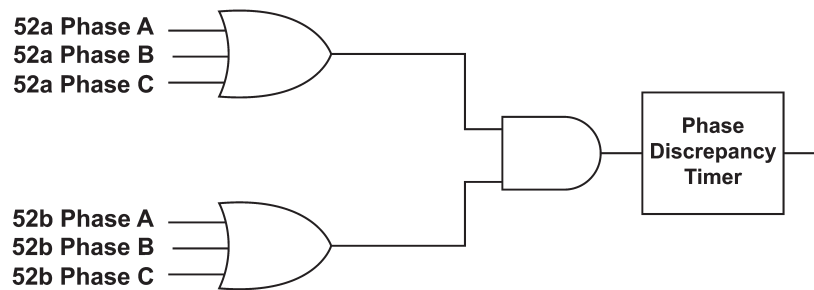


Figure 2—Circuit breaker phase discrepancy protection logic

Auxiliary contacts are mechanically or hydraulically linked to the main contacts of the circuit breaker, but can fail to operate because of mechanical problems, causing the 52a or 52b contact status to no longer follow the state of the main contact. In critical applications where the reliability of the auxiliary status is a concern, circuit breaker status discrepancy monitoring logic can be applied to monitor status of associated 52a and 52b contacts and alarm or take necessary control action if the contacts do not indicate the same main contact positions, for example, both 52a and 52b contacts being closed or open. This logic can be applied for an independent pole breaker as illustrated in Figure 3. Similar logic can be provided for three-pole operating circuit breakers using the single 52a and 52b status contacts available for that relay.

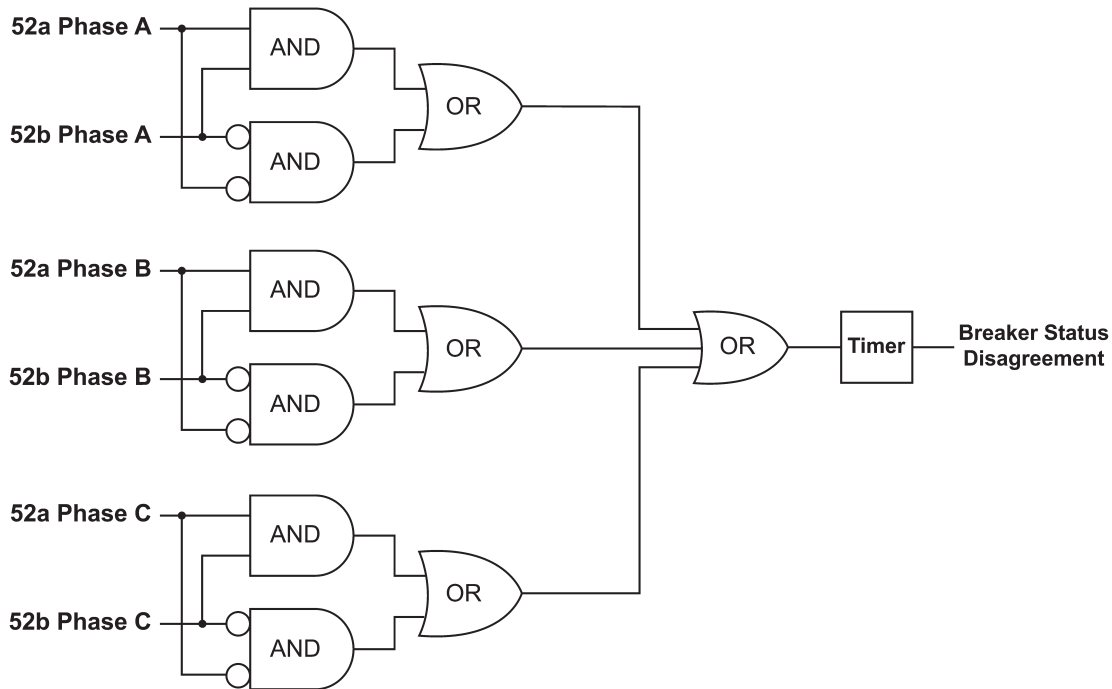


Figure 3—Circuit breaker status discrepancy monitoring logic

Microprocessor relays applied for fault detection may have some ability to identify the impending failure of a circuit breaker. This can be accomplished by identifying degraded performance, such as changes in operating time. These schemes can also track predictive quantities such as accumulated interrupted current or number of operations.

Circuit breakers with single-phase fault-clearing capability present additional considerations for BFP, which are covered later in this guide.

6. Breaker failure protection schemes

6.1 General

This clause describes breaker failure schemes that have received acceptance by the industry and are used in utility power systems. Common elements of a breaker failure scheme include the following:

- Scheme initiation by a circuit breaker trip signal, such as a protective relay that has operated to trip the breaker.
- Determination that the circuit breaker has tripped successfully. Sensing methods include reset of an overcurrent element (50BF) that responds to each measured phase current (50P) and possibly the residual current (50G), monitoring change in state of the circuit breaker auxiliary contact (52a, 52b, or 52aa), or some combination of these elements.
- A timer.
- Some means to trip and block the closing of adjacent circuit breakers.
- Optional: A separate output contact to issue a re-trip signal to the circuit breaker before activating a breaker failure output(s) with sufficient margin such that successful opening of the circuit breaker will prevent an undesired breaker failure output.
- Optional: A teleprotection channel to key a DTT to remote sources to activate tripping. The receiving terminal may also cancel reclosing of its circuit breaker(s) where applicable.

Schemes in this guide are illustrated using logic diagrams. Many of the schemes could also be implemented using conventional dc control schematics.

When choosing a scheme, it is important that the interaction of the aggregate components is thoroughly considered. Schemes vary in their degree of dependability versus security. Behavior unique to a particular type of relay can affect each scheme differently. Furthermore, performance can be impacted by equipment replacements and firmware upgrades.

Factors to be aware of include the following:

- The method of seal-in or latching of the primary relay output after fault detection
- Presence or absence of local current/fault detector supervision of the primary relay
- Sensitivity (pickup and dropout) of the 50BF current detectors
- Interaction of the scheme with local and remote automatic reclosing
- Impacts of credible component failures, such as welding shut of relay output contacts
- Reset of the BFP scheme

6.2 Basic breaker failure scheme

Basic BFP provides a means to trip adjacent current sources if a fault is detected by protective relays and the associated circuit breaker(s) fail to interrupt the fault. Figure 4 is a logic diagram showing a basic breaker failure scheme.



Figure 4—Basic breaker failure scheme

The following two conditions are used to monitor proper circuit breaker operation during a fault-clearing operation:

- a) Breaker failure sensing (BFS)
- b) Breaker failure initiate (BFI)

BFI indicates that the breaker failure scheme has been initiated due to a trip signal issued by a protective relay or from a contact on an auxiliary relay or lockout relay. BFS is used to determine that the circuit breaker has not successfully interrupted the fault. Figure 5 shows some breaker failure sensing options considered within the industry.

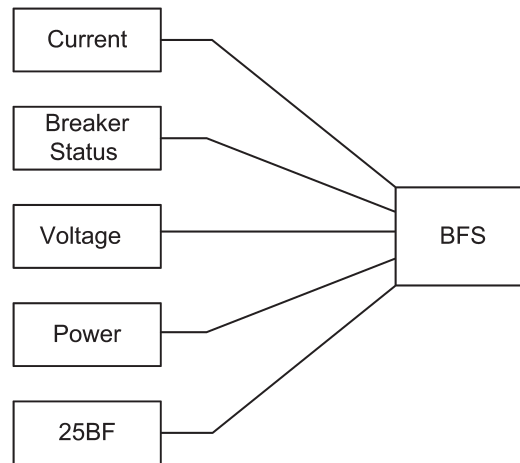


Figure 5—Breaker failure sensing options

- Current (50P/50G/50Q/50N): Current sensing is provided by monitoring the reset of non-directional instantaneous phase (50P), ground (50G), negative-sequence (50Q), or neutral (50N) overcurrent elements. Current supervision is the most common, secure, and reliable method of detecting successful opening of the circuit breaker.¹¹
- Circuit breaker status (52a/52b): Circuit breaker status sensing is provided by monitoring the state of 52a and/or 52b auxiliary contacts. The use of auxiliary contacts for supervision may not be reliable, as there are cases where they fail to represent the true status of the circuit breaker's main contacts. This method of breaker failure supervision is typically used in parallel with current supervision for applications where current supervision is not sensitive enough to reliably provide breaker failure sensing on its own. Circuit breaker status supervision is the most commonly used low/no current breaker failure sensing method, as it is the oldest method for this type of application.
- Voltage (27P/59G/59Q/59N): Voltage sensing is provided by monitoring the reset of phase (27P) undervoltage elements or ground (59G), negative-sequence (59Q), or neutral (59N) overvoltage elements. Voltage supervision is used for applications where current supervision is not sensitive, and the absence of voltage indicates successful interruption, the voltage source is only on one side, and the voltage sensing is on the non-source side of the circuit breaker.
- Directional power (32P/Q) functions on a desired value of power flow in a given direction, or upon reverse power [B1]. Real power, also known as active power (P), is consumed by resistive loads. Reactive power (Q) is either consumed by inductive loads or generated by capacitive loads. This sensing method can be applied to synchronous generator BFP in parallel with current sensing.
- Synchronism check (25): Synchronism check sensing is provided by monitoring the slip frequency, voltage magnitude difference, and angle difference across the circuit breaker. The idea behind this function is that if the breaker fails to open, then there should not be any slip frequency, voltage, and angle difference across the breaker. Synchronism check supervision is used for applications where the current supervision is not sensitive [B34]. This method is typically applied for generator breaker failure protection and is applied in parallel with a current-sensing scheme. This scheme uses VT inputs from both sides of the circuit breaker and synchronism check capability in the breaker failure relay. This scheme may need a separate timing element that is set slower than the current sensing scheme timer.

¹¹ Many of the schemes presented in this guide are shown using current based breaker failure sensing (BFS) traditionally referred to as 50BF. For applications that need other or a combination of sensing methods, many of the schemes, logic diagrams and figures can be adapted.

Figure 6 shows a typical timing chart for a current scheme.

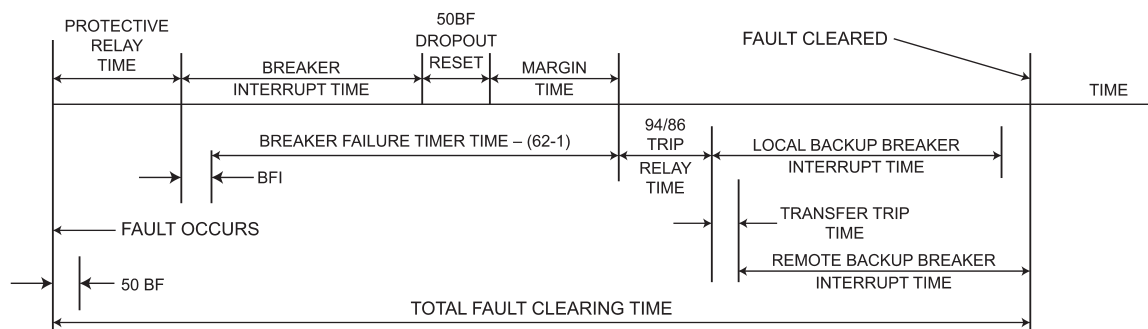


Figure 6—Fault clearing timing chart

The circuit breaker has failed to operate properly if both breaker failure sensing and breaker failure initiate (BFI) are present for a period greater than the expected breaker clearing time. A delay on the pickup timer (62–1) is set to a time delay that exceeds the breaker's normal clearing time with a margin. If current is still flowing through the breaker when the timer times out, it is determined that the breaker has failed. If the breaker operates properly, either one or both the breaker failure sensing and BFI inputs will de-assert and stop the operation of the timer.

The breaker failure scheme operates when the breaker failure timer (62–1) times out and a number of actions are initiated. Auxiliary devices (94) may be used depending on design philosophy, the number of contacts available, the interrupting rating of the output contacts, or relay targeting practices. Often, a lockout relay (86BF) is used as an auxiliary device.

For a breaker failure scheme to provide the desired response when the protected circuit breaker fails to interrupt fault current, the current detectors need to be set sensitive enough to respond to any fault condition for which the protective relays initiate trips to that breaker.

It is important to minimize breaker failure time delay settings, while not jeopardizing the correct operation or reducing the security of the circuit breaker failure scheme. Minimum breaker failure delay times are applied for all fault types (single- and three-phase tripping) to enhance system stability, limit equipment damage, improve coordination of overlapping protection schemes, and enhance the quality of supply by minimizing the duration of power system voltage sag.

Referring to Figure 6, by setting the breaker failure timer greater than the circuit breaker interrupt time (less BFI pickup as necessary) and the dropout of the breaker failure sensing element (50BF current detector) after the fault is cleared, the breaker failure scheme will not operate for a successful breaker operation. Adequate margin is taken into account to allow for maximum operating times. It is essential to set the breaker failure timer so that the total fault clearing time is less than the transient stability critical clearing time and prevents, or at least limits, damage to major equipment such as conductors and transformers. An attempt might also be made to prevent the shutdown of major customers' processes that may be affected by voltage sag. Depending on the sensitivity of these processes, it may not be possible to reduce the breaker failure clearing time enough for them to ride through the fault. As can be seen from Figure 6, the breaker failure scheme starts timing when a protective device requests the breaker to trip. Therefore, there is no need to provide additional delay within the breaker failure timer for external zones that may operate more slowly than breaker failure. When local backup protection is applied in addition to BFP, the BF timer is set less than the local backup protection time delay. For example, if there is a reverse protection providing additional local backup protection, the BF timer is set faster than the local backup protection time delay. This criterion for timer setting allows BF protection to operate before the station local backup protection.

Coordination of remote backup protective relays may also be taken into consideration so that the BFP operates first and with margin. Some relevant factors in determining an appropriate margin for the coordination of backup protection include the following:

- Impact on clearing time of backup protection for faults in its own protected zone.
- Impact of tripping by the backup protection for a breaker failure situation. In some cases, the zone protected by the backup protection may have to be cleared anyway for a breaker failure, and there would be little benefit in slowing down the backup protection to coordinate with the BFP.

6.3 Breaker failure re-trip function

Re-trip is a separate output contact from the BFP intended to prevent undesired breaker failure operations and loss of adjacent circuit elements for certain causes. Possible causes include human error during relay testing, false initiation of BFP from dc transients induced on control circuit wires, and failure to trip due to loose or shorted circuit breaker trip circuit wiring or non-functioning trip coils. Re-trip logic is designed to issue the re-trip signal to the circuit breaker with sufficient margin such that the successful opening of the circuit breaker due to the re-trip signal will cause the 50BF element to drop out (and the 52a to toggle open) before the breaker failure timer expires.

The re-trip circuit helps to alleviate the consequences of an easily made but infrequent operating error. The error occurs while performing relay testing on one of the two sets of line relays while the line is still in service. The trip circuit for the relay under test is disabled, but the breaker failure initiate circuit is not. When the test produces a trip output from the relay, the breaker failure initiate circuit could cause a breaker failure relay (BFR) operation if the load current is above the breaker failure current detector. With a re-trip circuit, the line circuit breaker will be tripped, but the more serious result of the breaker failure operation is avoided.

Power circuit breakers with two (or more) trip coils yield the opportunity to provide redundant actuation using separate, independent trip circuits. Best practices for initiating BFP, where two trip coils are provided, are described in 7.6 and illustrated by Figure 41.

Where primary relays are not redundant, or where it might be difficult to separate tripping outputs, such as for legacy electromechanical phase and neutral overcurrent relays, the breaker failure re-trip contact might be applied to the second trip coil circuit to mitigate failures of the first trip circuit (with the non-redundant or legacy relays).

Some utilities choose to apply both redundant relays of a protected circuit to a single trip coil and rely on a breaker failure re-trip contact to operate the second trip coil supplied from a separate control circuit.

Figure 7 illustrates the addition of re-trip logic. Two options for implementing re-trip logic are shown, one with emphasis on dependability (Figure 7a) and the other on security (Figure 7b). The dependability option asserts only on activating the BFI. The security option asserts re-trip on BFI in the presence of fault current above the user-selected fault detector (50BF) to reduce the possibility of unnecessarily opening the protected circuit breaker.

Re-trip generally includes a time delay (62–2 of Figure 7). The time delay can serve several purposes.

- The delay can identify, by slower measured overall trip time of the circuit breaker due to the delayed re-trip output, when a failure to trip by the first trip coil circuit occurs. When the breaker failure scheme has an internal sequence of events recording, the information can be used to determine whether the trip occurred by the re-trip or by tripping on the initial fault detection. This might be used to inform maintenance personnel that inspection may be beneficial even if the breaker successfully opens.