

IEEE Guide for Protection System Redundancy for Power System Reliability

IEEE Power and Energy Society

Developed by the
Power System Relaying and Control Committee

IEEE Std C37.120™-2021

IEEE Guide for Protection System Redundancy for Power System Reliability

Developed by the

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

Approved 9 November 2021

IEEE SA Standards Board

Recognized as an American National Standard

Abstract: This guide is developed to assist users in selecting the appropriate level of protection system redundancy for power system reliability based on the best industry practices. It defines protection system redundancy and examines the effect of protection system components on redundancy. Different concepts of redundancy as related to physical location, instrument transformer, relay scheme, and communication systems are discussed. Redundancy application considerations for various power system elements are presented.

Keywords: backup protection, breaker failure protection, communication systems, current transformers, dependability, IEEE C37.120™, primary protection, protection systems, redundancy, reliability, security, voltage transformers

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

Copyright © 2022 by The Institute of Electrical and Electronics Engineers, Inc.
All rights reserved. Published 28 February 2022. 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 978-1-5044-8157-1 STD25080
Print: ISBN 978-1-5044-8158-8 STDPD25080

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.

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

²Available 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

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

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

⁵Available 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 IEEE guide was completed, the C31 Working Group had the following membership:

Solveig Ward, *Chair*
Alla Deronja, *Vice Chair*

Jay Anderson	Nathan Gulczynski	Manish Patel
Philip Beaumont	Gene Henneberg	Jeffrey Pond
Tony Bell	Charles Henville	Daniel Reckerd
Matthew Black	Yi Hu	Gary Stoedter
Joerg Blumschein	Gary Kobet	Jonathan Sykes
Jeff Brown	Hillmon Ladner Garcia	Angelo Tempone
Robin Byun	Aaron Martin	Looja Tuladhar
Ritwik Chowdhury	Hugo Alexis Mezco	Paul Thompson
Randall Cunico	David Morrissey	Ian Tualla
Xiangyu Ding	George Moskos	Eric Udren
Kevin Donahoe	James O'Brien	Donald Ware
Robert Frye	Nolasco Orrego	Roger Whittaker
Allen Goldstein		Qiaoyin Yang

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

Jay Anderson	Gary Hoffman	Craig Palmer
Ian Backus	Ali Hooshyar	Manish Patel
Abu Bapary	Yi Hu	Christopher Petrola
Jeffrey Barsch	Richard Jackson	Benito Ramos
Michael Basler	Anthony Johnson	Moises Ramos
David Beach	Brian Johnson	R.K. Rannow
Steven Bezner	Bogdan Kasztenny	Bruce Rockwell
Matthew Black	John Kay	Charles Rogers
Brian Boysen	Yashar Kenarangui	M. Sachdev
Paul Cardinal	James Kinney	Miriam Sanders
Diego Chiozzi	Boris Kogan	Robert Schaerer
Ritwik Chowdhury	Thomas Koshy	Tony Seegers
Stephen Conrad	Jim Kulchisky	Robert Seitz
Randall Cunico	Mikhail Lagoda	Jerry Smith
Ratan Das	Chung-Yiu Lam	Gary Smullin
Alla Deronja	An Le	Wayne Stec
Kevin Donahoe	Daniel Lebeau	Paul Sullivan
Michael Dood	Ting Li	Michael Thompson
Neal Dowling	Albert Livshitz	Eric Udren
Thomas Dunmore II	Federico Lopez	Matthew Vacha
Paul Elkin	Don Lukach	James Van De Ligt
William English	Bruce Mackie	John Vergis
Kenneth Fodero	Vahid Madani	Quintin Verzosa
Fredric Friend	Todd Martin	Ilia Voloh
Rafael Garcia	Jeffrey McElray	Christopher Walker
Kamal Garg	Robert Messel	Solveig Ward
Jalal Gohari	Dean Miller	Donald Ware
Stephen Grier	Jeff Mizener	Keith Waters
Nathan Gulczynski	Arthur Neubauer	Kenneth White
Randy Hamilton	James Niemira	Philip Winston
Charles Henville	Joe Nims	Abu Zahid
Werner Hoelzl	James O'Brien	Marc Zeidman
Robert Hoerauf	P. Sivaraman	Sergio Zimath
	Lorraine Padden	

When the IEEE SA Standards Board approved this guide on 9 November 2021, it had the following membership:

Gary Hoffman, *Chair*
Jon Walter Rosdahl, *Vice Chair*
John D. Kulick, *Past Chair*
Konstantinos Karachalios, *Secretary*

Edward A. Addy
Doug Edwards
Ramy Ahmed Fathy
J.Travis Griffith
Thomas Koshy
Joseph L. Koepfinger*
David J. Law

Howard Li
Daozhuang Lin
Kevin Lu
Daleep C. Mohla
Chenhui Niu
Damir Novosel
Annette Reilly
Dorothy Stanley

Mehmet Ulema
Lei Wang
F.Keith Waters
Karl Weber
Sha Wei
Howard Wolfman
Daidi Zhong

*Member Emeritus

Introduction

This introduction is not part of IEEE Std C37.120-2021, IEEE Guide for Protection System Redundancy for Power System Reliability.

This guide is intended to assist protection engineers and technologists in applying redundancy for protective relaying systems; it also provides the user with information about what factors to consider when determining redundancy requirements. In addition, the guide addresses different approaches to applying redundancy depending on application area and present practices. It also provides real world examples.

Contents

1. Overview	14
1.1 Scope	14
1.2 Purpose	14
1.3 Word usage	14
2. Normative references	14
3. Definitions, acronyms, and abbreviations	15
3.1 Definitions	15
3.2 Acronyms and abbreviations	16
4. General considerations for redundancy	17
4.1 Overview	17
4.2 Redundancy fundamentals	17
4.3 Required degree of protection	19
4.4 Economic considerations	20
4.5 Impact of redundancy on reliability	20
4.6 Redundancy simplicity considerations	23
4.7 Relay technology effect on redundancy	24
4.8 Maintenance considerations	24
5. Component effect on protection system redundancy	24
5.1 General	24
5.2 Physical redundancy	25
5.3 Instrument transformer circuit redundancy	25
5.4 Merging units	28
5.5 Battery/dc source circuit redundancy	29
5.6 DC control circuit redundancy	32
5.7 Breaker trip coil circuit redundancy	32
5.8 Relay system redundancy	33
5.9 Communications channel redundancy	37
5.10 Local area network redundancy	41
5.11 Timing system redundancy	47
6. Redundancy application considerations	49
6.1 Overview	49
6.2 Generator protection	50
6.3 Bus protection	53
6.4 Transmission line protection	54
6.5 Transformer protection	57
6.6 Shunt reactor protection	58
6.7 Capacitor bank protection	60
6.8 Distribution protection	62
6.9 Breaker failure protection	62
6.10 Autoreclosing redundancy	64
6.11 System integrity protection schemes (SIPS)	64
6.12 Refurbishment considerations	67
Annex A (informative) Bibliography	69

List of Figures

Figure 1—Zone of protection visualization.....	18
Figure 2—Probability of a false trip in a redundant system	21
Figure 3—Probability of a missed trip in a redundant system	22
Figure 4—Two-out-of-three voting scheme	22
Figure 5—Dual secondary VT and separated CTs for redundant line protection.....	26
Figure 6—Two sets of VTs and separate CTs for redundant line protection	27
Figure 7—Dual battery dc circuit method	30
Figure 8—One dc circuit method	31
Figure 9—Dual dc circuit method	31
Figure 10—Basic PLC system	37
Figure 11—Two independent PLC channels, each coupled phase to ground.....	38
Figure 12—Two PLC channels coupled together via phase to phase.....	39
Figure 13—IED with switched ports	42
Figure 14—Parallel redundancy protocol	43
Figure 15—High-availability seamless redundancy	44
Figure 16—Programmed network redundancy via SDN	45
Figure 17—Redundancy in Ethernet LAN with IEC 61850 GOOSE.....	46
Figure 18—Generator protection with two relay systems (87U and 87G)	51
Figure 19—Generator redundant ground protection (87N and sub-harmonic injection)	52
Figure 20—Bus protection with high impedance (87Z) and low impedance (87B) bus differential relays	53
Figure 21—Bus protection with transformer differential and phase overcurrent relays	54
Figure 22—Redundant line protection example with same level of performance	55
Figure 23—Line protection with different levels of performance	56
Figure 24—Redundant line protection based on two different operating principles.....	56
Figure 25—GSU protection with dedicated transformer differential and redundant unit differential relays ..	58
Figure 26—Redundant protection for dry-type single-winding reactor	59
Figure 27—Redundant protection for oil-immersed shunt reactor	60
Figure 28—Example of transmission capacitor bank protection.....	61
Figure 29—Mixed redundant SIPS and relay system	65

Figure 30—Separate redundant SIPS and relay system.....	66
Figure 31—Mixed redundant substation SCADA and relay system.....	66
Figure 32—Separate redundant substation SCADA and relay system	67

List of Tables

Table 1—Redundancy influence on security and dependability	22
Table 2—Two-out-of-three voting scheme	23

IEEE Guide for Protection System Redundancy for Power System Reliability

1. Overview

1.1 Scope

This guide provides information about what factors to consider when determining the impact of protection system redundancy on power system reliability.

1.2 Purpose

The purpose of this guide is to provide information on protection system redundancy considerations by illustrating the purpose of redundancy and how it may be implemented in the protection system design.

1.3 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*).^{6,7}

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*).

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

⁶The use of the word *must* is deprecated and cannot be used when stating mandatory requirements; *must* is used only to describe unavoidable situations.

⁷The use of *will* is deprecated and cannot be used when stating mandatory requirements; *will* is only used in statements of fact.

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 guide.

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.⁸

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.

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

dependability: The degree of certainty that a protection system will respond when the fault or abnormal condition the protection system is intended to detect is present.

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.

protection system: A configuration of interconnected devices, including accessories, peripherals, and their interfaces, that is designed to detect and isolate a fault or abnormal condition from the power system.

redundancy: The quality of a relaying system that allows a function to operate correctly, without degradation, irrespective of the failure or state of one portion, since another portion performs the same function (not to be confused with backup).

relay system: An assembly that usually consists of measuring units, relay logic, communications interfaces, computer interfaces, and necessary power supplies.

reliability: The ability of a protection system to operate correctly taking into consideration both dependability and security.

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.

security: The degree of certainty that a protection system will not respond when the fault or abnormal condition the protection system is intended to detect is not present.

selectivity: A general term describing the interrelated performance of relays and breakers and other protective devices; complete selectivity being obtained when a minimum amount of equipment is removed from service for isolation of a fault or other abnormality.

⁸*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.

zone of protection (for relays): That segment of a power system in which the occurrence of assigned abnormal conditions should cause the protective relay system to operate.

3.2 Acronyms and abbreviations

A/D	analog to digital
CCVT	capacitive coupled voltage transformer
CT	current transformer
DCUB	directional comparison unblocking
DTT	direct transfer trip
EHV	extra high voltage
EMS	energy management system
GOOSE	Generic Object-Oriented Substation Events communication protocol
GSU	generator step-up transformer
HSR	high-availability seamless redundancy
HMI	human machine interface
I/O	input/output
IED	intelligent electronic device
LAN	local area network
LOP	loss of potential
MPLS	multi-protocol label switching
NCIT	non-conventional instrument transformer
NTP	network time protocol
POTT	permissive overreaching transfer trip
PPS	pulse per second
PRP	parallel redundancy protocol
RAS	remedial action scheme
RSTP	rapid spanning tree protocol
SCADA	supervisory control and data acquisition
SDN	software defined networking
SIPS	system integrity protection scheme
SONET	synchronous optical network
TAI	international atomic time
TDM	time division multiplexer
UTC	coordinated universal time
VT	voltage transformer
WAN	wide area network

4. General considerations for redundancy

4.1 Overview

As power system design has matured, the reliance on its availability has increased. Power system reliability is often measured, monitored, and regulated. The effort to provide consistent and optimized reliability is ongoing. One aspect of power system design that has a direct effect on power system reliability is its protection system.

There are two characteristics of the protection system that define how it affects power system reliability:

- Its ability to always operate when needed (dependability)
- Its ability to never operate when not needed (security)

Therefore, the effectiveness of the protection system is a compromise between security and dependability. However, the expectation is that the protection system operates correctly for unwanted conditions on the power system, in addition to unwanted conditions such as a failed protective device in the protection system itself.

Redundancy addresses failures in the protection system and, therefore, improves power system reliability. Protection system redundancy typically increases dependability and may decrease security.

Although local redundancy of components plays a major role in elevating the reliability of protection systems, remote protection systems may provide adequate reliability in some situations. Even if a remote protection system provides a lower level of performance, e.g., speed and selectivity, it may still provide clearing times that meet performance requirements.

A need for availability of a power system element influences a decision to apply redundant protection. Having a second set of high-speed independent protective relays for a power system element, such as a transmission line, might allow the line to remain in service when and if it becomes necessary to disable the first set of relays for testing or setting changes. The decision of whether to disconnect relays for maintenance or repair often depends upon the system conditions during the time of removal.

Protection system design balances technical requirements, reliability concerns, and costs with the goal of achieving a robust design that is simple to operate and maintain. The degree to which users apply redundancy is based on a mix of protection philosophy and the criticality of an individual system component along with customer and regulatory requirements. The individual component's assessment in each of these three areas often corresponds to the degree of redundant protection. The most critical system components, which typically also need to meet exacting customer and regulatory requirements, are typically protected with two redundant protection systems. These systems often include two sets of relays (sometimes from two different manufacturers and sometimes using different protection principles), two sets of ac input sources, two sets of dc trip sources, diverse communication routes, etc. Less critical system components, which typically also need to meet lesser customer and regulatory requirements, usually have less redundancy in the protection system.

4.2 Redundancy fundamentals

Protection system redundancy is a design of relaying, auxiliary equipment, and tripping circuits developed to reduce the possibility that a single component failure would prevent the protection system from sensing and isolating a fault in the zone of protection.

Therefore, the zones of protection need to be identified and understood to determine the level of redundancy. [Figure 1](#) is a visualization of these zones of protection at a substation. A zone can be modified by external data such as the status of a breaker or disconnect switch, but the assets available for protection are determined by the connected CTs and VTs. Note that for complete protection, adjacent zones must overlap, otherwise, there

would be gaps in protection. This can be seen in Figure 1 where, for example, the zone of protection a line overlaps with the zone of protection for a bus or the zone of protection for a bus overlaps with the zone of protection for a transformer.

The next step in the design is to identify what equipment needs to be operated to clear faults and abnormal conditions to optimize the protections system's selectivity.

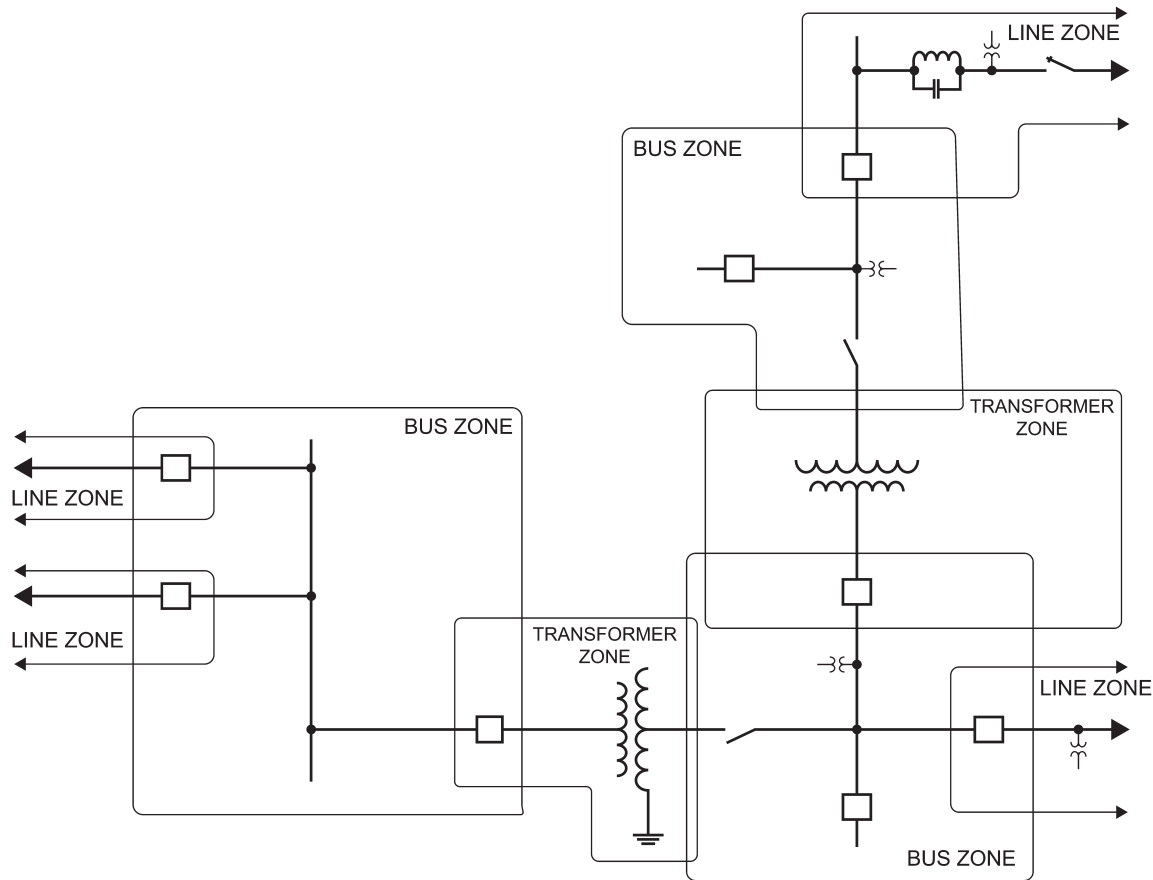


Figure 1—Zone of protection visualization

4.2.1 Purpose of redundancy

Redundancy is required for several reasons including governmental and regulatory requirements, power system reliability, customer satisfaction, system stability, and for maintenance purposes. These issues are dealt with in the remainder of this guide.

4.2.2 Redundancy versus backup

Redundancy is applied to protection systems in different ways to improve dependability, security, and availability. For example, redundant relay systems that utilize different operating principles can improve dependability and availability since either system, operating independently, can accomplish the intended purpose if the other system fails or is out of service for testing.

Note that redundant systems do not always have to be of comparable performance provided that each system fulfills the requirements for the application with regards to operating time, selectivity, etc. For example, if

stability studies have determined that a line can be adequately protected by step distance protection, a distance pilot relay in combination with a step distance relay can be considered a redundant protection system.

Upon the failure or loss of service of a protection system, another system could perform user defined functions. Since this is not a redundant system, it is considered a backup system. In this approach, different means are used to accomplish the same or equivalent functions.

Common convention is to define a redundant system as an additional system that has adequate performance to meet system requirements.

The terminology used to refer to redundant protection systems varies among users. They may be referred to as “System 1/System 2,” “System A/System B,” “Main/Redundant,” or as “Primary/Secondary.” Sometimes, they may be referred to as “Primary/Backup.” This latter terminology, “Primary/Backup,” unintentionally implies that one of the redundant protection systems performs the main function of protection, and the other helps only in the case of a failure of the first system. For example, it has a supervisory timer for its operating element. A backup protection can also operate when the primary is not available, or a component failure causes the primary not to detect a fault. Redundant protection systems are each fully capable in actual practice. Each system can detect and clear faults on its own. The terms “System A/System B” are used to refer to the redundant protection systems in the remainder of this guide to provide a consistent terminology and aid the reader’s understanding of the topics of discussion.

4.3 Required degree of protection

Several factors can affect the choice of types of protection such as overall performance, operating principles, zones of protection, etc. These types of protection are applied depending upon the performance requirements of a system, the critical nature of the protected power system element, and the desired selectivity and are listed as follows:

- *Primary protection* for each power system element such as a transformer, bus, line, etc., operates in the least amount of time and removes the least amount of equipment necessary to isolate faults located within the zone of that protected element. This type of protection is ascribed to each power system element to isolate only this element from its own failures or faults, and it does not operate for a fault or failure occurring on another element of the system, i.e., outside its zone of protection. A redundant application would provide two or more protection systems with the required performance.
- Another type, *local backup*, is a type of protection that is applied at the same substation as the primary protection of a power system element. It is intended to operate if the primary protection of the power system element fails. It typically operates faster and is more selective than the remote backup protection would otherwise be. An example is the breaker failure protection that protects the adjacent power system elements from faults if the breaker fails to operate to clear a fault. Backup protection may offer an appropriate degree of protection for the power system element if the primary protection is unavailable.
- The third type, *remote backup*, protects a power system element it is ascribed to from its own failures and faults and, additionally, may serve as a backup for a fault or failure occurring in the adjacent zone of protection. An example of this type of protection is step distance, which protects a designated line in its primary zone and serves as a remote backup for a downstream line in its backup zone should the protection assigned to the neighboring line malfunction or fail to clear a fault on that line. Thus, the step distance protection can be a combination of two protection types: primary and backup.
- Finally, the fourth type refers to *wide area system protection*, also referred to as system integrity protection scheme (SIPS) or remedial action schemes (RAS). SIPS is often used to maintain the reliable operation of the power system for critical single or multiple contingencies, and to achieve system performance objectives and preventing or reducing large-scale power outages. Often, the

consequences of a SIPS failure to operate when required may be significant; hence, SIPS redundancy considerations are addressed in this guide.

For power system elements that require fault isolation within a specific clearing time to maintain power system stability or other load service requirements, it often becomes necessary to have redundant protection systems that operate simultaneously but independently from each other. System B is applied to avoid the delayed clearing and additional circuit outages that would occur from remote backup operation if System A fails to operate. These additional circuit outages may sometimes lead to cascading events affecting the stability of a power system. System B can be a duplication of System A or it might rely on a diverse operating principle to selectively remove the fault. It operates at the same speed and removes the same equipment from service as System A. System B can operate concurrently with System A or in lieu of it when it is unavailable. To be independent, System B exists as separate hardware and measures separate instrument transformer circuits.

A common component of System A and System B protecting the power system elements is the power circuit breaker. A breaker failure protection is added to protect the power system from faults that are not cleared because the breaker has failed. Breaker failure protection operation avoids the consequence of delayed clearing and multiple outages that would otherwise occur from remote backup operation. Breaker failure protection operates more slowly than the primary protection and remove more elements from service than just the faulted element. However, the breaker failure protection generally operates more quickly and removes fewer elements than remote backup protection. It is common to use the breaker failure operating time as a design target to verify fault clearing within the critical clearing time at the specific location.

The breaker failure protection is a form of local backup protection. Redundancy applied to mitigate failures of other common components such as control batteries, breaker trip coils, and dc circuit breakers or fuses is further described in 5.5, 5.6, and 5.7.

The practice of applying redundant protection systems along with breaker failure protection for each power system element is typical for most transmission level equipment.

For power system elements or system locations where the performance of backup protection is considered acceptable, non-redundant protection systems may be deployed. In this case, there is only one level of backup if the primary protection system fails.

4.4 Economic considerations

Cost is an important factor in determining the level of redundancy to design into a relay system. The cost of the relay system is weighed considering the impact on its dependability and security and the resulting effect on the power system reliability. Each application deserves considerations such as the impact to reliability, value of standard design versus performance, asset strategy, maintenance lifecycle, and reducing potential setting errors. The level of load considered usually increases with the system voltage of the facilities in question. Therefore, it is safe to expect that the higher the voltage class of the protection system, the greater its impact, which results in the need for increased levels of protection redundancy.

4.5 Impact of redundancy on reliability

Redundancy increases the dependability of an overall protection system since the failure of one protection system would not affect the operation of the other. Generally, an increase in dependability decreases security as additional protection devices increase the risk for an unwanted operation. The voting scheme described in 4.5.5 illustrates one method, in which dependability and security can be improved. However, measures to increase dependability may not penalize security to an equal degree. The aim of a protection system design is to find the appropriate combination of the two factors to provide adequate reliability.

The optimal degree of dependability and security is typically determined based on the impact of unwanted operations versus the impact of a failure to operate during a fault condition. For example, the power system may not be greatly affected by a transmission line protection system's unwanted operation for a fault outside the protected line since automatic reclosing can quickly restore service. However, the failure of a bus protection system to operate in response to a bus fault would probably be cleared by remote backup protection, which may delay service restoration for a long time.

4.5.1 Dependability versus security

If a fault occurs and is isolated by a redundant System B relay, the fact that System A relay did not operate does not constitute a mis-operation; however, from an operational point of view this would typically be investigated in the chance that System A relay was defective in some respect.

In the following discussions, “redundant” refers to completely independent systems or components. The failure rate for each system or component is independent from the redundant system's failure rate. A failure in one device does not influence the other and the failures are not triggered by a common cause.⁹

For redundancy considerations in this example, the requirements given for intertripping¹⁰ (equivalent to direct transfer trip) teleprotection communications are used as follows:

- 99.9999% security, or expressed as probability of a false trip less than 10^{-6} (reciprocal of security)
- 99.99% dependability, or expressed as probability of a missed trip less than 10^{-4} (reciprocal of dependability)

4.5.2 Security in a redundant system

If redundant systems are equal and independent, the probability of a false trip is approximately equal to the sum of the probability for each system to give a false trip as graphically presented in Figure 2 and as follows:

- Probability for a false trip for a single system (P_{S_A} or P_{S_B}) is 10^{-6} or expressed as security: 99.9999%.
- Probability of a false trip for a redundant system ($P_{S_{AB}}$) is 2×10^{-6} or expressed as security: 99.9998%



Figure 2—Probability of a false trip in a redundant system

4.5.3 Dependability in a redundant system

The probability of a missed trip, however, is greatly reduced, resulting in much improved dependability. If the systems are equal and independent, both need to fail at the same time for a missed trip to occur. Therefore, the resulting probability of a missed trip is the product of the individual probability as graphically presented in Figure 3.

- Probability of a missed trip for a single system (P_{D_A} or P_{D_B}) is 10^{-4} or expressed as dependability: 99.99%.

⁹In actual installations, there may be common points of failures in redundant protection systems such as redundant schemes tripping a single trip coil or redundant schemes utilizing a single battery supply.

¹⁰As illustrated in teleprotection standard IEC 60834-1 [B23].