

IEEE Guide for Centralized Protection and Control (CPC) Systems within a Substation

IEEE Power and Energy Society

Developed by the
Power System Relaying and Control Committee

IEEE Std C37.300™-2024

IEEE Guide for Centralized Protection and Control (CPC) Systems within a Substation

Developed by the

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

Approved 11 December 2024

IEEE SA Standards Board

Recognized as an American National Standard

Abstract: This guide for Centralized Protection and Control (CPC) systems within a substation addresses the realization of various protection, automation, and control functions within a *CPC system* utilizing data collected from intelligent electronic devices. This guide includes protection, automation, and control functions within a substation, including interconnecting circuits using devices and their interconnections with suitable communication protocols.

This guide includes references to existing standards applicable to protection, automation, and control applications for various types of circuit elements such as generators, transformers, bus bars, shunt and series capacitor banks, reactors, transmission lines, and distribution lines. Some protection and control systems may be applied to protect the integrity of the power system, for example, to avoid cascading outages, equipment damage from unanticipated power system conditions beyond equipment emergency ratings, voltage collapse, angular instability, or other system problems. These systems are referred to as SIPS (system integrity protection schemes).

The guide addresses *CPC system* architectures for typical substation configurations. The guide addresses the reliability and maintainability of each architecture, along with their respective testing requirements. The guide also addresses *CPC-based system* development, installation, commissioning, troubleshooting, and maintenance.

Keywords: centralized protection and control, CPC, CPC system, CPC-based system, digital substation, IED, IEEE C37.300, intelligent electronic device, PIU, process interface unit, SIPS, system integrity protection scheme

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

Copyright © 2025 by The Institute of Electrical and Electronics Engineers, Inc.
All rights reserved. Published 9 May 2025. 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 979-8-8557-1669-6 STD27614
Print: ISBN 979-8-8557-1670-2 STDPD27614

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 IEEE 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 IEEE Societies and subcommittees of IEEE Standards Association (IEEE SA) Board of Governors. 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 involved in technical working groups 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 all standards, including but not limited to the warranties of merchantability, fitness for a particular purpose and non-infringement. IEEE Standards documents do not guarantee safety, security, health, or environmental protection, or compliance with law, or guarantee against interference with or from other devices or networks. 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 their 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 balloting process involves the review of documents in English only. In the event that an IEEE standard is translated, only the English language version published by IEEE is the approved IEEE standard.

Use by artificial intelligence systems

In no event shall material in any IEEE Standards documents be used for the purpose of creating, training, enhancing, developing, maintaining, or contributing to any artificial intelligence systems without the express, written consent of IEEE SA in advance. “Artificial intelligence” refers to any software, application, or other system that uses artificial intelligence, machine learning, or similar technologies, to analyze, train, process, or generate content. Requests for consent can be submitted using the Contact Us form.

Official statements

A statement, written or oral, that is not processed in accordance with the IEEE SA Standards Board Operations Manual is not, and 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, or be relied upon as, a formal position of IEEE or IEEE SA. 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. Statements made by volunteers may not represent the formal position of their employer(s) or affiliation(s). News releases about IEEE standards issued by entities other than IEEE SA should be considered the view of the entity issuing the release rather than the formal position of IEEE or IEEE SA.

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 subcommittees of the IEEE SA Board of Governors 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 revisions to an IEEE standard is welcome to join the relevant IEEE SA working group. You can indicate interest in a working group using the Interests tab in the Manage Profile & 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

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

² Available at: <https://standards.ieee.org/about/contact/>.

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 U.S. 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, neither IEEE nor its licensors waive any rights in copyright to the documents.

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 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

Technologies, application of technologies, and recommended procedures in various industries evolve over time. The IEEE standards development process allows participants to review developments in industries, technologies, and practices, and to determine what, if any, updates should be made to the IEEE standard. During this evolution, the technologies and recommendations in IEEE standards may be implemented in ways not foreseen during the standard's development. 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, data privacy, and interference protection practices and all applicable laws and regulations.

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>.

Participants

At the time this IEEE guide was completed, the H45 Working Group had the following membership:

Ratan Das, *Chair*
Paul Myrda, *Vice Chair*
Mital Kanabar, *Secretary*

Jay Anderson
Bruno Andre
Alexander Apostolov
Philip Beaumont*
Joerg Blumschein
Robin Byun*
Ritwik Chowdhury
Mohammad Dadash Zadeh
Evandro De Oliveira*
Richard Hunt
Erin Jessup

Jack Jester
Chikashi Komatsu
Raluca Lascu
Yuan Liao
Yuri Luskind*
Vahid Madani
Sakis Meliopoulos
Hugo Monterrubio
Bharat Nalla
Damir Novosel
Craig Preuss
Qun Qiu

Jean Raymond
Thomas Rudolph
Jose Ruiz
Mohindar Sachdev*
Jeff Shiles*
Arun Shrestha
Harsh Vardhan
Austin Wade
Donald Ware*
Joemoan Xavier
Qiaoyin Yang*

*Non-voting Member

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

Hani Al-Yousef
Saleman Alibhay
Jay Anderson
Bruno Andre
Boon Chong Ang
Ruby Annette
Butch Anton
Galina Antonova
Michael Basler
David Beach
Tony Bell
Martin Best
Steven Bezner
Sebastien Billaut
Jens Boemer
James Bougie
Bill Brown
Gustavo Brunello
Koti Reddy Butukuri
Peter Capelli
Paul Cardinal
Edgar Cenzone
zhiman chen
Ritwik Chowdhury
Stephen Conrad
Ratan Das
Robert Dempsey
Kurniawan Diharja
Kevin Donahoe
Michael Dood
Neal Dowling
Paul Elkin
William English

Jorge Fernandez Daher
Dale Finney
Rostyslaw Fostiak
Carl Fredericks
Fredric Friend
Jean-Sebastien Gagnon
Gopal Gajjar
Robert Ganser
Louis Garavaglia
Kamal Garg
Shubhanker Garg
Saurabh Ghosh
Jalal Gohari
Abel Gonzalez
Emanuel Grant
Richard Gray
Louis Gullo
Randy Hamilton
John Harley
Shane Haveron
Brian Herrmann
Michael Higginson
Thang Hochanh
Werner Hoelzl
Ali Hooshyar
Yi Hu
Richard Hunt
C. Huntley
Dmitry Ishchenko
Ayodele Ishola-Salawu
Richard Jackson
Jack Jester
John John

Anthony Johnson
Brian Johnson
Laszlo Kadar
Kurt Kainerder
Chintaka Kandapahala
Peter Kelly
Stuart Kerry
Yuri Khersonsky
Heshmatollah Khosravi
Jan-Philipp Kitzig
Gary Kobet
Boris Kogan
Raluca Lascu
Wang Lei
T Leopold
Chase Lockhart
Douglas Logan
Don Lukach
Greg Luri
Bruce Mackie
Vahid Madani
Todd Martin
Pedro Martinez-Julia
Mark Mcchesney
Jeffrey McElray
Scott Mix
Daleep Mohla
Melvin Moncey Joseph
Hugo Monterrubio
William Morse
Bruce Muschlitz
Paul Myrda
Nirmal K. Nair

Gayle Nelms
Rhonda Netzel
Arthur Neubauer
Mfanasibili Nkonyane
Sivaraman P
Lorraine Padden
Bansi Patel
Dhiru Patel
Manish Patel
Paras Patel
Shashikant Patel
Subhash Patel
Claire Patti
Dev Paul
Howard Penrose
Charles Pestell
Andrew Podgorski
Cam Posani
Vedanta Pradhan
Eric Pretorius

Craig Preuss
Priya Raghuraman
Farnoosh Rahmatian
Benito Ramos
Charles Rogers
Benjamin Rolfe
Thomas Rudolph
Ryandi Ryandi
Daniel Sabin
Vincent Saporita
Bartien Sayogo
Heribert Schorn
Oleksandr Sergeenko
Andre Felipe Silva Melo
Veselin Skendzic
Jeremy Smith
Jerry Smith
Chase Sun
David Tepen
Eric Thibodeau

Michael Thompson
Nikolay Tsanov
Eric Udren
Benton Vandiver
S. Venkata
John Vergis
Quintin Verzosa
Ilia Voloh
Austin Wade
David Wallace
John Wang
Lanyi Wang
Stephen Webb
Kenneth White
Terry Woodyard
Mina Yousef
Yu Yuan
Oren Yuen
Hugh Zhu
Waldemar Ziomek

When the IEEE SA Standards Board approved this guide on 11 December 2024, it had the following membership:

David J. Law, *Chair*
Jon W. Rosdahl, *Vice Chair*
Gary Hoffman, *Past Chair*
Alpesh Shah, *Secretary*

Sara R. Biyabani
Ted Burse
Stephen Dukes
Doug Edwards
J. Travis Griffith
Guido R. Hiertz
Ronald W. Hotchkiss
Hao Hu

Yousef Kimiagar
Joseph L. Koepfinger*
Howard Li
Xiaohui Liu
John Haiying Lu
Kevin W. Lu
Hiroshi Mano

Paul Nikolich
Robby Robson
Mark Siira
Lei Wang
F. Keith Waters
Sha Wei
Philip B. Winston
Don Wright

*Member Emeritus

Introduction

This introduction is not part of IEEE Std C37.300-2024, IEEE Guide for Centralized Protection and Control (CPC) Systems within a Substation.

This guide has been developed by the Power System Relaying and Control (PSRC) Committee of the IEEE Power and Energy Society (PES) for transition to next-generation protection and control systems within a substation, described as Centralized Protection and Control (CPC) systems. Prior to initiating this guide, the IEEE Power System Relaying Committee had commissioned a working group on the history and evolution of *CPC systems*, which completed its work in 2015 [B75].⁶ This guide draws from this report.

Over the past three decades, protection and control application⁷ has evolved from the use of discrete function⁸ electromechanical and solid-state devices to more recently integrated protection and control using intelligent electronic devices (IEDs) providing many functions. With technology moving away from discrete intelligent devices to more cognitive and collaborative systems, more emphasis could be on centralized systems. Today, there are examples of substation-level protection and control systems, such as *CPC systems*, that have been implemented in practice. Furthermore, there are examples of complex CPC-type systems for the more advanced system integrity protection schemes (SIPS) in operation. The PSRC decided to prepare a guide because of the many business, technical, and practical reasons for implementing *CPC systems*. The overarching need for *CPC systems* is driven by the following:

- Challenges of the changing grid, including regulatory requirements.
- Availability of intelligent sensors deployed broadly in substations.
- Availability of reliable, high-speed, and cyber-secure communication systems.
- Need for even more operational flexibility in a robust, reliable, and secure manner.

As the grid's dynamic conditions change in real time, there is a need for an adaptive and flexible protection and control system that addresses these challenges by utilizing the benefits of new technologies. There are many factors that impact system dynamics such as intermittency of renewable resources and adequacy of resource scheduling, impacts of inverter-based resources such as their control response and changes in load characteristics (including electrical vehicles). In addition, as a large amount of data is available through various databases and monitoring and control systems, users spend significant time and effort on data management. An optimized platform connects data for various monitoring, protection, and control applications using an approach that can boost efficiencies and the capabilities of engineering resources.

The enhancements in monitoring, protection, automation, and control functions inherent to a *CPC system* offer the agility needed to meet the users' needs. The enhanced capabilities further satisfy regulatory requirements and ongoing operational benefits. A *CPC system* that incorporates newly developed solutions and improves upon existing approaches realizes the next evolutionary step in monitoring, protection, automation, and control systems in addressing the needed agility to achieve improvements in resilience, reliability, availability, and capital cost, as well as ongoing operational benefits. Annex B provides more information on power system drivers, the need for new technologies, and more comprehensive coverage of the reasons for *CPC systems*.

⁶ Numbers in brackets correspond to the references listed in Annex A.

^{7, 8} The meaning of the words *application* and *function* are context-dependent. In protection, automation, and control context: an *application* may consist of one or many *functions* and a function in-turn may consist of many sub-functions or elements. Sometimes, a *function* is also referred to as an *application function*—refer to the title of the IEC TR 61850-7-500 [B58] to see a use of the word *application function*. Electrical power system device function numbers, acronyms, and contact designations are described in IEEE Std C37.2-2022 [B96].

A common language is needed for *CPC systems*; therefore, Clause 4 presents an overview of *CPC systems* and their ancillary components. This includes the process interface, communication networks, physical and cybersecurity, time synchronization, and the station battery system.

Clause 5 then assembles these building blocks into several different architectures for *CPC-based systems*. In addition, Clause 5 provides guidance on reliability (with example reliability calculations provided in Annex E), maintainability, scalability and flexibility, interoperability, and testability.

The *CPC system* approach requires a paradigm shift in all the activities by stakeholders in the life cycle management of the *CPC system*. To help with this paradigm shift, this guide addresses the system engineering aspects of implementing a *CPC-based system*. This includes ongoing operational considerations in testing, maintenance, documentation, and training that are discussed in Clause 6.

Disclaimer: *This document contains deprecated terminology and partly conforms to IEEE P3400/D3 November 2023, IEEE Draft Standard for Use of Inclusive Language in Technical Terminology and Communications [B70]. Non-inclusive (deprecated) language is shown in ~~strike through~~ following the replacement language. Future versions of this document may contain only the inclusive language.*

Contents

1. Overview	13
1.1 Scope	13
1.2 Purpose	13
1.3 Word usage	13
2. Normative references	14
3. Definitions, acronyms, and abbreviations	15
3.1 Definitions	15
3.2 Acronyms and abbreviations	15
4. Overview of a <i>CPC-based system</i>	17
4.1 General	17
4.2 <i>CPC system</i>	20
4.3 Process interface	20
4.4 Communication networks	24
4.5 Physical and cybersecurity	26
4.6 Time synchronization	26
4.7 Station battery system	27
5. <i>CPC-based system</i> architectures	27
5.1 General	27
5.2 Reference architectures	28
5.3 <i>CPC-based system</i> design considerations	35
6. System engineering and implementation	38
6.1 General	38
6.2 Requirements for a <i>CPC-based system</i>	39
6.3 Testing requirements	57
6.4 Maintenance requirements	62
6.5 Documentation requirements	64
6.6 Training requirements	70
Annex A (informative) Bibliography	73
Annex B (informative) Impact of changing power grid and need for new technologies	81
Annex C (informative) Evolution of protection, automation, control, communication, and SCADA	82
C.1 General	82
C.2 Evolution of protection, automation, and control technologies	81
C.3 Evolution of communication technologies	84
C.4 Evolution of SCADA/EMS/DMS technologies	85
Annex D (informative) IEC 61850 and IEC 61869 information	87
D.1 IEC 61850: Communication networks and systems for power utility automation	87
D.2 IEC 61869: Instrument transformers	88
Annex E (Informative) Reliability and availability evaluation for a <i>CPC-based system</i>	90
E.1 General	90
E.2 Reliability block diagram	90
E.3 Reliability and availability assessment	91

E.4 Reliability and availability indices for reference architectures	93
Annex F (informative) Traditional application examples for a <i>CPC system</i>	104
F.1 General	104
F.2 Protection	104
F.3 Automation and control	105
F.4 Analytics	108
F.5 Inter-substation protection and interface between substations	109
F.6 Monitoring and alarms	111
Annex G (informative) Advanced applications	114
G.1 General	114
G.2 Dynamic state estimation-based protection	114
G.3 Distributed energy resources management system aggregator	114
G.4 Distributed FLISR and high impedance fault location	115
G.5 Microgrid protection and control	115
G.6 Machine learning based applications	115
G.7 Incipient failure detection	116
G.8 Hidden failure detection	116
Annex H (informative) Testing approaches for a <i>CPC-based system</i>	118
H.1 General	118
H.2 Process interface unit	118
H.3 Communications networks	118
H.4 Protection	120
H.5 IEC 61850 based system testing capabilities	120
Annex I (informative) Example of a <i>CPC-based system</i>	121
Annex J (informative) Technology trends	123
J.1 General	123
J.2 Virtualization	123
J.3 Software-defined networking	123
J.4 Mitigation of effects from geomagnetic disturbance and electromagnetic pulse	125
J.5 Digital twin	126
J.6 Situational awareness	127
J.7 Vision for an electric grid of the future	128

IEEE Guide for Centralized Protection and Control (CPC) Systems within a Substation

1. Overview

1.1 Scope

This guide for centralized protection and control (CPC) systems addresses the realization of various protection, automation, and control functions within a *CPC system* utilizing data collected from intelligent electronic devices (IEDs). This guide includes protection, automation, and control functions in a substation, including interconnecting circuits using devices and their interconnections with suitable communication protocols.

This guide includes references to existing standards applicable to protection, automation, and control applications for various types of circuit elements such as generators, transformers, bus bars, shunt and series capacitor banks, reactors, transmission lines, and distribution lines. The guide addresses the reliability of each *CPC-based system* architecture for typical substation applications. The guide also addresses CPC development, installation, testing, troubleshooting, and maintenance.

1.2 Purpose

This guide summarizes the generally accepted practices for the use of centralized protection and control (CPC) systems within a substation.

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*).^{9, 10}

⁹ The use of the word *must* is deprecated and cannot be used when stating mandatory requirements, *must* is used only to describe unavoidable situations.

¹⁰ The use of *will* is deprecated and cannot be used when stating mandatory requirements, *will* is only used in statements of fact.

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. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments or corrigenda) applies.

IEC 61850-3, Communication networks and systems for power utility automation—Part 3: General Requirements.¹¹

IEC 61850-5, Communication networks and systems for power utility automation—Part 5: Communication requirements for functions and device models.

IEC 61850-7-4, Communication networks and systems for power utility automation—Part 7-4: Basic communication structure—Compatible logical node classes and data classes.

IEC 61850-9-2, Communication networks and systems for power utility automation—Part 9-2: Specific communication service mapping (SCSM)—Sampled values over ISO/IEC 8802-3.

IEC/IEEE 61850-9-3, Communication networks and systems for power utility automation—Part 9-3: Precision time protocol profile for power utility automation.

IEC 61869-9, Instrument transformers—Part 9: Digital output requirements based on IEC 61850-9-2 Merging unit (MU).

IEC 61869-13, Instrument transformers—Part 13: Stand Alone Merging Unit (SAMU).

IEC 62439-3, Industrial communication networks—High availability automation networks—Part 3: Parallel Redundancy Protocol (PRP) and High-availability Seamless Redundancy (HSR).

IEEE Std 1588™, IEEE Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems.^{12, 13}

¹¹ IEC publications are available from the International Electrotechnical Commission (<http://www.iec.ch/>).

IEC publications are also available in the United States from the American National Standards Institute (<http://www.ansi.org/>).

¹² IEEE publications are available from the Institute of Electrical and Electronics Engineers (<https://standards.ieee.org/>).

¹³ The IEEE standards or products referred to in Clause 2 are trademarks owned by the Institute of Electrical and Electronics Engineers, Incorporated.

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.¹⁴

centralized protection and control (CPC): The provision of functions such as protection, automation, control, monitoring, communication, and asset management performed by a centralized system rather than by a collection of discrete IEDs.

CPC-based system: CPC system(s) and other peripheral devices and services such as process interface unit, time synchronization system, and communication networks to provide the functionalities in a CPC system.

CPC system: A computing platform capable of providing protection, automation, control, monitoring, communication, and asset management functions.

CPC system third-party application: Software applications that are not developed by the CPC system manufacturer, which can be added or deleted during the life cycle of the CPC system, by using the interface provided (and disclosed) by the manufacturer of the CPC system.

3.2 Acronyms and abbreviations

For the purposes of this document, the following acronyms and abbreviations apply:

ADMS	advanced distribution management system
CAD	computer-aided design
CB	circuit breaker
CPC	centralized protection and control
Cs	current sensor
CT	current transformer
CVT	capacitive voltage transformer
DER	distributed energy resources
DERMS	DER management system
DFR	digital fault recorder
DMS	distribution management system
DNP	distributed network protocol
EMS	energy management system

¹⁴ *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.

ESW	Ethernet switch
FAT	factory acceptance testing
GNSS	global navigation satellite system
GOOSE	generic object-oriented system event
HMI	human-machine interface
HSR	high-availability seamless redundancy
IED	intelligent electronic device
I/O	input/output
IP	internet protocol
LAN	local area network
LPIT	low power instrument transformer
MMS	manufacturing message specification
MTTF	mean time to failure
MTTR	mean time to repair
MU	merging unit
NEIU	non-electric interface unit
PIU	process interface unit
PRP	parallel redundancy protocol
R-SV	routable sampled value
RBD	reliability block diagram
R-GOOSE	routable generic object-oriented system event
RSTP	rapid spanning tree protocol
RTU	remote terminal unit
SAT	site acceptance testing
SCADA	supervisory control and data acquisition
SCL	system configuration language
SDN	software-defined networking
SER	sequence of events recorder
SIPS	system integrity protection scheme
SIU	switchgear interface unit

SLD	single line diagram
SV	sampled value
TCP	transmission control protocol
TS	time source
UDP	user datagram protocol
Vs	voltage sensor
VT	voltage transformer
WAN	wide area network

4. Overview of a *CPC-based system*

4.1 General

The concept of a *CPC system* dates back almost to the beginning of the wide adoption of computers for businesses, starting with the first proposal published in 1969 (Rockefeller [B26]¹⁵), and the first installation as a field proof of concept in 1971 (Gilcrest, Rockefeller, and Udren [B27]). The early experimental systems focused on computer relaying in general and were limited by the technology available at the time. As protection, automation, control, and communications evolved (refer to Annex C), these advancements supported projects in the late 1980s and early 1990s that began to experiment with centralized protection and control specifically. Some of these early projects are briefly discussed in an IEEE Power System Relaying Committee WG K15 report [B75], and in WG K15 IEEE Transaction paper [B167].

Figure 1, an extension of Figure C.1 with the addition of Block 5, illustrates the evolution of the protection, automation, control, monitoring, asset management and communication system leading to a *CPC system*. Block 1 shows electro-mechanical and solid-state relays. Block 2 adds communications with a remote terminal unit (RTU) or data concentrator, the start of a substation automation system. Block 3 shows communications using protocols; block 3 also represents peer-to-peer communications using a generic object-oriented system event (GOOSE). Block 4 shows the transfer of digitized analog values directly to IEDs from merging units (MUs) using IEC 61850-9-2 sampled values (SVs). Block 5 indicates the transfer of sampled analog values from process interface units (PIUs) to *CPC systems*, as well as GOOSE messages between *CPC systems* and PIUs, and manufacturing message specification (MMS) messages transferred from PIUs to the *CPC system* as discussed in an IEEE PSRC WG K15 report [B75], and paper [B167]. Use of the “layer” terminology is in the IEEE PSRC WG K15 report [B75] and the same approach is used in Figure 1 and Figure C.1. The relationship between different layers and levels is clear in Figure 1 and Figure C.1.

Components of a *CPC-based system* include the following:

- A *CPC system* (refer to 4.2)
- The process interface (refer to 4.3)
- Communication networks (refer to 4.4)
- Physical and cybersecurity (refer to 4.5)

¹⁵ The numbers in brackets correspond to those of the bibliography in Annex A.

- Time synchronization (refer to 4.6)
- Station battery (refer to 4.7)

Protocols specified by IEC 61850-9-2 are used in this guide to communicate between a *CPC system* and other components of a *CPC-based system* such as a PIU. IEC 61850-9-2 provides a standardized approach for interoperability where the communication of MMS, GOOSE, and SV between components from different manufacturers can be part of the project implementation, while providing desired performance requirements. Some of the considerations for the use of the IEC 61850-9-2 specified protocols are as follows:

- Expected longevity of a standards-based approach allowing technology advancements.
- Compliance with regulatory requirements.
- Manufacturer-independent tools to support troubleshooting, maintenance, and hardware/software upgrades over the life cycle.
- Interoperability between all components of a *CPC-based system*.
- Scalability and flexibility.
- Testing efficiency.

While protocols specified by IEC 61850-9-2 are used in this guide, similar functionalities and performance can be achieved in a *CPC-based system* using protocols other than those included in IEC 61850-9-2 that are beyond the scope of this guide. In such a case, interoperability cannot always be achieved.

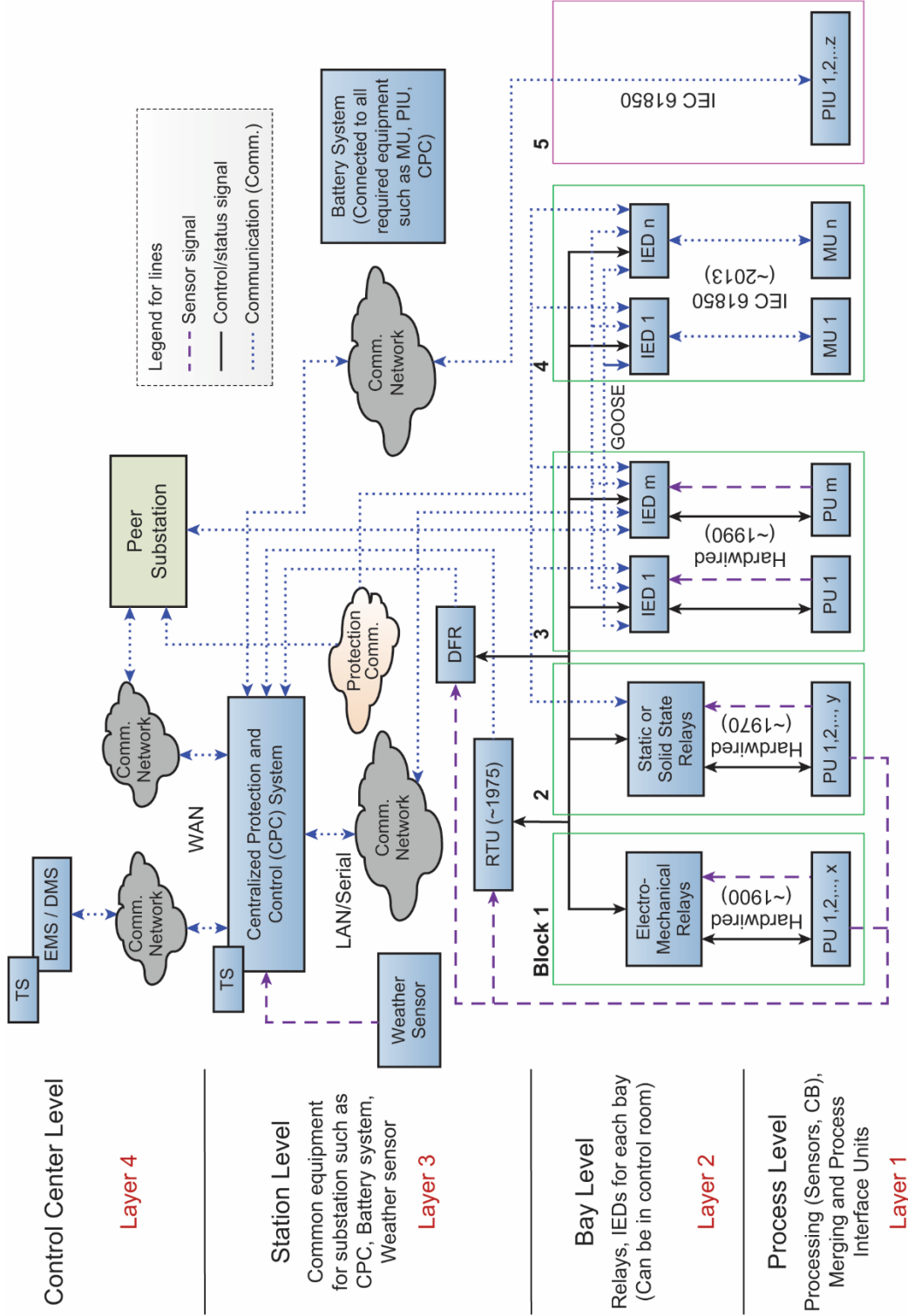


Figure 1—Evolution of CPC system

4.2 CPC system

A *CPC system* is the core of the *CPC-based system* within a substation. The *CPC system* provides protection, automation, control, and asset management application functions (refer to 6.2.7.9) for a substation.

The *CPC system* hardware characteristics to consider are as follows:

- Scalable, modular, and flexible
- Meets industry standard requirements, for example, environmental standard requirements as in 6.2.1
- Application-specific to meet specifications and standards of protection and control applications

Application-specific hardware can be built and certified using modular platforms that:

- Allow the end-user to choose from a wide selection of hardware modules and platform choices, independent of the software and application choices.
- Allow the end-user to select appropriate hardware modules that are already in use in their environment, or they have the expertise to support the operational needs of the *CPC system*.
- Allow the electric power industry to take advantage of mainstream hardware development, addressing applications in a broad spectrum of industries, supporting the use of large-scale real-time as in ISO/IEC/IEEE 24765 [B119] and non-real-time data processing applications.

A *CPC system* with a human-machine interface (HMI) can enable the visualization of the *CPC system* functions and control of substation equipment. In the past, the HMI could have been used primarily for visualization and thus not been critical to substation testing, operation, and maintenance; however, with a *CPC system*, the HMI becomes critical to perform these tasks.

4.3 Process interface

Sensors are the front-end interface of a *CPC-based system* with the power system process for collecting data, which in turn is used by the *CPC system* to make decisions for operating the system, such as controlling switching and isolating equipment. Recent advancements in sensor integration technology make a *CPC-based system* solution practical with the use of PIUs. Standardized high reliability communication technology allows the integration of PIUs with the *CPC system*. The integration supports the replacement of hardware at the end-of-useful life, as discussed in an IEEE PSRC WG I22 Report [B24] and upgrade of firmware/software during the life cycle of the *CPC system*, as discussed in Clause 6.

4.3.1 Process interface unit

A process interface unit (PIU) combines a merging unit (MU)—discussed in subclause 4.3.1.1, switchgear interface unit (SIU)—discussed in subclause 4.3.1.2, and non-electric interface unit (NEIU)—discussed in subclause 4.3.1.3, into one device. However, stand-alone MU (SAMU), SIU, and NEIU devices providing the functionalities of a PIU can also be used with a *CPC system*, which can be avoided for complexities associated with separate subsystems. In this guide, it is considered that MU, SIU, and NEIU functionalities are provided within a PIU. A PIU interfaces with voltage and current transducers to measure voltage and current signals. It also interfaces with primary switching devices, such as circuit breakers (CBs),

disconnectors, and grounding/earthing switches to monitor their status and control those devices. The PIU is also connected to an Ethernet switch or directly to a *CPC system*, typically via a patch panel. The PIU can publish measurement data and equipment status and accept control commands for equipment operation. Figure 2 shows an example of a PIU connection to process elements with IEC 61850-7-4 modeling of logical nodes inside the PIU.

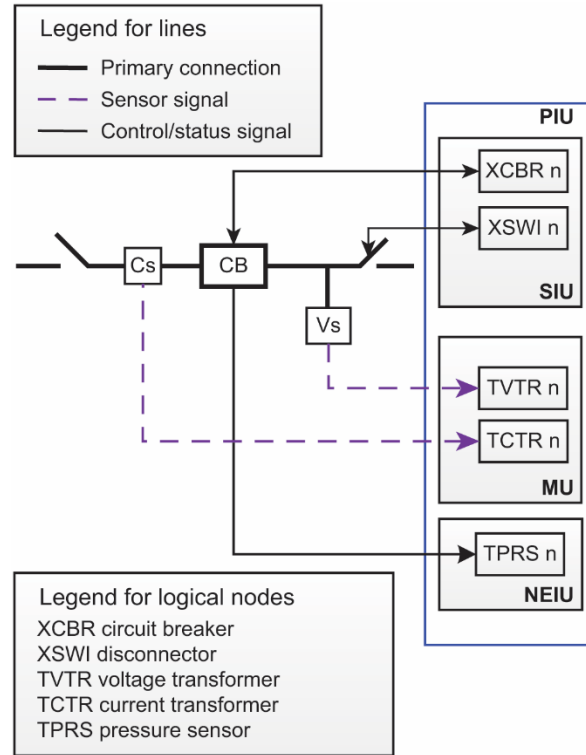


Figure 2—Typical process interface unit (PIU)

Two types of PIUs are considered for the purpose of this guide based on their applications as per end-user-defined practices. One substation can have a combination of two types of PIUs, based on end-user selection and preferences. Functionalities of both Type 1 and Type 2 PIUs are described in Table 1. As can be seen from Table 1, Type 2 PIU has additional functionalities as compared to Type 1 PIU. A protection IED with Type 1 PIU functionalities can be used as a Type 2 PIU.

Table 1—Type 1 and Type 2 PIU features

Feature	Type 1	Type 2
Functionality of a SAMU (SV) (as per IEC 61850-9-2, IEC 61869-9, IEC 61869-13) ^a	X	X
Publish analog values and equipment status as remote input/output I/O (GOOSE) functions	X	X
Bay equipment control interface and accept control commands for equipment operation	X	X
Overvoltage, Overcurrent (and other) protection functions	—	X
Trip associated circuit breakers during overvoltage and overcurrent conditions in case of communication failure with the <i>CPC system</i>	—	X
Additional control and automation functionality	—	X

^aIEC 61869-9 is a product family standard applicable to instrument transformers with digital output and SAMUs as per IEC 61869-13, providing a communication profile based on IEC 61850-9-2 (SV). 9-2LE [B161] is one possible communications profile available under IEC 61869-9.

4.3.1.1 Merging unit

IEC 61850-2 [B34] and IEEE Std C37.92-2023 [B100] describe the merging unit (MU) that publishes current and voltage measurements using standardized time-coherent digital signals. The logical node for the current transformer, TCTR, and logical node for the voltage transformer, TVTR, as per IEC 61850-7-4 can be used to derive a standard digital output from analog inputs in MU.

MUs typically have the following functionalities:

- Analog system comprising of conditioning of sensor signals, and some processing of voltage and current signals in which measurements are time-synchronized
- Digital system providing IEC 61850-9-2 or other compliant SV

Any MU that can interface with both conventional and non-conventional sensors allows the implementation of the *CPC-based system* in existing or new substations. The MU has several functions, as can be seen in Figure 3.

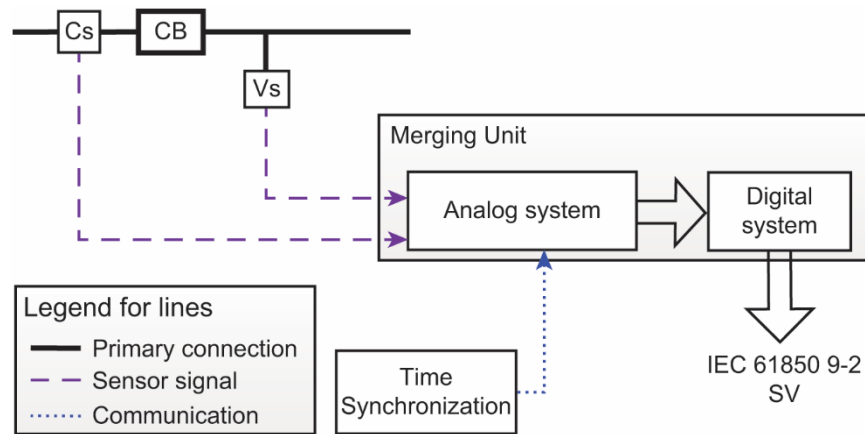


Figure 3—Typical merging unit

The MU can be considered as the analog input module of a conventional protection or other multifunctional IED. The difference is that, in this case, the substation communication network serves as the digital data bus between the input module and the protection functions in the IED.

Figure 3 shows a time synchronization interface via a communication connection. MUs communicate time-synchronized measurements to the *CPC system*. This makes time synchronization across the *CPC system* and *CPC-based system* critical in supporting protection applications, such as transformer protection, bus protection, generator protection, and wide-area interconnected systems. Refer to 4.6 for more discussion on time synchronization.

4.3.1.2 Switchgear interface unit

The switchgear interface unit (SIU) is the control and status interface for primary system equipment such as circuit breakers and disconnectors to the process bus (refer to Figure 2). A SIU that complies with IEC 61850-7-4 can support GOOSE messages with *CPC systems* and can also support MMS client and server communications.

4.3.1.3 Non-electric interface unit

The non-electric interface unit (NEIU) converts analog signals from non-electric sensors, such as CB insulating gas density, transformer oil temperature, or weather sensors, into time-synchronized streams of SVs according to IEC 61850-9-2 or GOOSE messages (including analog GOOSE messages) according to IEC 61850-8-1 [B37].

4.3.2 Sensors

Various types of sensors interface the PIU with the process. These sensors, such as a voltage sensor (Vs) and a current sensor (Cs), are connected to MU, SIU, or NEIU within the PIU.

4.3.2.1 Conventional current and voltage transformers

Conventional electromagnetic current transformer (as per IEC 61869-1 [B39], IEC 61869-2 [B40]) and voltage transformer (as per IEC 61869-3 [B41]) are the most widely used interfaces with the power system. Capacitive voltage transformers (CVTs, sometimes called capacitively coupled voltage transformers or CCVTs) (as per IEC 61869-5 [B42]) are generally used for transmission systems. Requirements for these measurement transducers for power system protection, automation, control, monitoring, asset management, and metering are actively maintained in the referenced standards.

4.3.2.2 Low power instrument transformers

Passive low power instrument transformers (LPITs), or similar sensors, have been studied to interface directly with microprocessor based IEDs. They are the successors of conventional iron core instrument transformers.

Different categories of LPITs are described by the IEC 61869 standard: Low Power Current Transformer (LPCT) as in IEC 61869-10 [B46] and Low Power Voltage Transformer (LPVT) as in IEC 61869-11 [B47]:

- Passive low power current transformers (LPCT) have an analog output proportional to the primary current. For example, LPCTs can have iron core coils with integrated shunts as a current-to-voltage converter (primary converter), or they can have an output signal proportional to the derivative of the primary current (such as air-core Rogowski coils as discussed in IEEE Std C37.235 [B109]).
- Passive low power voltage transformers (LPVT) are based on the voltage divider principle with an output signal proportional to the primary voltage. LPVT can be built, for example, as resistive dividers, capacitive dividers, or resistive-capacitive dividers.

According to a general block diagram given in IEC 61869-6 [B43], LPITs do not use an active primary converter (i.e., without any active electronic component). Therefore, there is no need for a primary power supply. Additionally, neither a secondary converter nor a secondary power supply is used in these LPITs.

LPITs based on passive sensors can use electronic components, or not, according to the type of sensors. Electronic LPITs, including optical transformers, are defined in IEC 61869-7 (voltage) [B44] and IEC 61869-8 (current) [B45]. An optical transformer is available for application in Orr et al. [B143].

When a *CPC system* interfaces with other optical devices such as optical measurement units (OMUs), for example, overexcitation (V/Hz) monitoring, refer to IEEE Std C37.241-2017 [B112].

4.3.2.3 Other types of sensors

There are many other types of sensors, in addition to voltage and current, that can be interfaced with the *CPC system*. Some of these sensors are as follows:

- Temperature sensor (e.g., use of a resistance temperature detector to measure ambient, winding, or oil temperature)
- Humidity sensor
- Transformer dissolved gas analyzer or other transformer insulation monitoring sensors
- Switchgear monitoring and control, including sulfur hexafluoride (SF6) gas pressure monitoring
- Transformer tap-changer monitoring and control
- Weather sensors such as wind speed sensors
- Station battery voltage measurement

The previous interface devices could be a stand-alone device or could be available as a function in multi-function devices. The output of these stand-alone sensors could be available as a DC mA/mV signal, a GOOSE message, or streaming SVs, which can be interfaced using the PIU.

4.4 Communication networks

A *CPC-based system* uses a communication network to connect the *CPC system* with the components of the *CPC-based system*. For example, the communication network connects PIUs to the *CPC system* and to the time synchronization source. The communication network includes a physical layer and a logical layer as defined in the Open Systems Interconnection (OSI) model, which are covered by cybersecurity (refer to 4.5).

Using standardized, high-reliability communication networks is helpful for the replacement of hardware at the end-of-useful life, failed hardware as discussed in an IEEE PSRC WG I22 Report [B24] and upgrade of firmware/software during the life cycle of the *CPC-based system*. Refer to 6.4 for more information on maintenance requirements for a *CPC-based system*.

4.4.1 Physical layer

A typical physical layer used in *CPC-based systems* is IEEE 802.3 (also called Ethernet) communications [B79] using optical fiber. Optical fiber provides reliable data communication with resistance to electromagnetic interference and supports the distance that likely exists between the different components of a *CPC-based system*.

The Physical Layer (PHY) is the layer in the open systems interconnection (OSI) model, as defined in ISO/IEC 7498-1 [B118]. Typically, a *CPC-based system* uses a variety of communication media that matches the performance requirements.

For example, physical distances can be hundreds or thousands of meters. Physical boundaries, such as crossing through a shielded control house and equipment enclosures, also affect the media performance requirements. Some cases require intermediate transitions of media types, e.g., optical fiber cables may require patch panels to transition from higher-strand count cables to patch cables connecting to the PIUs. The choice of media types depends upon the specifics of an installation.

One consideration of the physical layer is how it is laid out compared to the physical process. A communication path typically may not follow how the physical process is laid out and constructed, causing the installation of dedicated conduit runs that otherwise might not be installed. Communication network topology requirements are different from the requirements for electrical construction; thus, typically, the paths are not aligned.

Refer to IEEE Std 525 [B78] for guidance on the design and installation of communication cable systems inside substations. Refer to subclause 6.2.4 for communication network engineering. Refer to subclause 6.2.9 for communications with remote substations.

4.4.2 Data sharing and protocols

This guide considers the data models, protocols, services, and messaging of the IEC 61850-8-1 [B37], IEC 61850-7-4, IEC 61850-9-2, and IEC 61850-9-3 for sharing data and control commands between the devices that comprise the *CPC-based system*. It remains important that the communications methods complete a substation automation system and allow other mechanisms and protocols to coexist on the IEEE 802.3 (Ethernet) communication network. It is also important to account for enhancement and innovation in communications methods. The methods and protocols selected are standardized to help ensure interoperability.

The low latency, high data transmission rate, and bandwidth requirements lead to select protocols that operate at the data link layer using media access control (MAC) and logical link control. Protocols operating at this level have less overhead and need less processing power and time to encode and decode the messages to achieve faster communications.

Some communications needs, such as control services, require dedicated connections between devices. These needs are best met by protocols operating at a transport layer using transmission control protocol (TCP) or user datagram protocol (UDP) and internet protocol (IP) addressing.

4.4.3 High-level architecture

Figure 1 shows the general, high-level architecture of a *CPC-based system*. Support from the underlying communications network is important for the *CPC-based system* architecture. This includes the requirement to connect to other external elements that exist outside of the *CPC-based system*, such as supervisory control and data acquisition (SCADA) networks, as well as the requirement to connect to internal devices that comprise the *CPC-based system*, such as PIUs. With IEC 61850-9-2 communications, it is common to describe the external interface to SCADA and neighboring substations as “station bus,” and the internal interface to PIUs and primary equipment as “process bus.”

4.4.3.1 Station bus

The *CPC-based system* communication network includes a station bus that interconnects the *CPC system* with other elements that could exist outside of the *CPC system*, such as the SCADA system. According to IEC TR 61850-90-4 [B62], station bus typically implements protection-related data exchange between bay and station level, data exchange within the IEDs/systems at the bay-level, control-data exchange between bay-level and station level, and data exchange within the systems at the station level. Depending on system architecture, remote control-data exchange between a RTU or data concentrator with a remote control center and direct data exchange among the bays can be supported by the station bus. In addition, a *CPC-based system* requires an interface for managing its network components [e.g., Simple Network Management Protocol (SNMP) and syslog protocols]. Refer to 6.2.4 for specific performance requirements.

4.4.3.2 Process bus

IEC TR 61850-90-4 defines process bus as the “communication network that connects the IEDs at primary equipment level to other IEDs.” Process bus typically includes current transformer (CT) and voltage transformer (VT) SV data exchange between process and bay-level as per IEC 61869-9 as inputs to the *CPC system* and control related-data exchange between process level and bay-level where each PIU is also connected to the primary equipment for exchanging status and control information using GOOSE messages.

The majority of mission-critical devices like sensors and PIUs are interconnected by an Ethernet network using Layer 2 protocols, as defined in the OSI model (ISO/IEC 7498-1, [B118]) in order to meet requirements for low latency and fast switchover times (refer to 6.2.4 for specific requirements).

4.5 Physical and cybersecurity

Securing a *CPC-based system* involves both the physical security and the cybersecurity. Refer to IEEE Std 1402 [B82] for guidance on physical security. Industry regulations such as the North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) standards [B142] include relevant physical and cybersecurity requirements. Also refer to IEEE Std C37.240 [B111], IEEE Std 1686 [B88], IEC 62351-3 [B48], IEC 62351-5 [B49], IEC 62351-7 [B50], IEC 62351-8 [B51] and IEC 62351-11 [B52] for cybersecurity requirements for substation protection, automation, and control systems.

Physical security of a *CPC-based system*, as in a conventional IED-based system, is typically enabled through a physical access control system that can be impacted by the placement of PIU or MU in the substation yard. A physical access control system is generally comprised of electronics and a communication network. Physically separating the physical access control from the *CPC-based system* communication network(s) is a best practice.

4.6 Time synchronization

A *CPC-based system* requires accurate and reliable time synchronization of all system components to make valid operating decisions, provide consistent timing sources for sequential event recording for commissioning, for event analysis, aid with troubleshooting during start-up, root cause analysis of possible failures, and maintenance and life cycle related tracking. All components that make up the *CPC-based system*, including distributed components like PIU, sensors, network switches, and the *CPC system*, are synchronized to a common time source or sources in the case of a redundant timing system.

Time synchronization is achieved by one or more clocks providing a signal. Time synchronization signals can be published through the same packet-based communication network that connects the *CPC-based system* components together. This simplifies system architecture, as the time synchronization system is fully integrated into the *CPC-based system*.

Typically, synchronization is done using a common reference, such as coordinated universal time (UTC). Various sources of time are possible, for example, a global navigation satellite system (GNSS) or a terrestrial-based time distribution system such as ITU-T G.8275/Y.1369 [B121]. The use of common time references among various systems, such as SCADA and enterprise systems, is required to meet compliance and audit requirements.

Beyond working through the packet-based communication network, the time synchronization system meets specific requirements for time accuracy at all devices and during all operating conditions. The distributed time synchronization requirements typically range from equipment and systems integrated at the *CPC-based system* to maintain the correct functioning and operation of all local protection elements to allowing

user-defined information to be communicated with other *CPC Systems* either within the same substation, or other stations as needed, such as for SIPS purposes, or to be accessed by authorized users at the enterprise level. It is important that the design philosophy provides for the acceptable performance of protection and control functions (or backup functions) when the external time reference is unavailable.

Designing a *CPC-based system*, therefore, requires a basic understanding of implementing a robust, accurate time synchronization system over a packet-based communication network. Some options are discussed in IEEE Std 2030.101 [B93].

User awareness of technical requirements for a time source to help ensure resilient Positioning, Navigation, and Timing (PNT) of time synchronization equipment, including integrated PNT receivers and PNT source components, such as GNSS chipsets, and traceability of failure, are important factors in deciding the method of synchronization for a *CPC-based system*.

4.7 Station battery system

Today, most substation control functions use station battery systems to maintain the integrity of the substation monitoring, protection, and control independent from the ac power source and provide an additional level of resiliency. The *CPC system* can be specified as a dc-operated system and meet the relevant standard (refer 6.2.1), for transient susceptibility requirements, including input or output contacts where applicable.

5. *CPC-based system architectures*

5.1 General

CPC-based system architectures can be developed from reference architectures presented in Clause 5. Further variations of these architectures may be agreed between the *CPC system* provider and the end-user by utilizing the foundations discussed in this guide, including the redundancy requirements. Each architecture presented herein is simplified by **not** showing the following:

- Cybersecurity components, e.g., firewalls.
- Each level of redundancy.
- Subsystems providing the functionality within a *CPC system*.
- Direct connections over the station bus to neighboring substations or control centers via the RTU/gateway function inside the *CPC system*. Time synchronization source and method of synchronizing the IEDs. Refer to 4.6 and 6.2.6.1.
- PIU class: Type 1 or Type 2. Refer to 4.3.1.
- Specific network architectures. Refer to IEC TR 61850-90-4 for the engineering considerations to support performance and availability requirements for station bus and process bus.¹⁶

¹⁶ Possible integration of station bus and process bus making use of virtual local area network (VLAN) to manage the dataflow. In addition, IEC 62439-3 defines the technology and protocols (PRP and HSR) that enable different architectures with cross connections to provide the redundancy.

Terms “main” and “redundant” *CPC systems*, along with “System A” and “System B,” as applicable, are used in this guide for different architectures except for Type 1 and Type 2, (where “backup” is used) as defined for protection systems in IEEE Std C37.120 [B107]. Further coordination among *CPC systems* may be considered while designing the system. Each main/redundant *CPC system* may have its own redundancy and management.

5.2 Reference architectures

Seven different *CPC-based system* reference architectures, **Type 1** through **Type 5**, **Type 5a**, and **Type 3a**, are considered in this guide. Most of these reference architectures are based on the architectures discussed in the IEEE PSRC WG K15 report [B75].

5.2.1 Type 1

Figure 4 illustrates a Type 1 architecture where bay-level IEDs are interfaced with process level equipment over traditional copper wire. The IEDs perform main protection and control functions and communicate with the *CPC system* using different protocols and services according to each supported application's requirements.

With this architecture, the *CPC system* may perform backup protection and control functions of the entire substation, as well as other substation protection and control applications such as load shedding and breaker failure. The *CPC system* depends on each IED's ability to communicate the desired information. Individual IEDs at the bay-level perform main (System A) protection and control functions per bay; whereas one or more *CPC systems* can provide the backup (System B) functions for the entire substation. This architecture may replace individual redundant (System B) IEDs with one or more *CPC systems*. A Type 1 architecture has Cs/Vs signals to per bay IEDs that are not digitized. This architecture may provide challenges in testing and managing/maintaining the IEDs outside the control room.

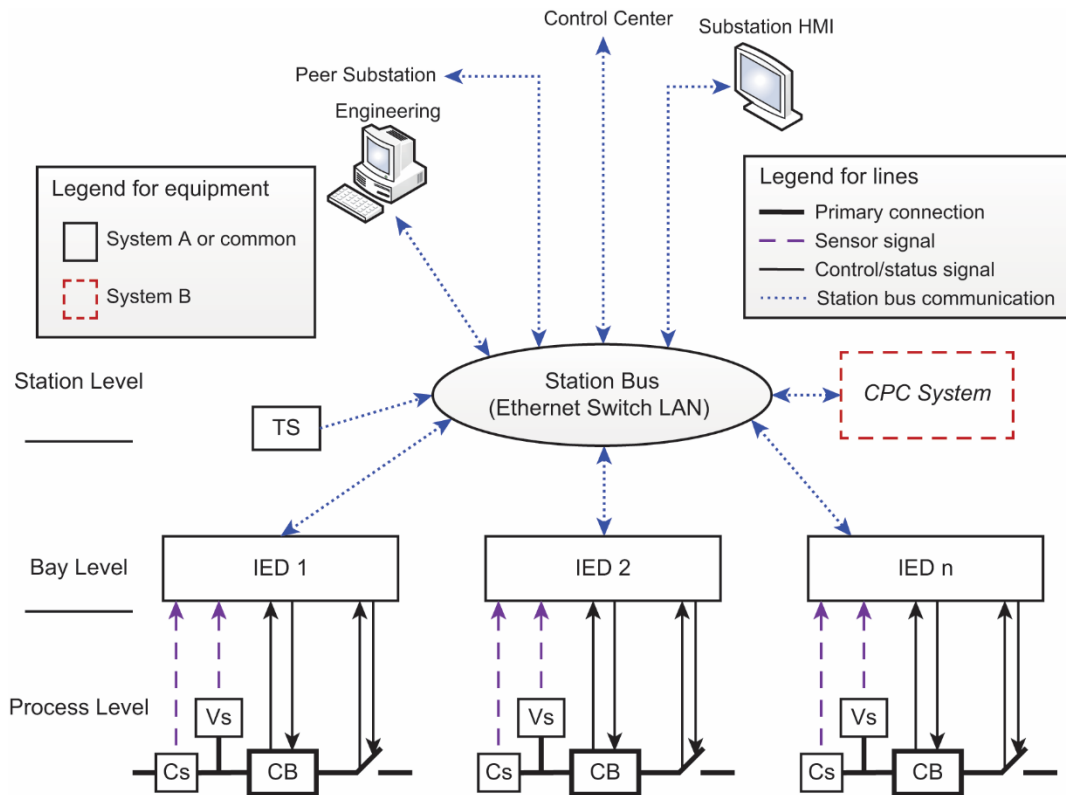


Figure 4—Type 1 architecture

5.2.2 Type 2

A Type 2 architecture connects IEDs and the *CPC system* to PIUs over multiple point-to-point process bus interfaces, as shown in Figure 5. Each PIU at the process level is connected to IEDs and the *CPC system* over a point-to-point connection. The same PIU may be directly interfaced with IEDs and *CPC systems* where the PIU sends SV to IEDs and *CPC systems* while publishing and subscribing to GOOSE messages between them. The *CPC system* may perform either main or redundant protection and control functions of the entire substation, as well as other station level protection and control applications. This architecture replaces all redundant IEDs with the *CPC System* and provides additional functionality at the station level, some of which cannot be possible with bay-level IEDs.

The Type 2 architecture allows the *CPC system* to communicate directly with PIUs at the process level to receive and send data without interfacing with bay-level IEDs. A redundant PIU and *CPC system* may exist in this architecture with independent point-to-point connections from each PIU to a redundant *CPC system*.

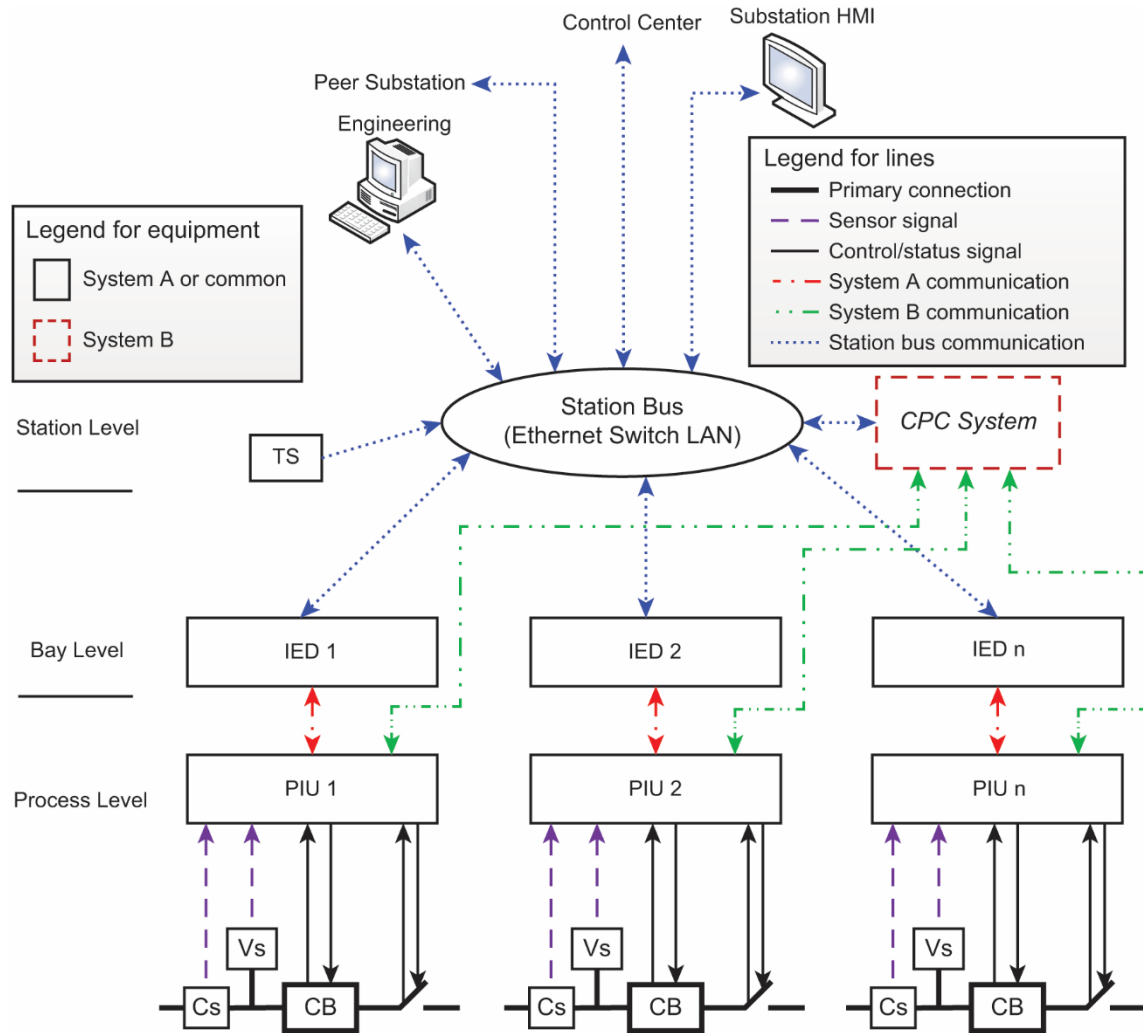


Figure 5—Type 2 architecture

5.2.3 Type 3

Figure 6 illustrates a Type 3 architecture, in which all individual bay-level protection and control IEDs are replaced by *CPC systems* at the station level. The PIUs at the process level are connected to *CPC systems* over point-to-point connection. The same PIU broadcasts data to each *CPC system*, such as SV, and each *CPC system* can interface with each PIU independently to publish and to subscribe messages, such as GOOSE. All protection and control functions within a substation are facilitated in each individual main and redundant *CPC system*. There can be more than two *CPC systems* at the station level to further enhance reliability and availability.

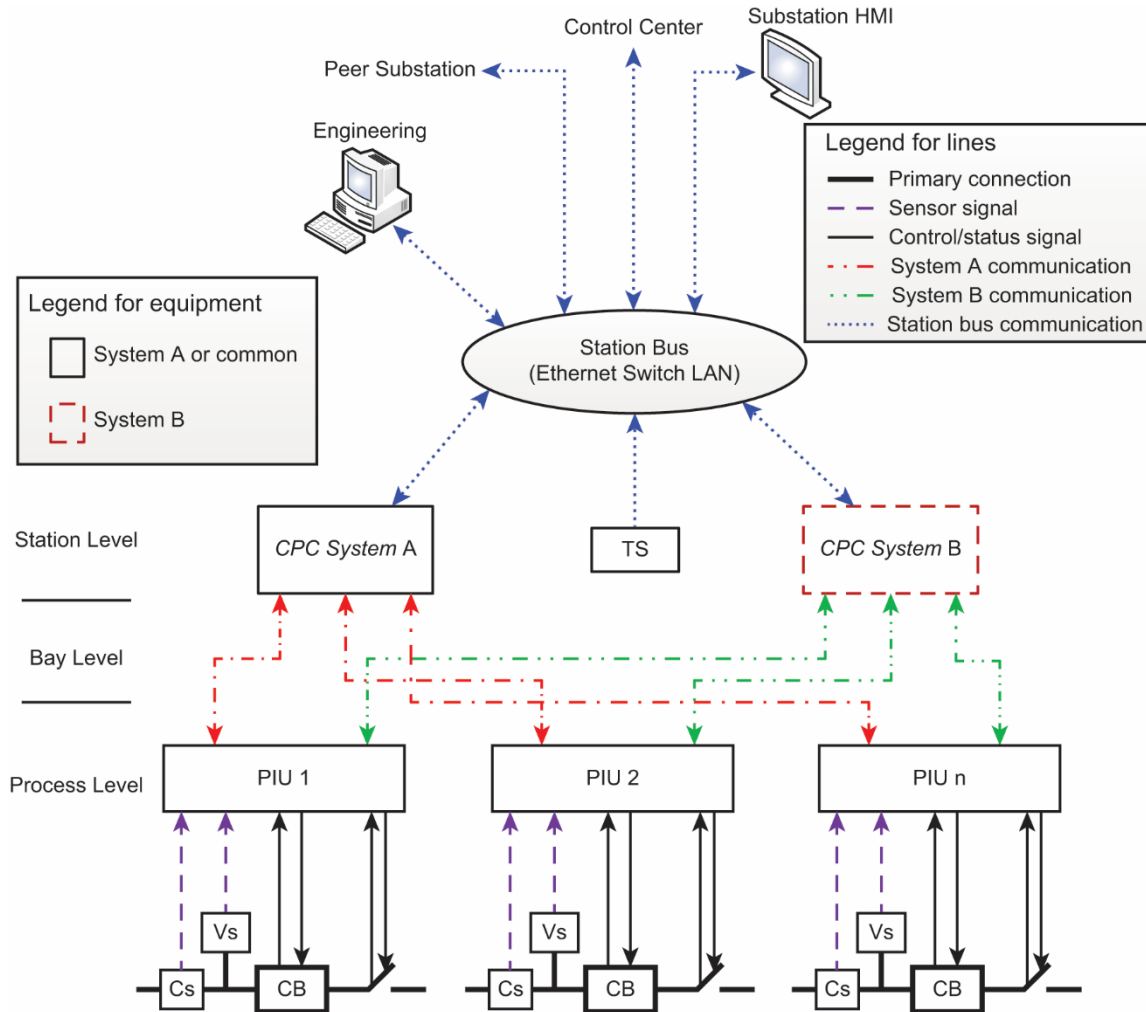


Figure 6—Type 3 architecture

5.2.4 Type 4

Figure 7 illustrates the Type 4 architecture that has an Ethernet communication network connecting the PIUs at the process bus level. In this architecture, PIUs at the process level may be interfaced with IEDs and the *CPC system* using a process bus. The same PIU broadcasts data to the IED and the *CPC system*, such as SV, and each IED and the *CPC system* can interface with each PIU independently to publish and to subscribe messages, such as GOOSE. Individual IEDs may perform main per bay protection and control functions, and the *CPC system* may provide redundant protection and control functions and station level protection and control applications.

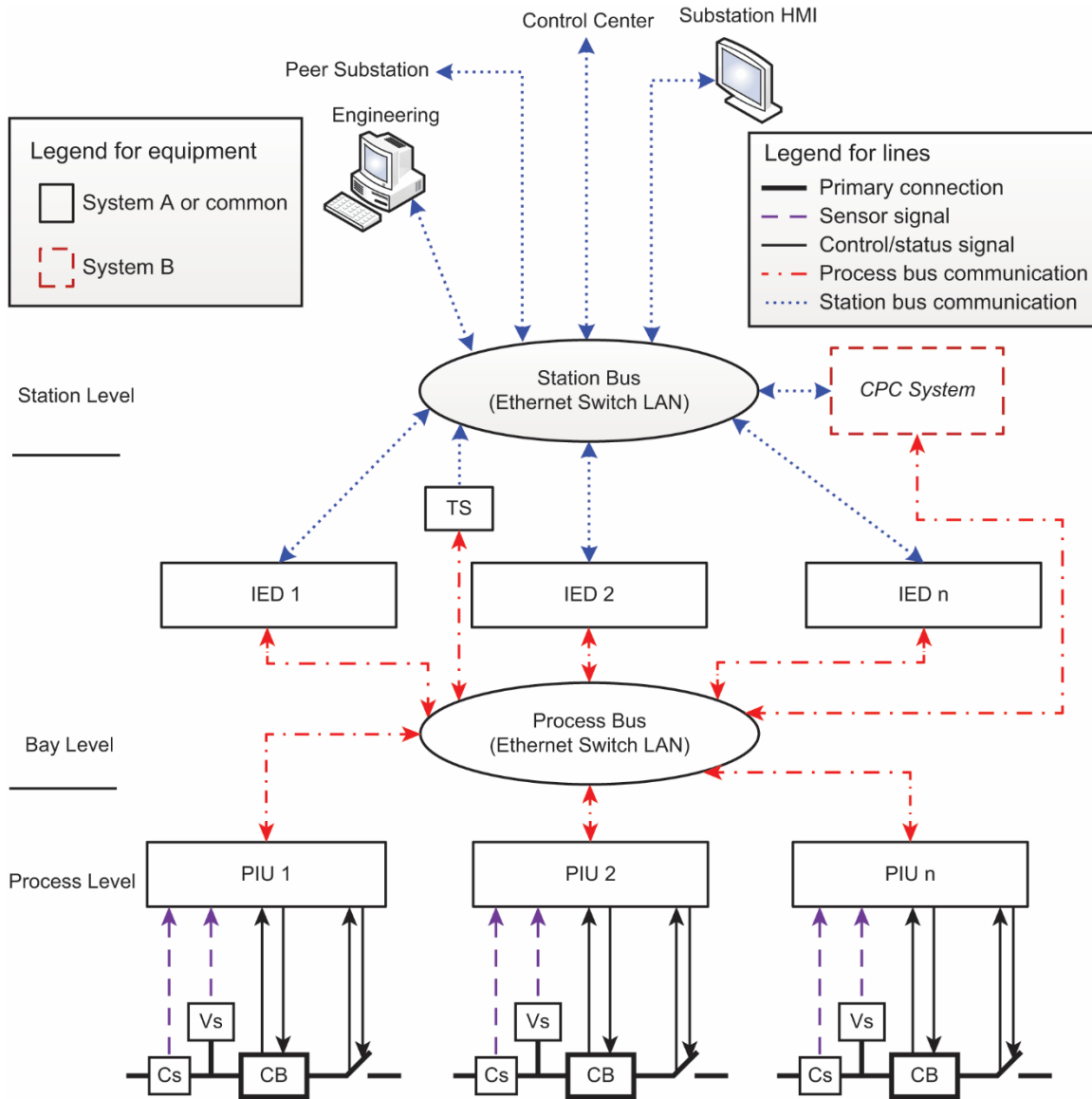


Figure 7—Type 4 architecture

5.2.5 Type 5

The Type 5 architecture, shown in Figure 8, illustrates the PIUs at the process level interfacing with the *CPC systems* over process bus. The same PIU broadcasts data to each *CPC system*, such as SV, and each *CPC system* can interface with each PIU independently to publish and to subscribe messages, such as GOOSE.

Since the *CPC systems* perform main and redundant protection and control functions, there can be more than two *CPC systems* at the station level to further enhance the reliability and availability of the entire system. PIUs at the process level are connected to the *CPC systems* using process bus.

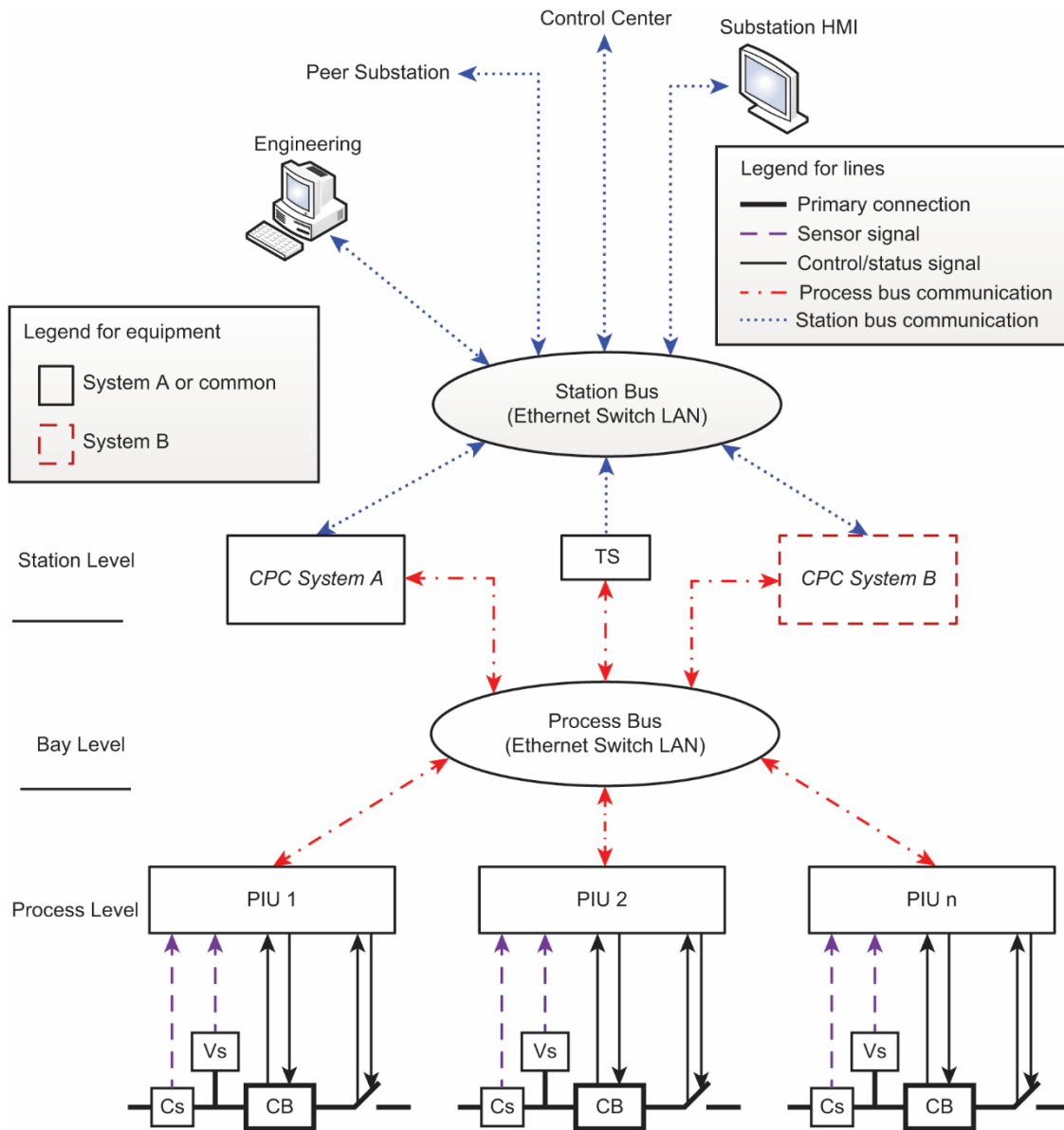


Figure 8—Type 5 architecture

5.2.6 Type 5a

Figure 9 illustrates Type 5a architecture with N-1 redundancy, to enhance the reliability of the substation protection and control system. Redundant Cs/Vs secondaries and I/O are connected to completely redundant (System-B) PIUs/CPC systems such as System-A and System-B.

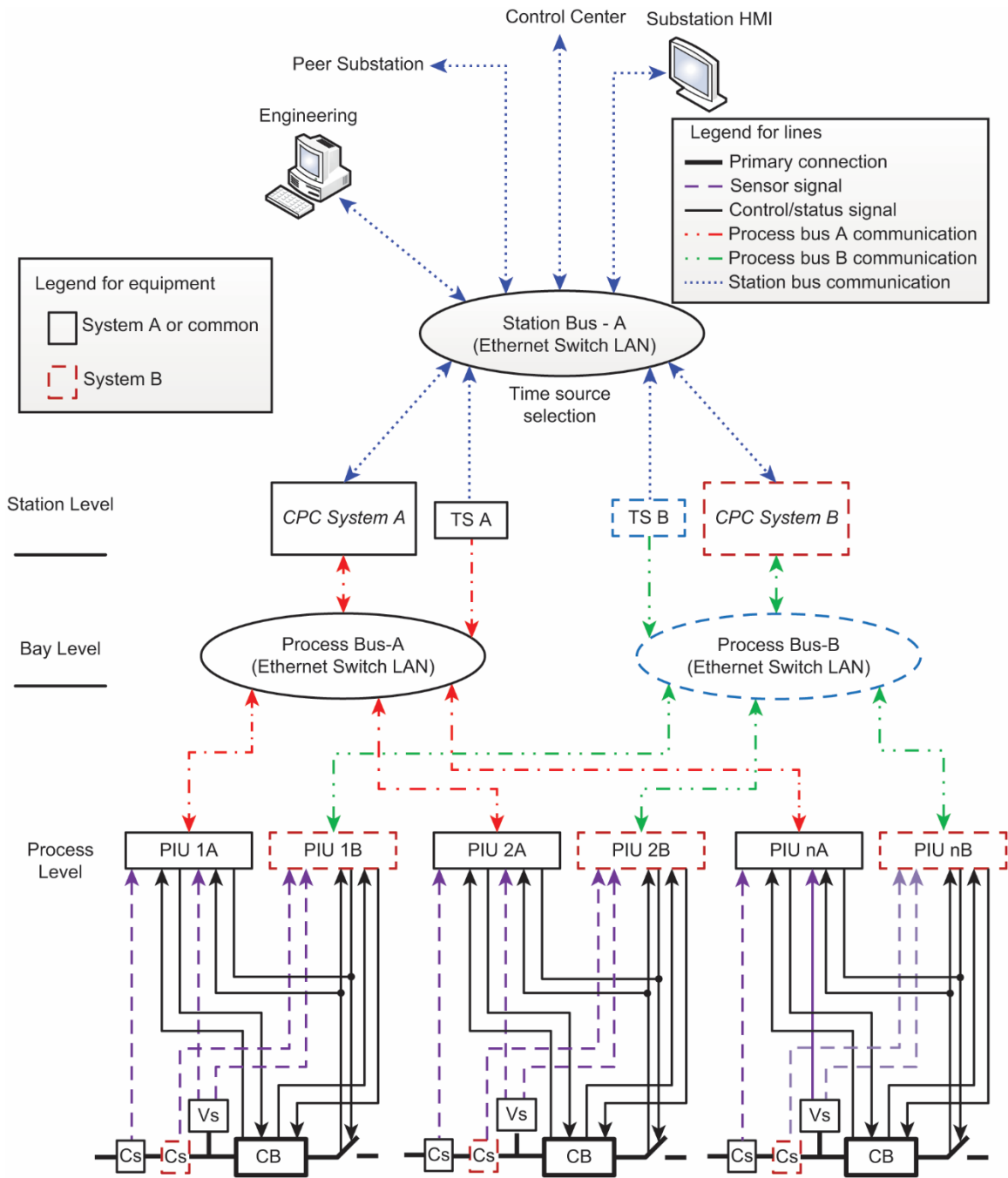


Figure 9—Type 5a architecture

5.2.7 Type 3a

Figure 10 shows Type 3a architecture with N-1 redundancy, which is derived from Type 3 architecture for comparison with the Type 5a architecture.

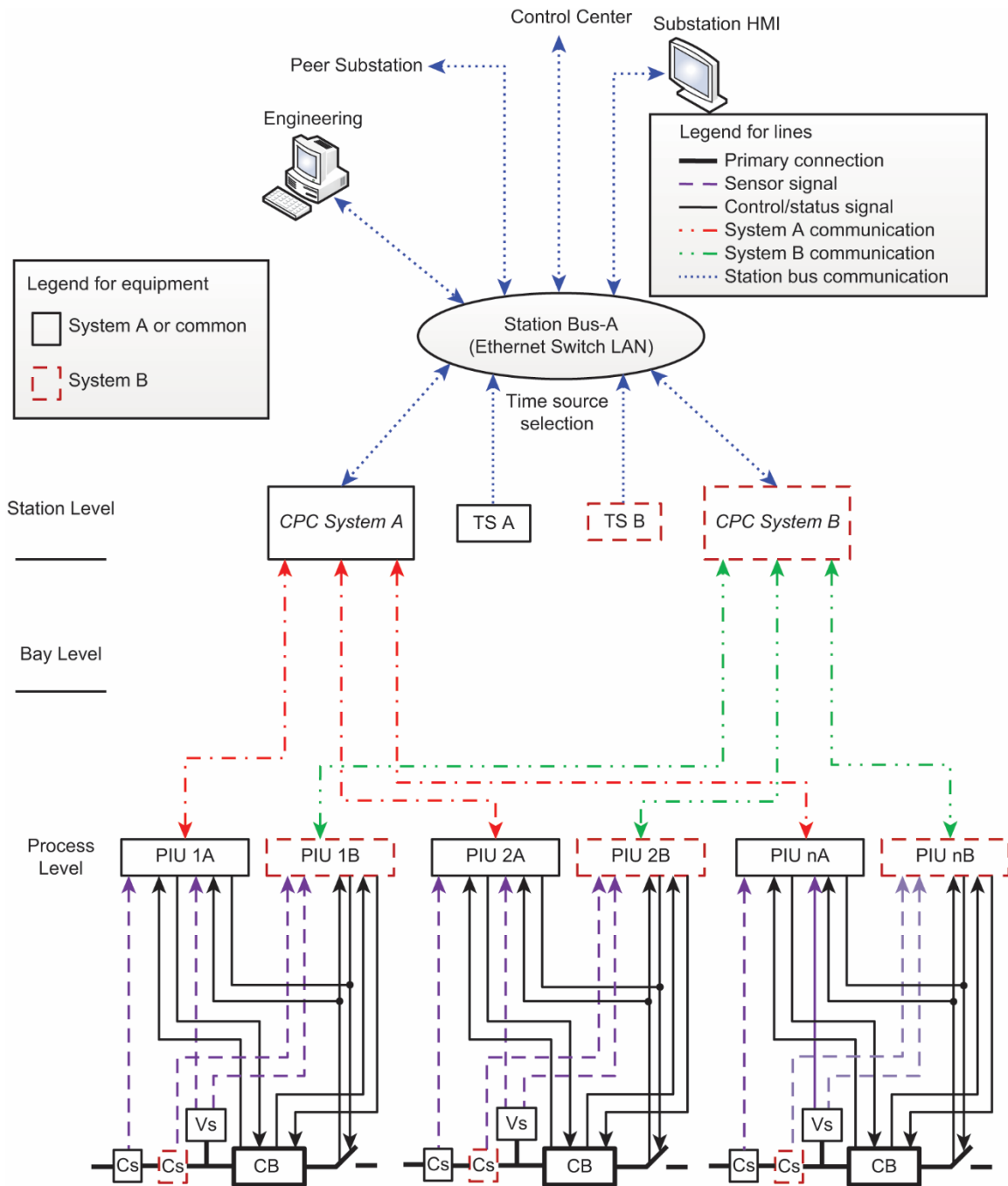


Figure 10—Type 3a architecture

5.3 CPC-based system design considerations

Considerations for the design of a *CPC-based system* are as follows:

- Reliability and availability
- Maintainability

- Scalability and flexibility
- Interoperability
- Testability

5.3.1 Reliability and availability

Reliability is the probability of a device (or system, in the context of this guide) performing its purpose adequately for the period of time intended under the operating conditions encountered. Reliability breaks down into four basic parts—probability, adequate performance, time, and operating conditions. Probability provides the numerical input for the assessment of reliability and also the first index of system adequacy. In many instances, it is the most significant index, but many more parameters are calculated and used, depending on the system and its requirements. These parameters are generally all termed *reliability indices*, and the term *reliability* is frequently used as a generic term describing all these indices rather than being solely associated with the term probability (Billiton and Allan [B150]).

Bauer [B21] defines failure as “the inability of a system or component to perform its required functions within specified performance requirements.” MTTF is the mean time to failure of the system or loss of service. Bauer [B21] defines availability as “the degree to which a system or component is operational and accessible when required for use.” A simple mathematical formula to compute availability is as follows:

$$\text{Availability} = \text{Uptime} / (\text{Uptime} + \text{Downtime})$$

Reliability index is more suitable for non-repairable systems, while reliability and availability indices are appropriate for repairable systems, such as *CPC-based systems*. Reliability of different *CPC-based system* architectures can be represented by the mean time to failure (MTTF) of the constituent systems represented at the system level, while hardware and software-related failures of constituent systems are not evaluated separately. Mean time to first failure is critical to demonstrate the reliability of the system. MTTF can be approximated as the mean time between failure (MTBF) for a repairable system, such as a *CPC-based system*, where the mean time to repair (MTTR) is significantly less compared to MTBF as shown in Figure 11 (Kasztenny et al. [B6] and Kanabar [B130]).

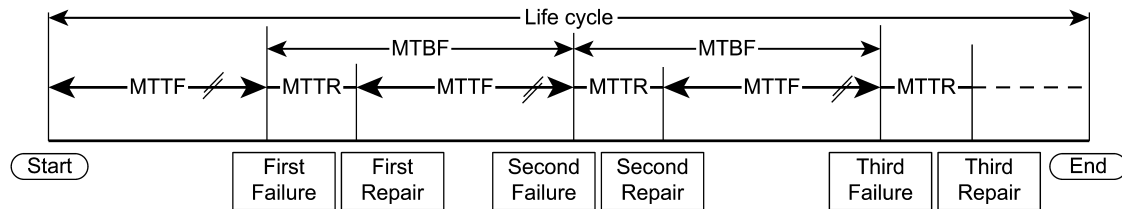


Figure 11—Life cycle of a *CPC-based system* showing the failure and repair relationship

For a *CPC-based system*, faults can be design weaknesses or vulnerabilities of internal components and external elements. Practical realities help to assure that no large and complex software product is ever completely free of residual software faults; defects are inevitable. Computer hardware components are vulnerable to physical phenomena that eventually cause them to fail (Bauer [B21]) or reach the end of their useful life. For mission-critical applications, end-users often evaluate and consider some type of redundancy, or an alternative system, to further reduce exposure to the failure of a system (Raheja and Gullo [B20]). Refer to 5.2 for reference architectures that address the redundancy of different approaches for *CPC-based system* configuration.

The IEC 61850-3 standard defines two reliability classes based on IEEE Std 1613 [B85] performance requirements and criteria. IEC 61850-8-1 [B37] specifies link redundancy as optional using IEC 62439-3

(PRP or HSR) or rapid spanning tree protocol (RSTP) while IEC 61850-9-2 also specifies link redundancy as optional using PRP or HSR. Therefore, the communication network redundancy is left to the substation design. It is important to analyze the reliability of *CPC-based system* architectures early in the design stage to select the right architecture to meet the availability requirement. The basics of reliability theory as applied for reliability analysis for *CPC-based system* architectures are discussed in Annex E.

The reliability (MTTF) and availability of *CPC-based system* architectures are evaluated and reported as examples in Annex E. The Reliability Block Diagram (RBD) technique, as in Annex E, is adopted to obtain the quantitative values of reliability (MTTF) and availability for the reference architectures.

Sample reliability (MTTF) and availability calculations for reference architectures are provided in Annex E with certain assumptions. End-users may use the information in Annex E for the computation of reliability (MTTF) and availability indices for various reference architectures or their variants for a given application to select the optimum architecture—noting that communication network design including the number, placement, and interconnection of switches as well as the use of redundancy schemes like HSR and PRP (including the connection with the *CPC system*), plays an important role on the reliability (MTTF) and availability indices and related economics of the solution selected.

5.3.2 Maintainability

The *CPC-based system* is designed for easy maintenance, including hardware and software upgrades for the *CPC system*. The different *CPC-based system* architectures discussed above provide the capability to replace a complete *CPC system*, including hardware and software upgrades, without any shutdown requirement of the system components. This aspect is one of the important features of a *CPC system* and may be included in all *CPC systems*. Built-in redundancy, to the extent of a complete *CPC system*, may be considered for each *CPC system* in various *CPC-based system* architectures discussed in 5.1 to accommodate for hardware failures and facilitate maintenance, including software upgrades, at a convenient time to avoid unscheduled maintenance (Gullo and Dixon [B127]).

5.3.3 Scalability and flexibility

Scalability refers to the extension of the capability of the *CPC system* such as accommodating more feeders than planned in a substation by upgrading system hardware, software, or both. Flexibility refers to the use of features available in a system based on changed system needs, such as the use of distance protection instead of directional protection. Many end-users consider the capacity of the *CPC system*, within a *CPC-based system*, to be expandable for immediate use and include provision for future expansions of the substation and life cycle planning while providing expected performance. Depending on the application, some end-users consider the ultimate station arrangement in support of scalability. Another key factor is that rapid technology changes, and associated interoperability, would lead to costly options if scalability is not considered to protect investment. Projected needs in a distant future involve considerable guesswork and may result in stranded investment, which can be avoided with a scalable *CPC system* design. An optimized *CPC system* capacity selection is helpful to avoid frequent upgrades, where incremental *CPC system* cost is outweighed by other costs associated with upgrades and related risks.

5.3.4 Interoperability

Any *CPC system* provided by one provider using IEC 61850-9-2 protocols is typically interoperable with such systems provided by other providers because data exchanges and coordinated operation are important between *CPC systems* within a substation or neighboring substations, depending on architecture and operation requirements such as for a differential protection application. In addition, each *CPC system* may be interoperable with PIUs from different providers supporting the IEC 61869-9 and IEC 61869-13 requirements.

5.3.5 Testability

The architecture of the *CPC-based system* could impact how the *CPC-based system* is tested. Similar to conventional systems, a *CPC-based system* has many components that may require testing through its operational life cycle. A *CPC-based system* may consist of one or more *CPC systems* that could allow for one to be taken out of service while the other is tested. This approach allows for verification of interfaces, permits testing of overlapping *CPC systems* interactions (if needed), and provides provisions for isolation of features or functions within each *CPC system* during testing.

It is important to consider the testability of a *CPC-based system* during architecting and different stages of engineering with user-desired test functionalities and test levels. A clear test plan document, including steps leading to the tests and steps to restore a *CPC-based system* to operation, is also an integral part of the system engineering and deployment steps (Gullo and Dixon [B127]).

It is also important to consider the self-diagnostics capability of a *CPC-based system* and the impact that self-monitoring has on the engineering design requirements. The self-diagnostics that impact the testing are typically reported before and after the *CPC-based system* is placed into service.

6. System engineering and implementation

6.1 General

The success of a *CPC-based system* implementation depends on system engineering to a large extent, as the components in a *CPC-based system*, including the *CPC system* work together even when provided by different vendors.

System engineering and the implementation of substations are discussed in the following standards, which may be useful while developing a *CPC-based system* specification:

- IEEE Std 1267-2019 [B81] discusses the development of specifications for turnkey substation projects.
- IEEE Std 1127-2013 [B80] discusses community acceptance and environmental compatibility in the design, construction, and operation of substations.

When an end-user wants to implement a *CPC-based system* using a turnkey process, then modifications to the specification as outlined in IEEE Std 1267 [B81] are expected, such as the following:

- Protection and control systems may be modified using information from this guide.
- Instrumentation and metering requirements may be replaced by the discussion of related *CPC-based system* requirements.
- The specification of SCADA/substation automation may be replaced by a discussion of related *CPC-based system* requirements.

A *CPC-based system* may not impact the community acceptance and applicable environmental compatibility as discussed in IEEE Std 1127 [B80].

Considerations may be given to the following aspects, as discussed in this guide, for a *CPC-based system* design, focusing on life cycle management: