



IEEE Recommended Practice for Network Communication in Electric Power Substations

IEEE Power and Energy Society

Developed by the
Power System Communications and Cybersecurity Committee

IEEE Std 1615™-2019
(Revision of IEEE Std 1615-2007)

STANDARDS



IEEE Recommended Practice for Network Communication in Electric Power Substations

Developed by the

Power System Communications and Cybersecurity Committee
of the
IEEE Power and Energy Society

Approved 5 September 2019

IEEE SA Standards Board

THIS IS A REDLINE DOCUMENT PRODUCED BY TECHSTREET, A BUSINESS OF CLARIVATE ANALYTICS

This document is intended to provide users with an indication of changes from one edition to the next. It includes a full-text version of the new document, plus an indication of changes from the previous version.

Redlines are designed to save time and improve efficiencies by using the latest software technology to find and highlight document changes. More professionals are using valuable new technologies like redlines, to help improve outcomes in a fast paced global business world.

Because it may not be technically possible to capture all changes accurately, it is recommended that users consult previous editions as appropriate. In all cases, only the current base version of this publication is to be considered the official document.

Redline Processing Notes:

1. ~~Red Text~~ - Red strikethrough text denotes deletions.
2. Blue Text - Blue underlined text denotes modifications and additions.

Abstract: Recommended practices for communication and interoperation of devices connected on an electric power substation Internet Protocol (IP) network are provided. An introduction to the concepts that need to be mastered as well as specific recommendations to follow when deploying the technologies are provided for the power engineer new to IP networking. Direction and requirements to facilitate interoperable electric utility information networks are provided for equipment manufacturers and system integrators.

Keywords: Distributed Network Protocol 3 (DNP3), Ethernet, fiber-optic, IEC 60870-5, IEC 61850, IEEE 1615™, intelligent electronic device (IED), Internet Protocol (IP), managed switch, network, network devices, noise sources, non-operational data, operational data, RS-232, RS-485, security awareness, Transmission Control Protocol (TCP), time synchronization, wireless network

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

Copyright © 2019 by The Institute of Electrical and Electronics Engineers, Inc.
All rights reserved. Published 8 November 2019. 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 978-1-5044-6137-5 STD23873
Print: ISBN 978-1-5044-6138-2 STDPD23873

IEEE prohibits discrimination, harassment, and bullying.

For more information, visit <http://www.ieee.org/web/aboutus/whatis/policies/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 documents are made available for use subject to important notices and legal disclaimers. These notices and disclaimers, or a reference to this page, appear in all standards and may be found under the heading “Important Notices and Disclaimers Concerning IEEE Standards Documents.” They can also be obtained on request from IEEE or viewed at <http://standards.ieee.org/IPR/disclaimers.html>.

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

IEEE Standards documents (standards, recommended practices, and guides), both full-use and trial-use, are developed within IEEE Societies and the Standards Coordinating Committees of the IEEE Standards Association (“IEEE SA”) Standards Board. IEEE (“the Institute”) develops its standards through a consensus development process, approved by the American National Standards Institute (“ANSI”), which brings together volunteers representing varied viewpoints and interests to achieve the final product. IEEE Standards are documents developed through scientific, academic, and industry-based technical working groups. Volunteers in IEEE working groups are not necessarily members of the Institute 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 Standards do not guarantee or ensure safety, security, health, or environmental protection, or ensure against interference with or from other devices or networks. 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.

IEEE does not warrant or represent the accuracy or content of the material contained in its standards, and expressly disclaims all warranties (express, implied and statutory) not included in this or any other document relating to the standard, including, but not limited to, the warranties of: merchantability; fitness for a particular purpose; non-infringement; and quality, accuracy, effectiveness, currency, or completeness of material. In addition, IEEE disclaims any and all conditions relating to: results; and workmanlike effort. 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: PROCUREMENT OF 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 should be considered 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, or 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 his or her views should be considered the personal views of that individual rather than the formal position of IEEE.

Comments on standards

Comments for revision of IEEE Standards documents are welcome from any interested party, regardless of membership affiliation with IEEE. However, IEEE does not provide 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 revisions to an IEEE standard is welcome to join the relevant IEEE working group.

Comments on standards should be submitted to the following address:

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

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

Copyrights

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, IEEE does not waive any rights in copyright to the documents.

Photocopies

Subject to payment of the appropriate fee, 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. 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. A current 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 ten years. When a document is more than ten 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 at <http://ieeexplore.ieee.org/> or contact IEEE at the address listed previously. For more information about the IEEE SA or IEEE's standards development process, visit the IEEE SA Website at <http://standards.ieee.org>.

Errata

Errata, if any, for all IEEE standards can be accessed on the IEEE SA Website at the following URL: <http://standards.ieee.org/findstds/errata/index.html>. Users are encouraged to check this URL for errata periodically.

Patents

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 <http://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.

Participants

At the time this draft recommended practice was completed, the Network Communications in Substations 1615 Working Group had the following membership:

Kevin Easley, Chair
Craig Preuss, Vice Chair
Ed Cenzon, Co-Secretary
Michael Dood, Co-Secretary

Farel Becker
James Bougie

Chris Huntley
Marc Laroix

Silvio Roesler
Eric Thibodeau

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

William Ackerman
David Aho
Ali Al Awazi
Jay Anderson
Philip Beaumont
James Bougie
Derek Brown
Gustavo Brunello
William Byrd
James Cain
Paul Cardinal
Yessenia Cevallos
Christopher Chelmecki
Randall Crellin
Ratan Das
Matthew Davis
Michael Dood
Kevin Easley
Ronald Farquharson
Kenneth Fodero
Mietek Glinkowski
Jalal Gohari
Edwin Goodwin
Randall Groves
David Haynes
Roger Hedding
Marco Hernandez
Werner Hoelzl
Gary Hoffman
Chris Huntley
Richard Jackson
Innocent Kamwa

Efthymios Karabetsos
George Karady
Stuart Kerry
Yuri Khersonsky
James Kinney
Boris Kogan
Bruce Kraemer
Jim Kulchisky
Chung-Yiu Lam
Lawrenc Long
Elvis Maculuba
Arturo Maldonado
Pierre Martin
John McDonald
C. Michael Miller
Jeff Mizener
Jerry Murphy
R. Murphy
Bruce Muschlitz
Arthur Neubauer
Michael Newman
Paul Nikolich
Joe Nims
James O'Brien
Lorraine Padden
Richard Paes
Bansi Patel
Charles Pestell
Percy Pool
Charles Rogers
Benjamin Rolfe
Thomas Rozek
Daniel Sabin

Miriam Sanders
Steven Sano
Bartien Sayogo
Robert Seitz
Devki Sharma
Mark Simon
Veselin Skendzic
Jeremy Smith
Jerry Smith
Michael Smith
Gary Smullin
Yuyin Song
Robert Stagg
Thomas Starai
Wayne Stec
Ryan Stone
David Tepen
Eric Thibodeau
Michael Thompson
Mark-Rene Uchida
Joe Uchiyama
James Van De Ligt
Roger Verdolin
John Vergis
James Volk
Khurram Waheed
Andrew West
Kenneth White
Aaron Wilson
Robert Wilson
Jian Yu
Oren Yuen

When the IEEE SA Standards Board approved this recommended practice on 5 September 2019, it had the following membership:

Gary Hoffman, *Chair*
Ted Burse, *Vice Chair*
Jean-Philippe Faure, *Past Chair*
Konstantinos Karachalios, *Secretary*

Masayuki Ariyoshi
Stephen D. Dukes
J. Travis Griffith
Guido Hiertz
Christel Hunter
Thomas Koshy
Joseph L. Koepfinger*
John D. Kulick

David J. Law
Joseph Levy
Howard Li
Xiaohui Liu
Kevin Lu
Daleep Mohla
Andrew Myles

Annette D. Reilly
Dorothy Stanley
Sha Wei
Phil Wennblom
Philip Winston
Howard Wolfman
Feng Wu
Jingyi Zhou

*Member Emeritus

Introduction

This introduction is not part of IEEE Std 1615-2019, IEEE Recommended Practice for Network Communication in Electric Power Substations.

IEEE Recommended Practice for Network Communication in Electric Power Substations was first published in 2007. Much of the guidance in the 2007 version of this document remains important and necessary in continuing to support legacy equipment.

There has been a dramatic change in the networking technologies since 2007. Security requirements and tools to address them have impacted design philosophies. Technical requirements unique to power industry applications previously precluded certain uses of Ethernet and TCP/IP (Transport Control Protocol/Internet Protocol), and these are being resolved through the creation of other standards.

Many new applications have created the need for higher bandwidth to support real-time operational awareness and to make this data available to many users beyond the traditional “system operators”. These include higher power system load factors, the introduction of distributed and variable generation, and the use of synchrophasors to support various power system applications.

Historically, serial connectivity (e.g., TIA-232-F) and protocols based on serial technology have dominated substation communications. Serial communication was taken to be inherently secure, both through limited physical accessibility and through obscurity of proprietary protocols. Substation inputs and control signals have been wired directly to protective relays, remote terminal units (RTUs), and recording/metering equipment.

The ability of Ethernet and TCP/IP to serve the large set of needs of the industry securely, reliably, and economically alters the landscape of electric utility communications. DNP3 IP is ubiquitous, and IEC 61850 (International Electrotechnical Commission) is designed as a network suite of functions. Historically, protective relays have been selected by power-system engineers without regard for network or protocol support, and communications have been accomplished using whatever adapters and converters were required. Now, although the protective functionality obviously remains paramount, lack of necessary network functionality may be used to disqualify equipment.

Contents

1. Overview	11
1.1 Scope	11
1.2 Purpose	11
1.3 Preface	11
1.4 Design philosophy	12
1.5 Factors in network design	12
2. Normative references	14
3. Acronyms and abbreviations	15
4. Electric utility information and communications technology (ICT)	17
4.1 Serial communication architecture	19
4.2 Ethernet network communication architecture	21
4.3 Other network technologies	24
4.4 Interfacing serial equipment to an Ethernet-based network	24
4.5 Moving from a serial system to an Ethernet-based architecture	26
4.6 Recommendations for utility networks	29
5. Data flows on Ethernet networks	29
5.1 Data flows	29
5.2 Characterization of data flows	32
6. Security issues and recommendations	34
6.1 Threats	35
6.2 Targets of attack	35
6.3 Cyber-attack techniques	35
6.4 Recommendations and techniques to address threats in a utility information system	36
7. Recommendations for Ethernet-based networks	39
7.1 Media	41
7.2 Reliability	43
8. Substation network design	44
8.1 Selection of communication architecture	44
8.2 Functional requirements	49
9. Interface and processing	51
9.1 Communication interfaces	51
10. Testing	53
10.1 Test planning	53
10.2 Testing plan framework	54
10.3 Testing	55
Annex A (informative) Security issues and awareness	60
A.1 Source of threats to the electric power system	60
A.2 Targets of attack in the electric utility network	61
A.3 Common cyber-attack techniques	63
A.4 Techniques to address threats to the electric utility network	66

Annex B (informative) Protocols used in and to substations.....	73
B.1 Services supported by the Internet Protocol Suite (IPS).....	73
B.2 Name-to-address mapping using DNS.....	73
B.3 Managed host configuration using Dynamic Host Configuration Protocol (DHCP).....	73
B.4 Bootstrapping an IP address using Bootstrap Protocol (BOOTP).....	73
B.5 Network management using Simple Network Management Protocol (SNMP).....	73
B.6 Time synchronization using Network Time Protocol (NTP)/IEEE Std 1588	74
B.7 Remote terminals using secure shell (SSH)/Telnet.....	74
B.8 IED access using Hypertext Transfer Protocol (HTTP)/HTTPS	75
B.9 File transfer using File Transfer Protocol (FTP)/Secure File Transfer Protocol (SFTP)	76
B.10 Rapid Spanning Tree Protocol (RSTP).....	77
B.11 High-availability Seamless Redundancy/Parallel Redundancy Protocol (HSR/PRP).....	77
B.12 IEEE 1815 (DNP3)	79
B.13 Protocol features	81
B.14 IEC 60870-5.....	83
B.15 IEC 61850	86
Annex C (informative) Internet Protocol Suite (IPS)	91
C.1 Introduction.....	91
C.2 IP layers	92
C.3 IP Addressing.....	95
C.4 IPv6.....	104
Annex D (informative) Interconnection diagrams for communications to and within substations	106
D.1 Single master station.....	106
D.2 Multiple master stations.....	107
D.3 Multiple master stations, multiple RTUs	108
D.4 Combination systems.....	109
D.5 Substation gateway connections (legacy to standard protocols).....	110
D.6 Networked systems	111
D.7 Network physical topologies	112
Annex E (informative) Serial communication channel analysis.....	116
E.1 Introduction.....	116
E.2 Specify the performance of a master station to RTU communication channel	116
E.3 Channel performance analysis procedure.....	117
E.4 Illustrative example	117
Annex F (informative) Protocol models.....	119
F.1 Master slave.....	119
F.2 Client-server model	121
F.3 Peer-to-peer networks.....	122
Annex G (informative) Network management.....	123
G.1 Configuring network settings in IEDs	123
G.2 Network management in the electric utility information system	124
G.3 Tools	124
Annex H (informative) Features of devices and media supporting Ethernet-based networks.....	128
H.1 General device features.....	128
H.2 Media features	131
H.3 Network devices	133
Annex I (informative) Bibliography.....	136

IEEE Recommended Practice for

Network Communication in Electric

Power Substations

1. Overview

1.1 Scope

This document defines a recommended practice for the design, testing, communication and operation ~~interoperation~~ of communications networks within, to, and from ~~devices connected on an~~ electric power substations. Security considerations are included in the above. ~~substation-Internet protocol (IP) network~~. It does not establish a new underlying communications standard. Instead, this ~~the~~ document presents guidelines and best practices for designing these communication networks ~~prescribes a specific set of existing conventions and definitions~~.

1.2 Purpose

This recommended practice provides direction for implementers who wish to produce interoperable and secure communications ~~equipment~~ for an electric power substation network. It also provides direction ~~criteria~~ for users, system integrators, and equipment manufacturers who need to establish requirements and design of communications networks within, to, and from ~~for~~ the electric power substation. This is meant to address both the physical and logical elements of the network ~~transfer of operational and non-operational data as well as configuration management~~.

1.3 Preface

Network communications is an important component of substation design because of the reliance of many utility applications on a variety of communication networks. This recommended practice recommends proven methods to specify network requirements, specify network schema, design network schema, and mitigate hazards and threats to networks in electric utility substations, while controlling the cost of the network and maintenance of the network. It is impossible for this recommended practice to be inclusive of all types of communication networks and protocols that could exist inside of substations. For example, advanced metering infrastructure (AMI) equipment may be installed inside substations, provide no interaction with the substation local area network (LAN), and be independently connected to the wide area network (WAN). So while impossible to cover every possible technology and protocol, there are many common technologies typical to many substations.

Ethernet and the Transmission Control Protocol/Internet Protocol (TCP/IP) are by far the dominant technologies in office and home use. The cost-effectiveness of IP over Ethernet, including factors of reliability, equipment availability, equipment costs, skilled labor available, and others, have made IP over Ethernet an obvious consideration for substation use.

In fact, IP over Ethernet is widely used in modern substation design, and has been shown to meet the needs very well-presuming proper design and implementation. Unfortunately, the ease of plugging some intelligent electronic devices (IEDs) into a router/switch combination, and plugging the router into a modem provided by an Internet service provider (ISP), may lead to such deployment in a substation environment without proper design and/or implementation.

Since an ad hoc network can quickly provide a high level of verifiable functionality, it can easily allow many important design requirements to be overlooked, such as those presented in this recommended practice. Some of these may be identified with minimal understanding or research, but many are more subtle and their importance may not be discovered until unreliable communications are observed, a power system disturbance occurs (such as those described in IEEE Std 1613) and causes the failure of communication equipment and its supported communications, simple IED and/or equipment failure occurs due to improper temperature ratings or clogged fans, or a breach of security occurs.¹

The use of IP over Ethernet is not presumed in this recommended practice. However, most of the principles here apply to any network technology, and are generally stated here in IP over Ethernet terms.

1.4 Design philosophy

Many decisions in network design are dependent upon the importance of the substation and the types and volume of data. A very robust, high-speed network could be designed and deployed at all substations. However, as cost is always a matter in proper utility operations, it is acknowledged that not all substations warrant the expense. Regardless, there are minimum practices necessary for diligent design of any network. Understanding the level of network performance required and elements for achieving the requirements are provided in this section. There are cost breakpoints in designing a network. In general, it is not possible to spend 10% more for a 10% “better” network. This and the cost of applying a high level of design effort to each substation leads to the common practice of designing two to four “classes” of network, and then evaluating for each new substation which class to employ.

¹Information on references can be found in Clause 2.

Historically, most substation IEDs were chosen using evaluation criteria that took precedence over communications capabilities. Relays were selected based on performance, function, and capability in their primary (protective) role. Meters were primarily selected based upon metering functions and displays. Frequently, communication capabilities were not included or not significantly weighted in the evaluation process. The result is that these substations have one or more IEDs that lack the interface (physical or protocol) preferred by communication engineers. These devices can still be placed on a network by using an intermediate device performing required media and protocol conversions.

1.5 Factors in network design

Factors in network design are as follows:

a) Cost of initial development

1) Equipment

2) Design

3) Labor

b) Continuing costs

1) Replacement of failed equipment

2) Labor

3) Recordkeeping

c) Risk of loss of data from substation (value of data)

d) Risk of loss of control to substation (value of control)

e) Risk of stolen data for profit

f) Risk of damage due to attack

- 1) External, terrorist
 - 2) External, mischief
 - 3) Internal, disgruntled employee
- g) Scope of possible damage
- 1) Single substation or part of substation
 - 2) System wide
- h) Methods of attack
- 1) Physical access to equipment
 - 2) Electrical or communications to equipment:
 - i) Wired
 - ii) Wireless
- i) Network equipment
- 1) Managed and unmanaged switches
 - 2) Media converters, modems, transceivers, etc.
- j) Media:
- 1) Copper wired cables
 - 2) Optical fiber cables
 - 3) Wireless
 - 4) Ancillary equipment such as cable trays, conduits, fiber distribution panels, patch panels, terminations, etc.

k) Legacy equipment/systems:

- 1) Serial, TIA-232-F (commonly known as RS-232)
- 2) Serial, TIA-485-A/TIA-422-B (commonly known as RS-485/RS-422)
- 3) Modems
- 4) MARS radio
- 5) Transducers

2. Normative references

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

IEEE Std [487.1™-2014](#) ~~1590™-2003~~, IEEE [Standard](#) ~~Recommended Practice~~ for the Electrical Protection of ~~Optical Fiber~~ Communication Facilities Serving ~~Electric~~ ~~, or Connected to, Electrical~~ Supply Locations [Through the Use of On-Grid Isolation Equipment](#). ^{1,2,3}

[IEEE Std 525™, IEEE Guide for the Design and Installation of Cable Systems in Substations.](#)

IEEE Std 802.1D™-2004 [\(Reaff 2011\)](#), IEEE Standard for Local and metropolitan area networks: Media Access Control (MAC) Bridges.

²The IEEE standards or products referred to in ~~this~~ Clause [2](#) are trademarks [owned by](#) ~~of~~ the Institute of Electrical and Electronics Engineers, [Incorporated](#) ~~, Inc.~~

³¹IEEE publications are available from the Institute of Electrical and Electronics Engineers ~~, 445 Hoes Lane, Piscataway, NJ 08854, USA~~ (<http://standards.ieee.org/>).

IEEE Std 802.1Q™-~~2018~~ ~~2005~~, IEEE Standard for Local and Metropolitan Area Networks—Virtual Bridged Local Area Networks.

[IEEE Std 802.3™-2018, IEEE Standard for Ethernet.](#)

IEEE Std 1613™ ~~2003~~, IEEE Standard Environmental and Testing Requirements for Communications Networking Devices in Electric Power Substations.

IEEE Std 1646™-~~2004~~, IEEE Standard Communication Delivery Time Performance Requirements for Electric Power Substation Automation.

[IEEE Std 2030™-2011 , IEEE Guide for Smart Grid Interoperability of Energy Technology and Information Technology Operation with the Electric Power System \(EPS\), End-Use Applications, and Loads.](#)

[TIA-232-F, Interface between Data Terminal Equipment and Data Circuit-Terminating Equipment Employing Serial Binary Data Interchange.⁴](#)

[TIA-334-C, Signal Quality at Interface between Data Terminal Equipment and Synchronous Data Circuit-Terminating Equipment for Serial Data Transmission.](#)

[TIA-404-B, Standard for Start-Stop Signal Quality for Non-Synchronous Data Terminal Equipment.](#)

[TIA-422-B, Electrical Characteristics of Balanced Voltage Digital Interface Circuits.](#)

[TIA-485-A, Electrical Characteristics of Generators and Receivers for Use in Balanced Digital Multipoint Systems.](#)

[TIA-530-A, High Speed 25 Position Interface for Data Terminal Equipment and Data Circuit-Terminating Equipment, Including Alternative 26-Position Connector.](#)

⁴[TIA publications are available from the Telecommunications Industry Association \(http://www.tiaonline.org/\).](http://www.tiaonline.org/)

~~IEEE Std C37.115™, IEEE Standard Test Method for Use in the Evaluation of Message Communications Between Intelligent Electronic Devices in an Integrated Substation Protection, Control, and Data Acquisition System.~~

3. Acronyms and abbreviations

For the purposes of this document, the following acronyms and abbreviations apply. The *IEEE Standards Dictionary Online* should be consulted for terms not defined in this clause.⁵

ACSI abstract communication service interface

AES advanced encryption standard

AMI advanced metering infrastructure

APCI Application Protocol Control Information

ARP Address Resolution Protocol

ASDU Application Service Data Unit

ASN.1 Abstract Syntax Notation One

ATM asynchronous transfer mode

BER bit error rate ~~basic encoding rules~~

BOOTP Bootstrap Protocol

CIP Critical Infrastructure Protection

COMTRADE common~~command~~ format for transient data exchange

CRC cyclic redundancy check

⁵ IEEE Standards Dictionary Online is available at: <http://dictionary.ieee.org>.

CSMA ~~carrier sense multiple access (Ethernet)~~

[DA](#) [distribution automation](#)

[DCE](#) [data circuit-terminating equipment](#)

DCS distributed control system

DES/3DES data encryption standard

DHCP Dynamic Host Configuration Protocol

~~DMD~~ ~~differential mode dispersion~~

DMS distribution management system

DNP/DNP3 Distributed Network Protocol, version 3.0

DNS domain name system

DoS denial of service

~~DTCC~~ ~~digital tap changer controller~~

EMI electromagnetic interference

EMS energy management system

[EPS](#) [electric power system](#)

FTP File Transfer Protocol

[GMS](#) [generation management system](#)

GOOSE generic object oriented substation event

GPR ground potential rise

GPS global positioning system

GSSE generic substation status event

GUI graphical user interface

[HDLC](#) [high-level data link control](#)

[HEMP](#) [high-altitude electromagnetic pulses](#)

HMI human-machine interface-

[HSR](#) [high availability seamless redundancy](#)

HTML hypertext markup language-

HTTP Hypertext Transfer Protocol

IANA Internet Assigned Numbers Authority

ICMP Internet Control Message Protocol

[ICT](#) [information and communications technology](#)

IDS intrusion detection system

IED intelligent electronic device

IETF Internet Engineering Task Force

~~IGMP~~ ~~Internet group management protocol~~

IP Internet Protocol

IPS Internet Protocol Suite

IPv6 Internet Protocol, version 6

~~IRIG~~ ~~inter range instrumentation group~~

ISO independent system operator ~~(or International Organization for Standardization)~~

[ISP](#) [Internet service provider](#)

IT information technology

LAN local area network

[LRU](#) [logical remote terminal unit](#)

~~LED~~ ~~light emitting diode~~

MAC media access control

~~Mb/s~~ ~~mega (10^6) bits per second~~

MIB management information base (SNMP)

MMS manufacturing message specification

[MTU](#) [maximum transmission unit](#)

NAT network address translation

[NERC](#) [North American Electric Reliability Corporation](#)

NTP Network Time Protocol

OID object identifier

~~QoS~~ ~~quality of service~~

OSI open systems interconnection

[PLC](#) [programmable logic controller](#)

PPP Point-To-Point Protocol

[PODIF](#) [Power Quality Data Interchange Format](#)

[PRP](#) [Parallel Redundancy Protocol](#)

PSTN public switched telephone network

[QoS](#) [quality of service](#)

[RC-4](#) [Rivest Cypher](#)

RCP remote copy

RFC request for comment document

RFI radio frequency interference

RMON remote traffic monitoring

[RS232](#) [Recommended standard 232, or TIA-232-F](#)

[RS485](#) [Recommended standard 485, or TIA-485-A](#)

RSA (Rivest, Shamir, Adelman) encryption algorithm

[RSTP](#) [Rapid Spanning Tree Protocol](#)

RTO regional transmission organizations

RTU remote terminal unit

SCADA supervisory control and data acquisition

SCL substation configuration language

SCP secure remote copy

[SDN](#) [software defined networking](#)

~~SCSM~~ ~~specific communication service mapping~~

~~SFP~~ ~~small form factor pluggable~~

SFTP Secure File Transfer Protocol

SGIRM Smart Grid Interoperability Reference Model

SNMP Simple Network Management Protocol

SNTP Simple Network Time Protocol

~~SONET~~ ~~synchronous optical network technologies~~

SPAN switched port analyzer

~~STP~~ ~~shielded twisted pair wire~~

SSH secure shell

SV sampled value

SWC surge withstand capability

SYN synchronize

TCP Transmission Control Protocol

Telco telecommunication service company

UART Universal Asynchronous Receiver/Transmitter

UDP User Datagram Protocol

UHF ultra high frequency

~~UTP~~ ~~unshielded twisted pair wire~~

VLAN virtual local area network

VPN virtual private network

WAN wide area network

4. Electric utility information and communications technology (ICT) ~~system architecture~~

Clause 4 first addresses the link between IEEE Std 2030-2011 and substation network design, and then answers the following two questions in broad terms:

- What is the justification for moving from a traditional serial-communication architecture to a network-based one?
- What is a general strategy for performing the upgrade?

In answering these questions, two technologies are considered for the upgrade, namely serial-to-network conversion equipment and the transition from analog to digital channels.

IEEE Std 2030-2011 provides a roadmap in establishing the Smart Grid Interoperability Reference Model (SGIRM). The SGIRM is a conceptual representation of smart grid infrastructure from three architectural perspectives: electric power systems (EPS), communications, and information technology. EPS integration with ICT achieves seamless operation of electric generation and delivery, while providing end-use benefits and permitting two-way power flow with communication and control. Reliability of the EPS is increasingly affected by the ICT infrastructure. Substation communication networks are actually network architectures supporting communications inside and to electric power substations, accounting for a small portion of the overall ICT. The safety and reliability of the EPS should prevail in the event of a disruption of the ICT infrastructure. This recommended practice addresses this goal through providing recommended practices for the design, installation, testing, and maintenance of the substation's portion of the overall ICT infrastructure.

IEEE Std 2030-2011 provides high level descriptions of the entities, or actors, that require communication channels to and within the substation and terminate at data acquisition/control equipment in the substation. Historically, there was only one actor with its own ICT [for example, a supervisory control and data acquisition (SCADA) master connection using only a 1200 baud or 9600 baud modem on a leased-line phone circuit]. Typically, actors were added with their own dedicated and independent ICT for each required communication channel, such as with the addition of protection relay communications, remote engineering access, metering, additional utilities, and other applications over time. Example actors are aligned with IEEE Std 2030-2011 and are discussed in more detail in Clause 5.

As the amount of data required by these different applications grows (data volume), the ICT may not be able to transport and process it in a timely fashion (information transfer time), without increasing bandwidth (data versus speed). As the distance grows between intelligent electronic devices (IEDs) using TIA-232-F technology, converting to other technologies that can support the distance is required [this may be a simple change to serial fiber technology or TIA-485-A, or a more complex conversion to Ethernet that may involve “serial/port/terminal servers” or true Ethernet between the devices, which may also need to address fiber for distance or electromagnetic interference (EMI) isolation]. A networked architecture for the ICT adds capabilities supporting improved reach (distance), information transfer time, latency, synchronicity, information reliability, data volume, and security (confidentiality, integrity, and availability), as well as scalability. Different communication architectures provide tradeoffs between these characteristics.

IEEE Std 1615 can be applied as follows:

- After the ICT evaluation has been accomplished as outlined in IEEE Std 2030-2011, meaning a communication architecture has been selected and will be applied to substations.
- During ICT evaluation of the classification of data flows as described in IEEE Std 2030-2011, meaning that a communication architecture has yet to be selected.

- Without applying the IEEE Std 2030-2011 SGIRM, which may be a situation where the utility has no overall strategic plans for an overall smart grid infrastructure and wants to start deploying networks in substations to support different applications as either the first deployment of substation communications or to upgrade from older serial technology that cannot support those applications.

The remainder of Clause 4 only applies when the latter two scenarios exist, because the remaining clauses describe the limitations and advantages of serial communication architectures, network communication architectures, and moving from a serial to network architecture.

~~An electric utility information system is defined for this recommended practice as a set of interrelated applications, data acquisition/control equipment, and communication channels designed to provide specific functions for the utility. Frequently, the overall information system is designed and controlled as separate subsystems, each with its own set of components. Examples include supervisory control and data acquisition (SCADA), energy/distribution management systems (EMS/DMS), protective relaying, equipment monitoring, power quality evaluation, and system planning and design. Regardless of the specific functions being performed or the level of integration between components, all of these subsystems can be viewed similarly with respect to the communication architecture. Each has data that needs to be transported, and equipment that needs to be configured and monitored. The data must also be processed.~~

~~An electric utility information system is an "overlay" technology in that its sole purpose is to improve the operation of another system—namely, the electric power system. The usefulness of the information system is always expressed in terms of the amount of efficiency that can be gained in the operation of this other system.~~

~~The usefulness of any information system depends on three factors (see Figure 1):~~

- ~~a) What information is available and how can it be used (data)~~
- ~~b) The timeliness of delivery and ability to react to changes (speed)~~
- ~~c) The maintenance and overhead required for upkeep and expansion (maintenance)~~

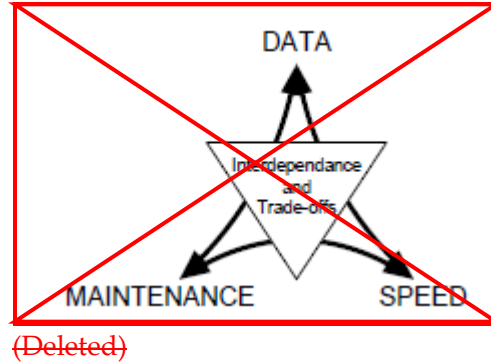


Figure 1—Information system usefulness factors

Each of these factors interact with the other two and inevitable tradeoffs are made based on cost and/or technology limitations. For example, as the amount of information that needs to be delivered grows, it may not be possible to transport and process it in a timely fashion (data versus speed). Simply adding wider communication channels and faster processors can drive up costs (speed versus maintenance). Moreover, as the database grows, the time to maintain the system also grows (data versus maintenance).

A networked architecture for an electric power information system adds capabilities to all three factors and mitigates some of the tradeoffs that have been present in traditional systems. However, new tradeoffs and techniques are present and should be considered in the design and upgrade of these systems.

4.1 ~~Traditional~~ Serial communication architecture

The historically dominant ~~electric power~~ serial communication architecture is illustrated in Figure 1 and 2. ~~The system~~ consists of equipment at one or more central locations (typically control centers), at substations, and along feeders. ~~Data users could be SCADA master stations, engineering workstations, planning, maintenance, protection, or other types of computers accessing data on demand.~~ This architecture has evolved over time to facilitate the interconnection of many different types of actors (such as SCADA master stations, remote access, planning, maintenance, protection, non-operational data, or other types of computers accessing data on demand) to IEDs ~~equipment~~ using many different serial protocols and channels. The serial channels to the substation are typically point-to-point (TIA-232-F) but can also be point-to-~~point and point-to~~-multipoint (TIA-485-A). One or more serial channels will terminate at the. ~~The remote terminal unit (RTU)/data concentrator function described by IEEE Std C37.2™ [B22], which~~ typically supports several serial ~~many~~ channels itself at a time and provides its collected data to each actor via a local I/O and protocol conversion. Separate dedicated channel.⁶ ~~or ad hoc channels are required for maintenance and non-operational data retrieval.~~

⁶The numbers in brackets correspond to those of the bibliography in Annex I.

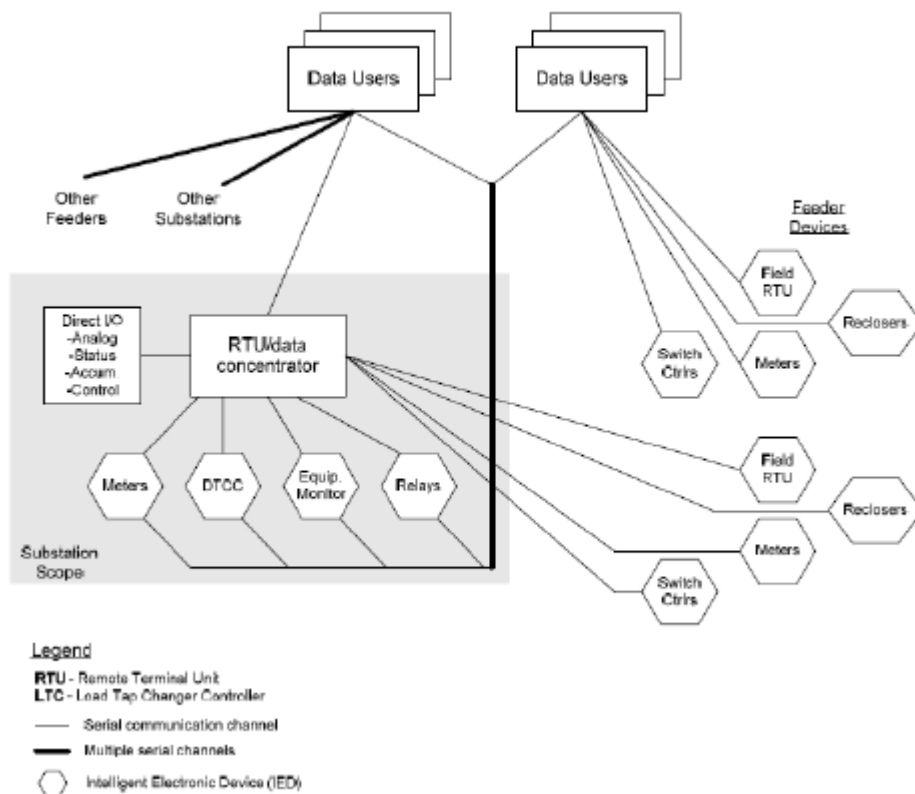


Figure 1—Traditional serial-communication architecture

[Table 1 describes characteristics that explain considerations necessary for traditional serial communications.](#)

Table 1—Serial Communication Architecture characteristics

Characteristic	Serial Communication Architecture
Reach (distance)	TIA-232-F is typically limited to distances of less than 30 m (100 ft), depending upon the selected baud rate and cable quality (lower capacitance is better), which can be extended using fiber optic transceivers or converting to TIA-485-A if this is too short for the application. With a distance limitation over 300 m (1,000 ft), TIA-485-A distance limitations are typically not relevant to most substations.
Information transfer time	Lower speed serial technology limits the data rate. The data occurrence interval and information transfer time (or data update rates) on serial are impacted by the number of IEDs sharing a single communication channel, the amount of data each IED is transmitting, and the processing time for the IED to decode the poll and assemble the response. As serial systems grow over time, it is common to accumulate many IEDs, both inside the substation and on feeders that connect to the serial system via a small number of external channels. Radio links and multipoint leased lines support the use of many devices in this fashion. However, the tradeoff is response time, as all master/slave protocols utilize the channel in a time-multiplexed manner. The available channel bandwidth for each IED is proportional to the inverse of the number of devices using the channel, so performance of the entire channel suffers as more and more IEDs are added to it. Inside a substation, serial channels are similarly limited as the number of IEDs connected to one channel increases. In addition, as point counts increase, this may also require the end device more time to assemble a response and require more time to transmit a complete response.
Latency (includes access, propagation, and reception delay)	Depending on the amount of data, number of devices on each serial channel, and the serial channel speed, data may not be obtained in the desired interval.
Synchronicity and determinism	Serial channel performance may be somewhat predictable, but likely not deterministic nor synchronistic.
Information reliability	Providing redundancy in serial systems requires careful design in order to get true redundancy, which will likely double the number of data concentrators and complicate the data collection and cabling design. Fiber optic transceivers can be used to provide the required isolation from the electromagnetic interference (EMI) environment described by IEEE Std 1613. Careful selection of communication cable may also be required for the application per IEEE Std 525.
Data volume	As systems get larger, and more IEDs are deployed, the sheer volume of point data that needs to move over the communication links increases. Also, serial channels are static and typically implement protocols that allow only communication where one device polls (the master) all of the others (the slaves) for data. It is often desirable to partition different types of data or data with different priorities into multiple logical channels in a communication architecture. Whereas SCADA protocols will generally allow multiple addresses on a serial channel, single serial channels do not allow multiple protocols. It is possible to interleave serial communications using proprietary methods to provide two channels of communication on a single serial port.
Security (confidentiality, integrity, and availability)	There is a general perception that serial communication is somehow secure and, therefore, does not require any, or limited security. Serial communications may, however, still be vulnerable to security concerns, including the interception of data streams that could allow serial messages to be modified, forged, reordered, or replayed. IEEE Std 1711™ [B19] discusses methods of securing serial communications. Security of serial communications may be cheaper and easier to obtain.

(New)

Characteristic	Serial Communication Architecture
Scalability	IED manufacturers provide information that frequently does not map into SCADA protocols or at least cannot be transported well between different protocols (e.g., event logs, oscillography files, power quality data, or non-operational data discussed in Clause 5). An engineer who wants to access this additional information must either go out to the remote site to access the IED or more serial communication channels that are dedicated for this purpose. As IEDs become more sophisticated and flexible supporting more data flows as discussed in Clause 5, they require more configuration. More often than not, this configuration is accomplished via a dedicated "maintenance port" on the IED with either a terminal program or proprietary software used to access the IED. Even a moderately sized system quickly accumulates dozens of configuration channels that must be planned, designed, tested, and managed. As pure serial systems expand, the number of IEDs required to collect the data scales linearly to some proportion of the IEDs. In addition, a relationship may need to be created to have a master data concentrator that collects data only from the data concentrators. For example, many data concentrators have only 16 "RS232" (TIA-232) serial ports, so as the number of IEDs expands, the number of data concentrators increases by one concentrator for every 16 IEDs. In this scenario, a substation of 80 IEDs requires a minimum of five data concentrators.

(New)

4.1.1 Limitations

The limitations of this communication architecture are:

- ~~—Speed and connectivity:~~ As systems get larger, and more intelligent electronic devices (IEDs) are deployed, the sheer volume of point data that needs to move over the communication links increases. Low speed modem technology limits the data rate and causes bottlenecks at the data concentrators and communication controllers. Also, the paths between devices are static and function in a master/slave mode. There is only one way to get data from a remote device and that may involve one or more intermediate devices to pass or translate the information.
- ~~—Logical channels:~~ It is often desirable to partition different types of data or data with different priority into multiple logical channels in a communication architecture. Whereas SCADA protocols will generally allow multiple addresses on a serial channel, they do not allow multiple protocols on a single channel.

- ~~– **New sources of data:** IED manufacturers provide information that frequently does not map into SCADA protocols or at least cannot be transported well between different protocols (e.g., event logs, oscillography files, power quality data, etc.). An engineer who would like to access this additional information must either go out to the remote site to access the IED, or install another communication circuit dedicated for this purpose.~~
- ~~– **Configuration management:** As IEDs and RTUs become more sophisticated and flexible, they require more configuration. More often than not, this configuration is accomplished via a dedicated “maintenance port” on the device with either a terminal program or unique software. Even a moderately sized system quickly accumulates dozens of configuration procedures that generally involve being at the physical location of the device.~~

4.1.2 Advantages

There are advantages to using serial [communication architectures as follows](#): ~~devices~~

- Some serial architectures [may be seen as](#) ~~are~~ more reliable, [more secure](#), and less expensive than networks. [Careful comparison is required, because it is easy to conclude that a small serial network using copper serial cables will be cheaper and more reliable than an Ethernet LAN using fiber cables and an improperly sized and specified Ethernet switch.](#)
- For small systems with small point counts, low-speed serial systems [for only SCADA channels](#) can still meet their intended functional requirements.
- ~~– It is possible to interleave serial communications to provide two channels of communication on a serial port.~~
- ~~– Security of serial communications may be cheaper and easier to obtain.~~
- Serial systems may also have a smaller impact on substation battery size due to smaller power requirements of port-powered devices.

4.2 Ethernet network Networked communication architecture

~~Figure 3 shows an alternative to the system described in 4.1 using a network as the communication infrastructure.~~

Figure 2 shows an Ethernet network architecture where ~~Notice that~~ all IEDs ~~devices~~ do not necessarily have to be on a ~~local-area-network (LAN)~~ to be accessible to the network. In Figure ~~2 3~~, the feeder communication circuits can use serial protocols that transport the network packets [e.g., Point-To-Point Protocol (PPP)]. The remote IEDs are allowed to be part of the network and therefore accessible by the data users.

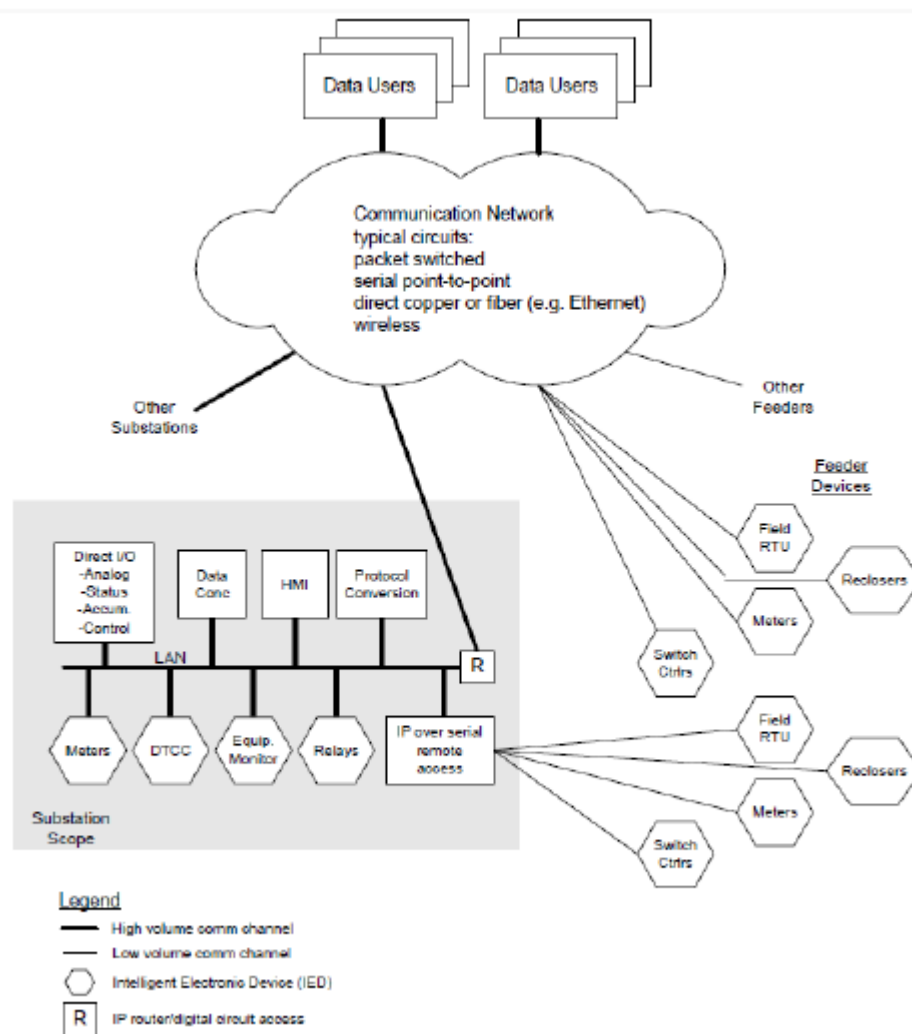


Figure 2 — Networked information system

Table 2 describes characteristics that explain considerations necessary for Ethernet communications.

Table 2—Ethernet Network Communication Architecture characteristics

Characteristic	Ethernet Network Communication Architecture
Reach (distance)	Ethernet network distances using copper cables span between TIA-232-F and TIA-485-A distances, but cannot reach TIA-485-A distances without conversion to optical fiber cable.
Information transfer time	Ethernet networks can deliver information transfer times to support IEC 61850 generic object oriented substation event (GOOSE) message performance requirements.
Latency (includes access, propagation, and reception delay)	
Synchronicity and determinism	Requires dedicated network queue allocations.
Information reliability	A network will typically allow more redundancy options that will leverage the network, both in physical connections (two Ethernet ports) and various versions of redundant operations. Just like serial systems, network redundancy results in more data concentrators, but depending upon capability there may only need to be two. Also, network redundancy may present somewhat simpler data collection and cabling design. Communication cables, especially copper Ethernet cables, need to be suitable for their installation environment. These cables also require separation from control cables in a cable tray and from fluorescent lights. Use of fiber optic transceivers can be used to provide the required isolation from the EMI environment described by IEEE Std 1613. See IEEE Std 525 for more information on the design recommendations. Adding the appropriate cable trays to support the required separation in existing substations may not be as straightforward and simple as it is a greenfield substation. The design of information technology (IT) networks is not the same as the design of critical operations networks that must be on 24×7×365. While many fundamental concepts overlap, the design of substation networks must be suitable for that environment, which is much different from a commercial building environment. Environmental conditions are also very different, such as temperature, humidity, and vibration, which are addressed in IEEE Std 1613 and IEEE Std 525.
Data volume	Ethernet LAN in a substation, along with a high-speed digital interconnection to the control center, greatly increases the available communication bandwidth. SCADA communication protocols typically consume little bandwidth on a 100 Mbps network. Networks can support multiple logical channels across multiple IEDs. Two IEDs on a network can be transferring data via one protocol while two other devices simultaneously transfer data via another protocol.
Security (confidentiality, integrity and availability)	Introducing networks into substations may require access control for substations, to better secure them in order to address new cybersecurity programs. Network cybersecurity is a significant issue. The risks should be completely identified and mitigated in order to adequately protect the substation IEDs and network from cyber-attack. See IEEE Std 1686™ [B18] for cybersecurity features that may be desirable. See Clause 6 for criteria to determine if the substation network is properly secured.

(New)

Characteristic	Ethernet Network Communication Architecture
Scalability	The network layer protocol provides a direct link to IEDs from anywhere on the network without worrying about what other protocols happen to be in operation on the same network. Depending on IED functionality, engineers could upload additional information from IEDs with minimal impact (assuming adequate bandwidth and device processing power) to other processes (e.g., SCADA) and without additional hardware. Each IED merely has to provide another protocol port number for those additional functions. The added bandwidth and multi-protocol capabilities of IEDs mean that a separate maintenance port may only be needed to initially configure the IED. After that, all configuration activities could take place over the network from a central location.

(New)

4.2.1 Improvements

A networked architecture improves on the limitations noted in 4.1.1 as follows:

- ~~— **Speed and connectivity:** An Ethernet LAN in a substation along with a high-speed digital interconnection to the control center greatly increases the available communication bandwidth. The network layer protocol provides a direct link to devices from anywhere on the network without worrying about what other SCADA protocols happen to be in operation on the same network.~~
- ~~— **Logical channels:** Network protocol stacks support multiple logical channels across multiple devices. Two devices on a network can be transferring data via one protocol while two other devices simultaneously transfer data via another protocol.~~
- ~~— **New sources of data:** Engineers can upload additional information from IEDs with minimal impact (assuming adequate bandwidth) to other processes (e.g., SCADA) and without additional hardware. Each IED merely has to provide another protocol port number for file or auxiliary data transfer.~~
- ~~— **Configuration management:** The added bandwidth and multi-protocol capabilities of modern network protocols mean that a separate maintenance port may only be needed to setup the initial parameters to get the device on the network. After that, all configuration activities can take place over the network from a central location. Other advanced features become possible such as auto-discovery of equipment and standardized configuration procedures.³~~

³ ~~The utility's testing and validation process may need to be harmonized with the "new" concept of off site configuration management.~~

4.2.2 Challenges

Adding [Ethernet](#) networks to substations can introduce the following significant challenges:

- Training [and organizational structure](#): Those who are familiar with [IT networks](#) ~~networking equipment~~ are generally not familiar with substations [or the “always on”, critical nature of control systems](#). Those who are familiar with substation [IEDs](#) ~~devices~~ may not be familiar with networking. In many cases, overlap does not exist, so training [the](#) ~~for~~ personnel on both sides is required, and some organizational realignment may be needed to bridge the gaps [prior to the start of design](#).
- ~~Access control: Introducing networks into substations may also lead to the application of information technology (IT) principles to a control system environment in the substation. User IDs, password management, and access management can become significant hurdles or result in serious problems. Passwords that must change periodically, lock-out access after login failures, or present other situations may impact the operational effectiveness of a substation network.~~
- ~~Cyber security: Network cyber security is a significant issue that may pose an unacceptable risk to those who believe it is impossible to adequately secure the substation network. While cyber security is a major concern, the risks should be completely identified and mitigated in order to adequately protect the substation network from cyber attack. See 6.2 for criteria to determine if the substation network is properly secured.~~
- Battery power: Networking devices can add substantial requirements to the substation battery. [For substation upgrades/retrofits](#), ~~resulting in~~ larger [batteries may be required](#) ~~battery sizes~~ to support the networking equipment during extended outages. Battery calculations should [always](#) be revisited during system design to [help](#) ensure the battery system will support [all IEDs in the substation automation System, including substation networking devices \(switches, routers, firewalls, serial servers, etc.\)](#) ~~networking devices~~.

4.3 Other network technologies

[Token Ring, Fieldbus, Modbus Plus, Profibus, and other technologies are also used in electric power substations. Many of the principles in this document are applicable across technologies, although other technologies may not support their implementation.](#)

4.4 Interfacing serial equipment to [an Ethernet-based](#) a network

Substation [IEDs](#) ~~devices~~ are frequently chosen using evaluation criteria that take precedence over communications capabilities. Relays are ~~primarily~~ selected based upon ~~protection~~, performance, function, and capability [in their primary \(protective\) role](#). Meters are primarily selected based upon metering functions and displays. Frequently, communication capabilities are not included or not significantly weighted in the evaluation process. The result is that the substation has one or more new or existing [IEDs](#) ~~devices~~ that have one or more serial interfaces with no network interface. These serial devices can still be placed on a network by using an intermediate device with both a network connection and serial connection.

[These intermediate devices can be classified into](#) ~~There are~~ two general classes of serial-to-network converters—those that are protocol-independent and those that are protocol-specific—~~(see Figure 4)~~. Each has its place in a modern electric power information system.

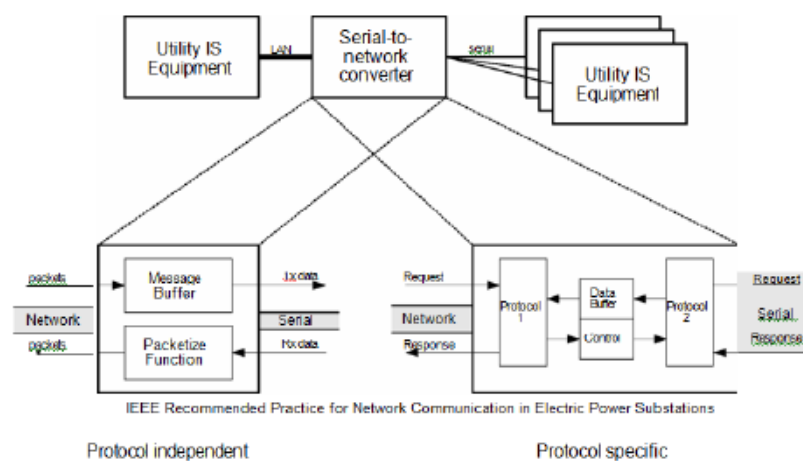


Figure 3— Serial-to-network converters

4.4.1 Protocol-independent converter

The protocol-independent converter is sometimes called a “terminal server” (also known as a “port server” or “serial server”) ~~in traditional information systems~~ and typically supports ~~up from 1~~ to 16 serial ports ~~but can be as high as 32 or even 48 ports~~. A terminal server ~~is~~ is used when both pieces of equipment to be interfaced understand the same protocol, and merely requires a physical conversion of network packets to/from a serial data stream. It is typically not protocol aware or does not understand the single protocol being used. ~~(usually RS232 or RS485).~~

4.4.2 Protocol-aware converter

When a serial server is protocol aware, that awareness is usually leveraged by the device to improve overall connectivity and functionality. For example, when using addressable protocols such as Modbus and Distributed Network Protocol, Version 3.0 (DNP3) (IEEE Std 1815), some serial servers will route messages from the network to a specific serial port based upon the address contained in the protocol. On the serial side, some of these devices will take a single serial message and send it to multiple IEDs on the network side.

A protocol-aware converter can be two types. In the first type, the converter is aware of simple protocol functionality and allows messages to be routed between the Ethernet network and serial ports and vice-versa, without protocol conversion (but perhaps protocol encapsulation).

The second type is a more complicated protocol-specific converter ~~is~~ used when two IEDs ~~pieces of equipment~~ cannot communicate because they use different protocols [i.e., one could be Modbus and the other DNP3 (IEEE Std 1815)]. This is a more sophisticated ~~device than the protocol-independent~~ converter because ~~in terms~~ of how each network's interface is handled and the amount of configuration required. Some converters ~~devices~~ translate requests and responses on protocol 1 directly to/from protocol 2. A prerequisite for this design is a one-to-one mapping between requests and data types of the two protocols. More often, the IED lets ~~devices let~~ both protocols run separately. Data and control are stored in a generic format, and converted by the protocols as appropriate. This type of design requires much more configuration information. This type of protocol-specific conversion is typically supported by a data concentrator, but can also be accomplished in a simpler protocol converter.

4.5 Moving from ~~to~~ a serial system to an Ethernet ~~network-based architecture~~ system

Moving from a serial communication architecture to an Ethernet-based network architecture could
~~The move to a network architecture should~~ be justified by one or more of the following needs:

- Ability to deploy and enable new technologies such as IEC 61850 communications [including GOOSE, manufacturing message specification (MMS), and Process Bus].
- Faster data update rates: Ethernet networks provide higher speeds that can support faster update rates than serial can support, typically independent of the number of IEDs on a substation LAN in comparison to the number of IEDs on a serial channel.
- ~~— **Better response time:** As systems grow over time, it is common to accumulate many devices, both at the substation and on feeders that connect to the information system via a small number of channels. Radio links and multipoint leased lines support the use of many devices in this fashion. However, the trade-off is response time as all master/slave protocols utilize the channel in a time-multiplexed manner. The available channel bandwidth for each device is proportional to the inverse of the number of devices, so performance of the entire channel suffers as more and more devices are added.~~

- Important and timely data access: If a utility requires the ability to analyze faults, ~~and~~ obtain other power quality related data, obtain other asset management related data, or obtain files that contain large amount of data, it will likely install IEDs that can provide this information. Depending on the importance that a utility places on this data or the time-critical nature of this data, this could be the sole justification for installing an Ethernet ~~a communication~~ network because too many low-speed serial connections. ~~All sophisticated system-level applications~~ are required using serial communications ~~dependent on the quality of the real power system inputs. Also, it may be necessary for engineers to retrieve data already in the system and correlate it with data that is only available in other formats from the IEDs.~~
- Reduction of configuration and system management time: Reconfiguration and maintenance of substation IEDs ~~devices in an electric utility information system~~ is an ongoing process. A common misconception is that access to the maintenance facilities of ~~RTUs, data concentrators, and~~ IEDs is only done at commissioning. In practice, there are a number of reasons to use the facilities on a more frequent basis, such as scheduled updates and system diagnostics. There can be reasons for access that are not just maintenance. For example, it may be desirable for operators or engineers to be able to dynamically change relay settings in response to an outage or seasonal loads. Remote access is supported by serial and Ethernet-based networks. Remote access can be used for more than maintenance activities, such as checking configurations, checking error logs or reports, checking device health, obtaining device reports, and obtaining files. While cybersecurity concerns exist with allowing remote access via either method, the benefits of reduced travel time for widely dispersed assets can be very tangible. As bandwidth increases with Ethernet-based networks, response times decrease and the amount of data that can be obtained increases over the same time interval when compared to serial systems.

- Ability to multiplex channels of information: ~~The Internet protocol suite (IPS) supports multiple channels allowing concurrent access to a device.~~ With serial non-routable serial communications, separate physical links may be ~~are~~ needed for SCADA, remote access, file retrieval, and to a substation human-machine interface (HMI). A vendor may be able to support one or two of these connections over one serial port with limited impact to either's performance. An Ethernet-based network supports multiple logical ports allowing concurrent access to an IED using a variety of protocols, provided the IED supports multiple concurrent connections. Many IEDs still have limited resources and therefore support a limited number of concurrent connections. For example, one IED may support up to five concurrent connections of any protocol combination, but only two instances of IEEE 1815 (DNP3) are supported. Another example may be an IED that supports only two concurrent IEEE 1815 (DNP3) connections and no other logical ports are used at all.

- Reduction of system expansion costs: Ethernet-based networks can also reduce overall system costs when compared with a serial system. While serial devices ~~may initially be~~ ~~are~~ ~~probably~~ cheaper, as system functionality increases along with the number of IEDs devices, serial systems require more connections that ~~may~~ ~~will~~ offset the additional costs of installing an Ethernet-based network depending upon system architecture and functionality Ethernet. Initial deployment costs ~~may linearly~~ ~~will~~ increase with serial systems as system functionality increases. Expansion of serial systems will most likely be more expensive because serial port densities are not as great as Ethernet port densities, and multiple serial ports are most likely required to support multiple functions. Both serial and Internet Protocol Suite (IPS) systems have scalability issues, but serial systems typically encounter these values at lower numbers of IEDs. Serial ports on data concentrators or RTUs are limited to some small number, typically 16, 32, or 48. Some of these connections may be a mix of single or multi-drop serial connections. For serial systems with larger device counts beyond what a single data concentrator can support, more data concentrators may be needed with master-slave relationships, and some vendors provide tools to make this process "easier". On Ethernet-based systems, typically one data concentrator can support up to 128 concurrent connections for polling IEDs on an Ethernet-based network. But in the end, Ethernet-based systems suffer from similar expansion problems as serial systems, but they typically occur at larger IED counts ~~when multiple functions are required~~.
- Ubiquity of Ethernet: Ethernet-based networks are ~~is~~ widely supported and understood in IT departments ~~and~~. A huge body of knowledge exists in the public domain for installation and deployment. These networks Ethernet can also be easily monitored and managed using tools that are standards-based, ~~e.g., simple network management protocol (SNMP)~~. Ethernet also supports a wide range of applications across the utility enterprise without requiring a different or separate network.

- Redundancy: There are many forms of redundancy that can be implemented in serial and Ethernet-based networks. Typically, redundant serial networks are more difficult to implement and more complex because of the singular nature of each connection to each IED. Ethernet-based networks may provide advanced redundancy features, not only for redundancy in the communication path to the IED, but also to provide a range of simple to robust failover schemes.

By comparing costs with benefits, a business case can develop the financial justification for migrating to Ethernet-based architectures. Some benefits may be easier to monetize, or easier to develop the cost savings.

4.5.1 Strategy for upgrading

As will always be the case, the primary needs of the particular system drive the upgrade strategy. A utility should use the process outlined in the SGIRM to develop an interoperable architecture that ensures the upgrade can support the data sources that can give the most important information. Upgrading from a serial communication architecture system to an Ethernet network architecture can be accomplished in two ways: top-down or bottom-up.

~~Upgrading from a traditional information system to a networked system can be accomplished in two ways: top-down or bottom-up.~~

4.5.1.1 Top-down approach

The following steps constitute a top-down approach~~constitutes the following steps:~~

- a) Upgrade communications to the substation from serial to Ethernet-based network and add a network interface to one or more substation IEDs. ~~the RTU/data concentrator~~
- b) Add an Ethernet-based ~~a~~ network within the substation that connects all IEDs by upgrading them to network connectivity or via serial servers.
- c) Upgrade communications to the feeder IEDs ~~devices~~ and make them network accessible using serial servers or upgrade them to network connectivity.

~~The top-down approach has the following advantages and disadvantages:~~

4.5.1.1.1 Advantages to top-down approach:

The top-down approach has the following advantages:

- Adds bandwidth where it is needed most, ~~the~~ the substation-to-utility ~~control center~~ communications. ~~load is the aggregate of that portion of the system~~
- Improves access to the RTU/data concentrator and, potentially, other IEDs.
- Allows replacing analog lines with more robust digital channels.
- May allow inclusion or consolidation of other communications services on a single communication channel (e.g., ~~service (for example,~~ phone, video surveillance, ~~etc).~~
- May provide options for redundant communications to the substation.
- May reduce communications costs, depending upon consolidation of analog circuits and digital circuit bandwidth.
- ~~— May allow replacing analog lines with more reliable digital channels~~
- ~~— May reduce wire line costs based on distance charges~~

4.5.1.1.2 Disadvantages to top-down approach:

The top-down approach has the following disadvantages:

- May significantly increase communication costs if bandwidth requirements remain low.
- Initially only allows access to the RTU/data concentrator; this IED ~~device~~ may not be the most important data source or the highest bandwidth consumer.
- Requires upgrading equipment at the control center.
- Forces additions to workforce skill sets.

4.5.1.2 Bottom-up approach

The bottom-up approach constitutes the following steps:

- a) Add a network within the substation and connect as many IEDs as possible to that network via direct connections or serial servers.
- b) Upgrade communications to the feeder IEDs ~~devices~~ and make them network accessible.
- c) Upgrade communications to the substation and add a network interface to the RTU/data concentrator if not already accomplished.

4.5.1.2.1 Advantages to bottom-up approach:

The bottom-up approach has the following advantages ~~and disadvantages~~:

- Most work can be limited to the substation with little effect on the SCADA master.
- Lower initial communication costs.

4.5.1.2.2 Disadvantages to bottom-up approach:

The bottom-up approach has the following disadvantages:

- Does not allow access to systems ~~system~~ outside of substations ~~substation~~ until later in the evolution.
- Does not improve ~~increase~~ response time from the control center.
- May require initial upgrade to networked IEDs or, depending on the protocol, the addition of a serial/port/terminal server. If this feature is not available from the current vendor, replacement costs are increased significantly.
- Forces additions to workforce skill sets

~~As will always be the case, the primary needs of the particular system drive the upgrade strategy. A utility should list the goals of the upgrade, focused primarily on which data sources can give the most important information. A comparison of these goals with the lists above should give an indication of which approach will best suit the situation.~~

4.5.2 Converting from analog leased to digital leased lines

Some utilities have relied on leased communication lines from a telecommunication service company (Telco) provider [for substation communications. There may be separate communication lines for SCADA, protection, remote access, metering, equipment monitoring, etc.](#) In many cases, the utilities did so with the belief that the line was dedicated, end-to-end, to the sole function of their use. These lines handled analog signals.

Analog lines are disappearing in the Telco world. A solid copper wire pair connecting two points disappeared years ago. The copper pair delivered to the utility is really just wires to the nearest Telco network center. From that point forward, the traffic on the wires becomes digital signals through the Telco network. The Telco performs the A-to-D and D-to-A conversion and reserves a packet connection for that traffic. So for all practical purposes, the connection is permanent and essentially [dedicated but not necessarily](#) private.

Telcos charge different rates for digital service. For the equivalent of an analog leased line, 56 [kbps](#) ~~kb/s~~, they charge a higher base rate; however, they charge only for the distance to the nearest Telco digital hub. Where the utility pays the end-to-end distance charges for an analog line, it will pay a lesser distance charge for digital [lines](#) ~~line~~, potentially saving the utility Telco charges. Note this assumes the utility has already installed any required Telco isolation equipment [as per IEEE Std 487.1™-2014](#). Should a line that is not equipped with isolation be converted, it loses its “grandfathered” status and would need to be equipped for isolation at utility expense.

It is possible for a utility to convert leased lines from analog to digital, decrease the combined basic and distance charge, and gain additional bandwidth. The additional bandwidth may permit added communications [connections for more than just SCADA or protection as previously discussed](#) ~~capability for network traffic~~.

4.6 Recommendations for utility networks

All electric utility networks should use the IPS for the transfer of operational and non-operational data as well as configuration management. In addition, the following are recommended:

- Each utility should develop a plan for private IP address allocation (see C.3 5.2.3).
- Private addressing should ~~shall~~ be employed on electric utility substation networks (see C.3 5.2.4).
- Substation information systems should not be connected to a public or utility-wide network unless the security measures discussed in Clause 6 are evaluated and put in place. ~~except through a properly configured router/firewall housed in a secure area.~~
- ~~— Link layer message exchange should be used for IEC 61850 Generic Object Oriented Substation Event (GOOSE) messages [B15] (Annex D).~~

5. Data flows on Ethernet networks

6. ~~Data classification and security for IPS networks~~

6.1 ~~Types and uses of data~~

As previously discussed, Ethernet ~~IPS~~ networks provide the capability of supplying multiple logical connections to one physical IED. Each one of these logical connections produces a data flow across the Ethernet network. According to IEEE Std 2030-2011, each data flow is categorized based upon data use characteristics. ~~device. While the bandwidth available in a network can be very high, transferring all of the data from IEDs on the network while also using the same network for an IEC 61850 process bus and protection functionality may pose bandwidth problems. It is still therefore important to evaluate the data requirements that the network is to support.~~