



# IEEE Recommended Practice for Network Communication in Electric Power Substations

---

**IEEE Power Engineering Society**

Sponsored by the  
Substations Committee

1615<sup>TM</sup>

---

IEEE  
3 Park Avenue  
New York, NY 10016-5997, USA  
8 August 2007

**IEEE Std 1615<sup>TM</sup>-2007**



# **IEEE Recommended Practice for Network Communication in Electric Power Substations**

Sponsor  
**Substations Committee**  
of the  
**IEEE Power Engineering Society**

Approved 8 March 2007  
**IEEE-SA Standards Board**

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

**Keywords:** address allocation, communication media, DNP3, electric utility, Ethernet, fiber-optic, IEC 60870-5, IEC 61850, Intelligent Electronic Device (IED), Internet protocol (IP), managed switch, network, network cable, network devices, noise sources, non-operational data, operational data, security awareness, substation, 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 © 2007 by the Institute of Electrical and Electronics Engineers, Inc.  
All rights reserved. Published 8 August 2007. 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.

Linux is a registered trademark of Linus Torvalds in the United States and other countries.

Unix is a registered trademark of The Open Group.

Windows is a registered trademark of Microsoft Corporation in the United States and other countries.

Wireshark is a registered trademark of Gerald Combs.

Print: ISBN 0-7381-5531-4 SH95630  
PDF: ISBN 0-7381-5532-2 SS95630

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

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

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

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

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

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

**Interpretations:** Occasionally questions may arise regarding the meaning of portions of standards as they relate to specific applications. When the need for interpretations is brought to the attention of IEEE, the Institute will initiate action to prepare appropriate responses. Since IEEE Standards represent a consensus of concerned interests, it is important to ensure that any interpretation has also received the concurrence of a balance of interests. For this reason, IEEE and the members of its societies and Standards Coordinating Committees are not able to provide an instant response to interpretation requests except in those cases where the matter has previously received formal consideration. At lectures, symposia, seminars, or educational courses, an individual presenting information on IEEE standards shall make it clear that his or her views should be considered the personal views of that individual rather than the formal position, explanation, or interpretation of the IEEE.

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

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

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

## Introduction

This introduction is not part of IEEE Std 1615-2007, IEEE Recommended Practice for Network Communication in Electric Power Substations.

In the spring of 2002, a task force was formed (TF1) from the membership of working group C3 in the Substations Committee of the IEEE Power Engineering Society. The overall responsibility of C3 is to facilitate the development of standards for electric network control systems. The same group had just successfully finished IEEE Std 1379™-2000 Recommended Practice for Data Communications Between Remote Terminal Units and Intelligent Electronic Devices in a Substation, which covered serial communications within the electric utility substation. A need was identified to provide the same type of guidance for the emerging practice of network communications. However, unlike IEEE Std 1379 which focuses on the two recommended protocols, the decision was made that a much more general approach was needed for the broad topic of network communication.

### The audience for this recommended practice

Many electric power utility engineers do not have a background in network communications. They are well-versed on the practice of serial communication channels, which are ubiquitous throughout this sector. These channels take the form of many point-to-point or point-to-multipoint links from central communication centers and within substations. The protocols typically used on these channels are not routable and are optimized for the particular equipment or data type. Engineers can see the benefits of using the Internet protocol suite on various physical technologies such as Ethernet, but the technical knowledge of how to apply such a communications infrastructure to the problem of data gathering seems foreign in many respects. The primary audience of this recommended practice is those looking for guidance and direction in this area.

The other groups that can benefit from this recommended practice are equipment manufacturers, system integrators, and utility consultants. One of the primary concerns for this group, as it relates to the implementation and deployment of equipment, is to provide communication network and devices for utilities that interoperate without the need for special additions, customizations, or configuration options. This document is designed to recommend practices to meet this goal.

### Brief foreword to the clauses

Clause 1 contains the scope and purpose of this document.

Clause 2 contains the normative references.

Clause 3 contains a list of acronyms and abbreviations specific to this document.

Clause 4 answers two questions for the reader in broad terms: a) What is the justification for moving from a traditional serial-communications architecture to a network-based one? and b) What is a general strategy for performing the upgrade? It also outlines two technologies to consider during the upgrade, namely serial-to-network conversion equipment and the transition from analog to digital channels.

Clause 5 introduces the Internet protocol suite and the services relevant to this recommended practice. It also provides a description of IP addressing and recommendations for address allocation in the substation.

Clause 6 defines the types of data available for use in an electric utility substation information system. The priority of the data and a general sense for how the data is used by different departments is listed. The second part of this clause presents a list of security related issues that a utility engineer must be aware of along with recommendations to address these issues.

Clause 7 addresses three important system-level issues: performance of the network as it relates to speed/latency, time synchronization, and immunity of the network equipment to noise and other environmental factors.

Clause 8 illustrates how devices are managed over the network and lists some basic tools that a utility network engineer should employ for troubleshooting and maintenance.

Clause 9 characterizes the forms of communication media and network devices that are used in a utility substation network. It provides recommendations regarding media selection for typical communication paths.

Clause 10 specifies the requirements for a predictable, real-time Ethernet suitable for the most demanding substation network applications (e.g., protective relaying).

Annex A provides an outline of the threats to the information system, where the targets of the attacks are located, how these attacks are carried out, and techniques and technologies to address these threats. Once cognizant of this outline, the utility engineer is in a stronger position to approach the specifics of his or her information system using existing security standards and technology.

Annex B, Annex C, and Annex D present the primary, standardized methods for transferring information in electric utility substations. DNP3 over IP and IEC 60870-5-104 are serial protocols that have been extended to include network facilities. IEC 61850 comprises object models, mapping of the models to a communication protocol, and a configuration language. Each method has a section describing how the features address the recommendations of this document, IEEE Std 1615.

## Notice to users

### Errata

Errata, if any, for this and all other standards can be accessed at the following URL:

<http://standards.ieee.org/reading/ieee/updates/errata/index.html>.

Users are encouraged to check this URL for errata periodically.

### Interpretations

Current interpretations can be accessed at the following URL:

<http://standards.ieee.org/reading/ieee/interp/index.html>.

### Patents

Attention is called to the possibility that implementation of this recommended practice may require use of subject matter covered by patent rights. By publication of this recommended practice, no position is taken with respect to the existence or validity of any patent rights in connection therewith. The IEEE shall not be responsible for identifying patents or patent applications for which a license may be required to implement an IEEE standard or for conducting inquiries into the legal validity or scope of those patents that are brought to its attention.

## Participants

At the time this draft recommended practice was submitted to the IEEE-SA Standards Board for approval, the C3TF1 Working Group had the following membership:

**Michael Thesing**, *Chair*

**John Tengdin**, *Vice-chair*

William J. Ackerman  
Wayne Block  
Christoph Brunner  
Jim Cai  
Mason Clark  
Jim Coats  
Ken Cooley  
Pierre Cote  
Steve Dalyai  
Michael J. Dood  
Gary R. Engmann  
Jim Evans

Etienne Fortin  
Russ Fanning  
Ron Farquharson  
Bill Harlow  
Dennis Holstein  
Chris R. Huntley  
Marc Lacroix  
Greg L. Luri  
John D. McDonald  
Bruce A. Muschlitz  
Dan Nordell

Craig M. Preuss  
Wally Prystajacky  
Peter J. Raschio  
Jim Recchia  
Sam Sciacca  
Veselin S. Skendzic  
Lee Smith  
Luc Tetreault  
Tim Tibbals  
Garnet Tremere  
Peter Wong  
Deryk Yuill

The following individuals served as authors of one or more clauses during the development of this recommended practice.

Christoph Brunner  
Jim Coats  
Michael J. Dood

Chris R. Huntley  
Bruce A. Muschlitz  
Veselin S. Skendzic

John T. Tengdin  
Michael P. Thesing  
Garnet Tremere

The following individuals are not part of the C3TF1 Working Group; however, they provided invaluable input during the development of this recommended practice.

Joe White

Caroline Rossier-Lang

Bill Godwin

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

William J. Ackerman  
Steven C. Alexanderson  
Ali Al Awazi  
Philip G. Beaumont  
Gabriel Benmouyal  
Robert W. Beresh  
Stuart H. Bouche  
Steven R. Brockschink  
Gustavo A. Brunello  
Christoph Brunner  
Terrence M. Burns  
William A. Byrd  
Thomas Carpenter  
James S. Case  
Manish Chaturvedi  
Danila Chernetsov  
Keith Chow  
Frances M. Cleveland  
Stephen P. Conrad  
Tommy P. Cooper  
R. W. Corlew  
James R. Cornelison  
Ratan Das  
J. P. Disciullo  
Kevin E. Donahoe

Carlo Donati  
Michael J. Dood  
Randall L. Dotson  
Neal B. Dowling, Jr.  
Paul R. Drum  
Donald G. Dunn  
Gary R. Engmann  
Kenneth J. Fodero  
James M. Gardner  
Michael J. Garland  
Devon L. Gayle  
Jeffrey G. Gilbert  
Keith I. Gray  
Randall C. Groves  
Phillip B. Havens  
John F. Hawkins  
Roger A. Hedding  
Gary A. Heuston  
Gary R. Hoffman  
Chris R. Huntley  
Raj Jain  
Lars E. Juhlin  
Innocent Kamwa  
Gael Kennedy  
Javeed A. Khan

Joseph L. Koepfinger  
Jim Kulchisky  
Saumen K. Kundu  
Marc Lacroix  
Chung-Yiu Lam  
Lawrence D. Long  
Daniel M. Lubar  
Greg L. Luri  
Bruce D. Mackie  
Keith N. Malmedal  
D. J. Marihart  
John D. McDonald  
Dean H. Miller  
Georges F. Montillet  
Charles A. Morse  
Jerry R. Murphy  
Bruce A. Muschlitz  
Michael S. Newman  
Chris L. Osterloh  
Lorraine K. Padden  
Donald M. Parker  
William G. Petersen  
Percy E. Pool  
Craig M. Preuss  
Iulian E. Profir

Peter J. Raschio  
R. E. Ray  
Michael A. Roberts  
Charles W. Rogers  
Miriam P. Sanders  
Bartien Sayogo  
Thomas Schossig  
Tony L. Seegers

Devki N. Sharma  
Mark S. Simon  
Veselin S. Skendzic  
Cameron L. Smallwood  
John H. Spare  
Charles R. Sufana  
Richard P. Taylor  
William T. Taylor

John T. Tengdin  
Michael P. Thesing  
Michael J. Thompson  
Demetrios A. Tziouvaras  
William P. Waudby  
James W. Wilson, Jr.  
Larry S. Young  
Oren Yuen

When the IEEE-SA Standards Board approved this Standard on 8 March 2007, it had the following membership:

**Steve M. Mills**, *Chair*  
**Robert M. Grow**, *Vice Chair*  
**Don F. Wright**, *Past Chair*  
**Judith Gorman**, *Secretary*

Richard DeBlasio  
Alexander D. Gelman  
William R. Goldbach  
Arnold M. Greenspan  
Joanna N. Guenin  
Julian Forster\*  
Kenneth S. Hanus  
William B. Hopf

Richard H. Hulett  
Hermann Koch  
Joseph L. Koepfinger\*  
John D. Kulick  
David J. Law  
Glenn Parsons  
Ronald C. Petersen  
Tom A. Prevost

Narayanan Ramachandran  
Greg Ratta  
Robby Robson  
Anne-Marie Sahazizian  
Virginia C. Sulzberger  
Malcolm V. Thaden  
Richard L. Townsend  
Howard L. Wolfman

\*Member Emeritus

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

Satish K. Aggarwal, *NRC Representative*  
Alan H. Cookson, *NIST Representative*

Lorraine Patsco  
*IEEE Standards Program Manager, Document Development*

Matthew J. Ceglia  
*IEEE Standards Program Manager, Technical Program Development*

## Contents

|                                                                                           |    |
|-------------------------------------------------------------------------------------------|----|
| 1. Overview .....                                                                         | 1  |
| 1.1 Scope .....                                                                           | 1  |
| 1.2 Purpose .....                                                                         | 1  |
| 2. Normative references.....                                                              | 1  |
| 3. Acronyms and abbreviations .....                                                       | 2  |
| 4. Electric utility information system architecture.....                                  | 3  |
| 4.1 Traditional serial-communication architecture .....                                   | 4  |
| 4.2 Networked communication architecture .....                                            | 6  |
| 4.3 Moving to a network-based system .....                                                | 8  |
| 5. Internet protocol suite (IPS) and services .....                                       | 12 |
| 5.1 IP layers .....                                                                       | 13 |
| 5.2 IP Addressing .....                                                                   | 15 |
| 5.3 Recommendations for utility networks.....                                             | 19 |
| 6. Data classification and security for IPS networks .....                                | 19 |
| 6.1 Types and uses of data.....                                                           | 19 |
| 6.2 Security issues and recommendations .....                                             | 21 |
| 7. System level requirements in substation networks .....                                 | 24 |
| 7.1 Performance requirements of a substation network .....                                | 24 |
| 7.2 Time synchronization .....                                                            | 25 |
| 7.3 Substation noise sources .....                                                        | 25 |
| 8. Network management tools and practices for an electric utility information system..... | 26 |
| 8.1 Vendor-specific network devices.....                                                  | 27 |
| 8.2 Network management in the electric utility information system .....                   | 28 |
| 8.3 Tools .....                                                                           | 30 |
| 9. Media and device alternatives for the substation network.....                          | 34 |
| 9.1 Media .....                                                                           | 34 |
| 9.2 Network devices .....                                                                 | 42 |
| 10. Substation LAN requirements .....                                                     | 44 |
| 10.1 Port speed and fiber-optic interface .....                                           | 45 |
| 10.2 Full duplex operation and collision-free environment.....                            | 45 |
| 10.3 Priority queuing .....                                                               | 45 |
| 10.4 Virtual LAN support.....                                                             | 46 |
| 10.5 Loss-of-link management .....                                                        | 46 |

|                                                                                                   |    |
|---------------------------------------------------------------------------------------------------|----|
| 10.6 Rapid-spanning tree algorithm support.....                                                   | 46 |
| 10.7 Flow control.....                                                                            | 47 |
| 10.8 Multicast propagation control.....                                                           | 47 |
| 10.9 Remote monitoring, port mirroring, and diagnostic support.....                               | 47 |
| 10.10 Environmental hardening.....                                                                | 47 |
| 10.11 MAC filtering and port lockout .....                                                        | 48 |
| 10.12 Summary recommendations to support real-time protection over Ethernet.....                  | 48 |
| Annex A (informative) Security issues and awareness .....                                         | 49 |
| A.1 Source of threats to the electric power system.....                                           | 49 |
| A.2 Targets of attack in the electric utility network .....                                       | 50 |
| A.3 Common cyber-attack techniques.....                                                           | 52 |
| A.4 Techniques to address threats to the electric utility network .....                           | 55 |
| Annex B (informative) DNP3—IP networking.....                                                     | 61 |
| B.1 DNP3 protocol overview .....                                                                  | 61 |
| B.2 History of DNP3 .....                                                                         | 61 |
| B.3 Protocol features .....                                                                       | 62 |
| B.4 Features of the DNP3 protocol pertinent to this recommended practice, IEEE Std 1615-2007..... | 65 |
| B.5 DNP3 definition documents.....                                                                | 66 |
| Annex C (informative) IEC 60870-5-104.....                                                        | 67 |
| C.1 Background/history.....                                                                       | 67 |
| C.2 Functionality in a network environment .....                                                  | 68 |
| C.3 Features of IEC 60870-5-104 pertinent to this recommended practice, IEEE Std 1615-2007.....   | 69 |
| C.4 IEC 60870-5-104 definition documents.....                                                     | 70 |
| Annex D (informative) IEC 61850.....                                                              | 71 |
| D.1 Overview and history of IEC 61850 .....                                                       | 71 |
| D.2 The information model according to IEC 61850 .....                                            | 73 |
| D.3 Information exchange .....                                                                    | 73 |
| D.4 Configuration management.....                                                                 | 75 |
| D.5 Features of IEC 61850 pertinent to this recommended practice, IEEE Std 1615-2007 .....        | 76 |
| Annex E (informative) Bibliography.....                                                           | 77 |



# IEEE Recommended Practice for Network Communication in Electric Power Substations

## 1. Overview

### 1.1 Scope

This document defines a recommended practice for communication and interoperation of devices connected on an electric power substation Internet protocol (IP) network. It does not establish a new underlying communications standard. Instead, the document prescribes a specific set of existing conventions and definitions.

### 1.2 Purpose

This recommended practice provides direction for implementers who wish to produce interoperable communications equipment for an electric power substation network. It also provides criteria for users, system integrators, and equipment manufacturers who need to establish requirements for the transfer of operational and non-operational data as well as configuration management.

## 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 1590™-2003, IEEE Recommended Practice for the Electrical Protection of Optical Fiber Communication Facilities Serving, or Connected to, Electrical Supply Locations.<sup>1, 2</sup>

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

---

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

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

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

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

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

IEEE Std 802.3™-2005, IEEE Standard for Information Technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—specific requirements Part 3: Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications.

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

|          |                                            |
|----------|--------------------------------------------|
| ACSI     | abstract communication service interface   |
| AES      | advanced encryption standard               |
| ARP      | address resolution protocol                |
| ASN.1    | Abstract Syntax Notation One               |
| BER      | basic encoding rules                       |
| BOOTP    | Bootstrap Protocol                         |
| COMTRADE | command format for transient data exchange |
| CRC      | cyclic redundancy check                    |
| CSMA     | carrier sense multiple access (Ethernet)   |
| DCS      | distributed control system                 |
| DES/3DES | data encryption standard                   |
| DHCP     | dynamic host configuration protocol        |
| DMD      | differential mode dispersion               |
| DMS      | distribution management system             |
| DNS      | domain name system                         |
| DNP/DNP3 | distributed network protocol, version 3.0  |
| DoS      | denial of service                          |
| DTCC     | digital tap changer controller             |
| EMI      | electromagnetic interference               |
| EMS      | energy management system                   |
| FTP      | file transfer protocol                     |
| GOOSE    | generic object oriented substation event   |
| GPR      | ground potential rise                      |
| GPS      | global positioning system                  |
| GSSE     | generic substation status event            |
| GUI      | graphical user interface                   |
| HMI      | human-machine interface                    |
| HTML     | hypertext markup language                  |
| HTTP     | hypertext transfer protocol                |
| IANA     | Internet Assigned Numbers Authority        |
| ICMP     | Internet control message protocol          |
| IED      | intelligent electronic device              |
| IETF     | Internet engineering task force            |
| IDS      | intrusion detection system                 |
| IGMP     | Internet group management protocol         |

|       |                                                                                 |
|-------|---------------------------------------------------------------------------------|
| IP    | Internet protocol                                                               |
| IPv6  | Internet protocol, version 6                                                    |
| IPS   | Internet protocol suite                                                         |
| IRIG  | inter-range instrumentation group                                               |
| ISO   | independent system operator (or International Organization for Standardization) |
| IT    | information technology                                                          |
| LAN   | local area network                                                              |
| LED   | light emitting diode                                                            |
| MAC   | media access control                                                            |
| Mb/s  | mega (10 <sup>6</sup> ) bits per second                                         |
| MIB   | management information base (SNMP)                                              |
| MMS   | manufacturing message specification                                             |
| NAT   | network address translation                                                     |
| NTP   | network time protocol                                                           |
| OID   | object identifier                                                               |
| QoS   | quality of service                                                              |
| OSI   | open systems interconnection                                                    |
| PPP   | point-to-point protocol                                                         |
| PSTN  | public switched telephone network                                               |
| RCP   | remote copy                                                                     |
| RFC   | request for comment document                                                    |
| RFI   | radio frequency interference                                                    |
| RMON  | remote traffic monitoring                                                       |
| RSA   | (Rivest, Shamir, Adelman) encryption algorithm                                  |
| RTO   | regional transmission organizations                                             |
| RTU   | remote terminal unit                                                            |
| SCADA | supervisory control and data acquisition                                        |
| SCL   | substation configuration language                                               |
| SCP   | secure remote copy                                                              |
| SCSM  | specific communication service mapping                                          |
| SFP   | small form-factor pluggable                                                     |
| SFTP  | secure file transfer protocol                                                   |
| 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                                                                    |
| SWC   | surge withstand capability                                                      |
| TCP   | transmission control protocol                                                   |
| Telco | telecommunication service company                                               |
| UDP   | user datagram protocol                                                          |
| UTP   | unshielded twisted pair wire                                                    |
| VLAN  | virtual local area network                                                      |
| VPN   | virtual private network                                                         |
| WAN   | wide area network                                                               |
| WLAN  | wireless local area network                                                     |

## 4. Electric utility information system 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)

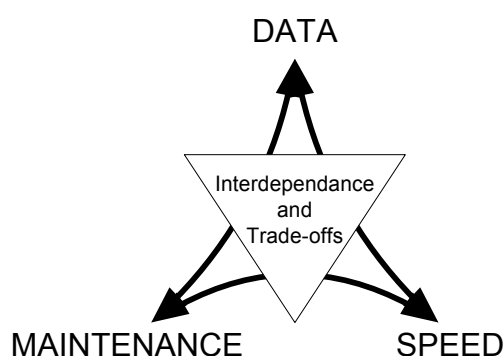


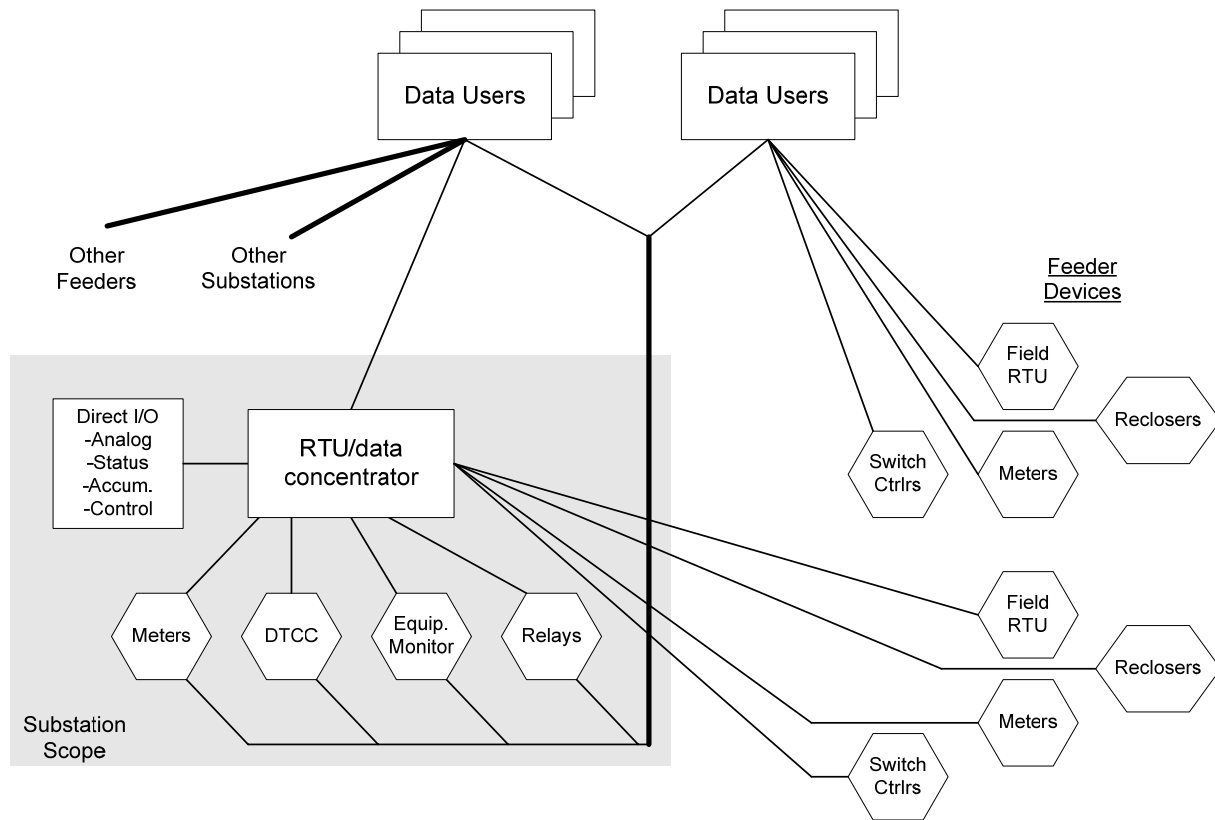
**Figure 1—Information system usefulness factors**

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 dominant electric power serial-communication architecture is illustrated in Figure 2. The system consists of equipment at one or more 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.



#### Legend

- RTU - Remote Terminal Unit
- LTC - Load Tap Changer Controller
- Serial communication channel
- Multiple serial channels
- ⬡ Intelligent Electronic Device (IED)

**Figure 2—Traditional serial-communication architecture**

This architecture has evolved over time to facilitate the interconnection of many different types of equipment using many different serial protocols. The serial channels can be point-to-point and point-to-multipoint. The remote terminal unit (RTU)/data concentrator function typically supports many channels at a time and provides local I/O and protocol conversion. Separate dedicated or ad-hoc channels are required for maintenance and non-operational data retrieval.

#### 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 devices:

- Some serial architectures are more reliable and less expensive than networks.
- For small systems with small point counts, low speed serial systems 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 Networked communication architecture

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

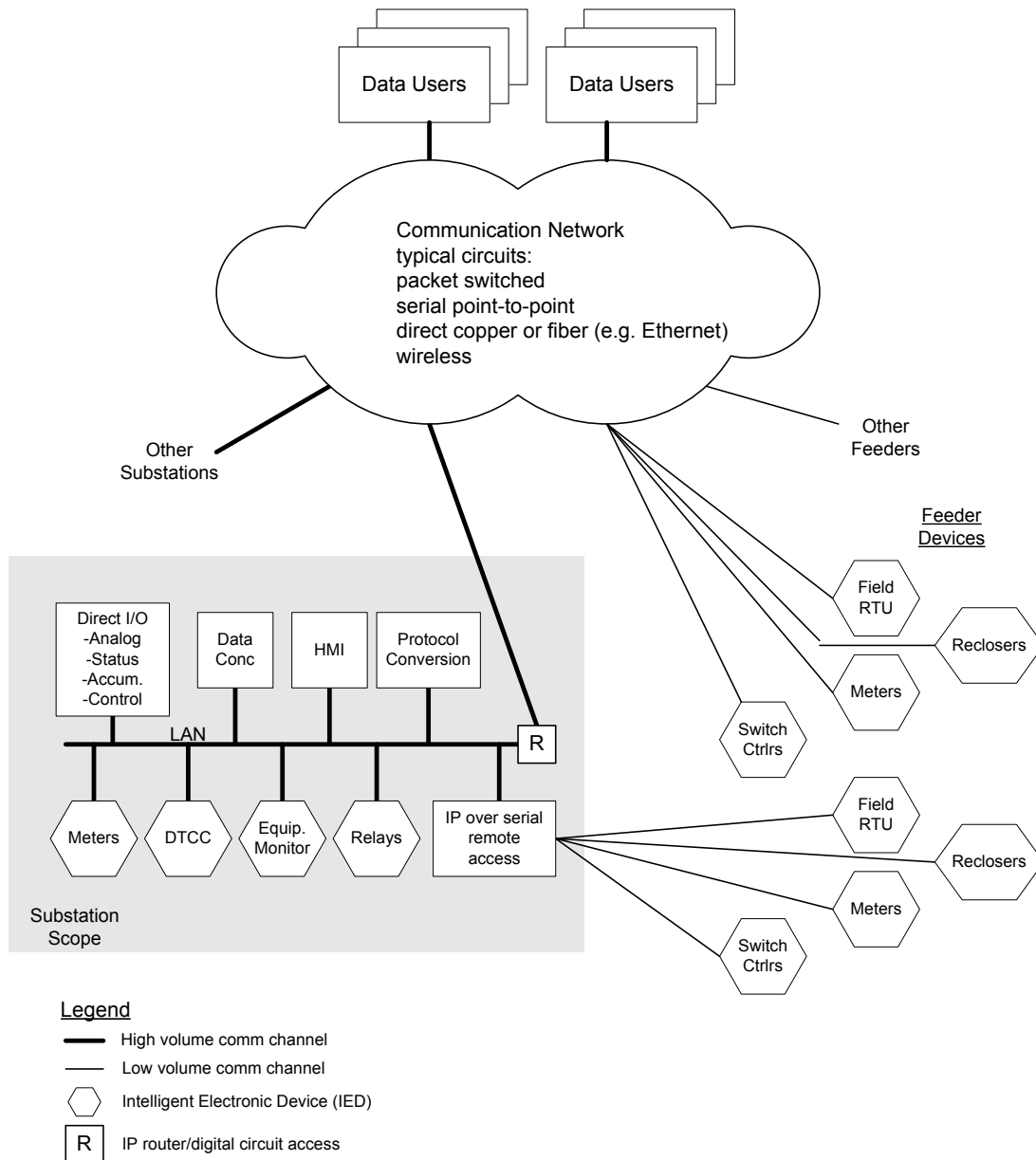


**Figure 3—Networked information system**

Notice that all devices do not necessarily have to be on a local area network (LAN) to be accessible to the network. In Figure 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.

#### 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.<sup>3</sup>

#### 4.2.2 Challenges

Adding networks to substations can introduce the following significant challenges:

- **Training:** Those who are familiar with networking equipment are generally not familiar with substations. Those who are familiar with substation devices may not be familiar with networking. In many cases, overlap does not exist, so training for personnel on both sides is required and some organizational realignment may be needed to bridge the gaps.
- **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, resulting in larger battery sizes to support the networking equipment during extended outages. Battery calculations should be revisited during system design to ensure the battery system will support the substation networking devices.

#### 4.3 Moving to a network-based system

The move to a network architecture should be justified by one or more of the following needs:

- **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, it will likely install IEDs that can provide this information. Depending on the importance that a utility places on this data, this could be the sole justification for installing a

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

communication network. All sophisticated system-level applications are 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 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.
- **Ability to multiplex channels of information:** The Internet protocol suite (IPS) supports multiple channels allowing concurrent access to a device. With non-routable serial communications, separate physical links are needed for SCADA, remote access, file retrieval, and substation human-machine interface (HMI).
- **Reduction of system expansion costs:** Ethernet can also reduce overall system costs when compared with a serial system. While serial devices are probably cheaper, as system functionality increases along with the number of devices, serial systems require more connections that will offset the additional costs of installing Ethernet. Initial deployment costs 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 when multiple functions are required.
- **Ubiquity of Ethernet:** Ethernet is widely supported and understood in IT departments and a huge body of knowledge exists in the public domain for installation and deployment. Ethernet can also be easily monitored 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.

### 4.3.1 Strategy for upgrading

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

#### 4.3.1.1 Top-down approach

The top-down approach constitutes the following steps:

- a) Upgrade communications to the substation and add a network interface to the RTU/data concentrator
- b) Add a network within the substation
- c) Upgrade communications to the feeder devices and make them network accessible

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

#### *Advantages:*

- Adds bandwidth where it is needed most; the substation-to-control center communications load is the aggregate of that portion of the system
- Improves access to the RTU/data concentrator and potentially, other IEDs
- May allow inclusion or consolidation of other communications service (for example, phone, video surveillance, etc.)
- May allow replacing analog lines with more reliable digital channels

- May reduce wire line costs based on distance charges

***Disadvantages:***

- May significantly increase communication costs
- Initially only allows access to the RTU/data concentrator; this device may *not* be the most important data source
- Requires upgrading equipment at the control center
- Forces additions to workforce skill sets

#### **4.3.1.2 Bottom-up approach**

The bottom-up approach constitutes the following steps:

- a) Add a network within the substation
- b) Upgrade communications to the feeder devices and make them network accessible
- c) Upgrade communications to the substation and add a network interface to the RTU/data concentrator

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

***Advantages:***

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

***Disadvantages:***

- Does not allow access to system outside of substation until later in the evolution
- Does not increase response time from the control center
- May require initial upgrade to networked IEDs or, depending on the protocol, the addition of a 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.

#### **4.3.2 Interfacing serial equipment to a network**

Substation devices are frequently chosen using evaluation criteria that take precedence over communications capabilities. Relays are primarily selected based upon protection, performance, function, and capability. 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 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.

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.

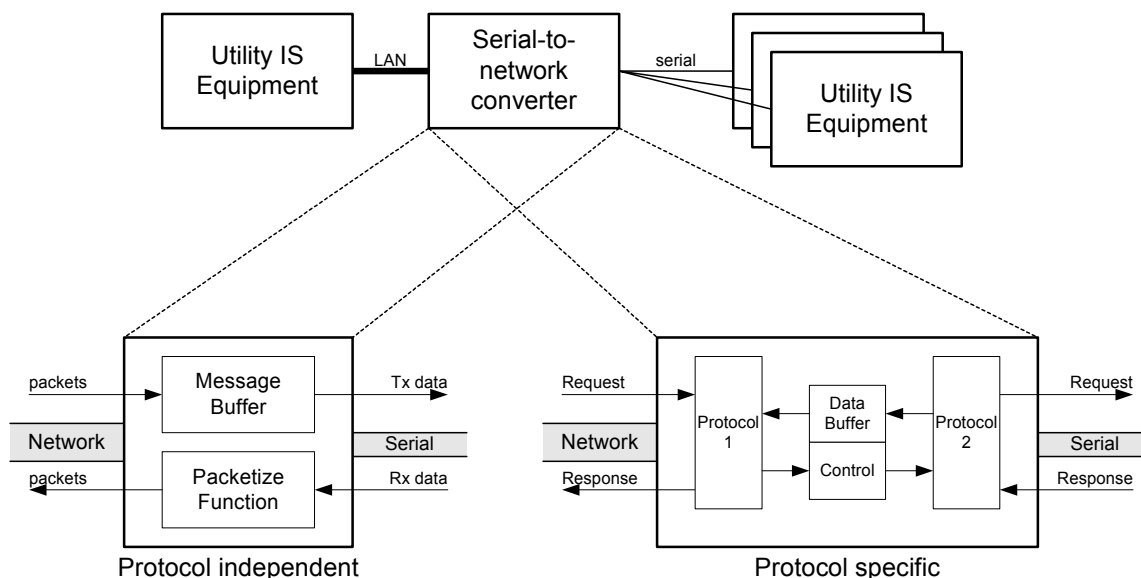


**Figure 4—Serial-to-network converters**

The protocol-independent converter is sometimes called a “terminal server” (also known as a “port server”) in traditional information systems and typically supports from 1 to 16 serial ports. It 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 (usually RS232 or RS485).

A protocol-specific converter is used when two pieces of equipment cannot communicate because they use different protocols. This is a more sophisticated device than the protocol-independent converter in terms of how each interface is handled and the amount of configuration required. Some 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, 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.

#### 4.3.3 Converting from analog leased to digital leased lines

Some utilities have relied on leased communication lines from a telecommunication service company (Telco) provider. 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 private.

Telcos charge different rates for digital service. For the equivalent of an analog leased line, 56 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 line, potentially saving the utility Telco charges. Note this assumes the utility has already installed any required Telco isolation equipment. 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 capability for network traffic.

## 5. Internet protocol suite (IPS) and services

The IPS is platform-independent and supported universally around the world. It is highly scalable, i.e., local area network (LAN) to wide area network (WAN), and many quality implementations exist for both embedded and workstation operating systems. The growth of the Internet has fueled the large availability of equipment and has proved that the IPS is capable of transporting tremendous quantities and types of data. With some tailoring, the security protocols and mechanisms developed, and being developed, for the Internet are applicable to electric utility networks.

The most attractive reasons for choosing the IPS for electric utility networks are as follows:

- Simplified integration between existing networks
- Leverage existing equipment and standards

The IPS is composed of several protocols that provide data transport services and a number of applications for network-related activities. It is commonly referred to “TCP/IP,” after the two most important protocols in it: the transmission control protocol (TCP) and the Internet protocol (IP), which were also the first two defined. However, the IPS refers to the entire set of protocols developed by the Internet community. The Internet protocols are defined by request for comment (RFC) documents available from the Internet Engineering Task Force (IETF)<sup>4</sup> as public domain works. Although some of the RFCs specify the Internet protocols, many of the RFCs are for information or application guidance only and are not official standards. While the IPS can be roughly fitted to the open systems interconnection (OSI) model that describes a fixed set of seven layers and some vendors like to use this model, some believe that fitting the IPS to the OSI model does more to confuse than to help. Note that the IPS does not define the data link and physical layer because the IPS was designed to accommodate any underlying network technology.

Table 1 lists the Internet protocols pertinent to this clause.

**Table 1—Internet protocols for this recommended practice**

| Name                                             | RFC        | Description                                                                                                                |
|--------------------------------------------------|------------|----------------------------------------------------------------------------------------------------------------------------|
| IP                                               | 791        | Network layer of the IPS                                                                                                   |
| TCP                                              | 793        | Connection-oriented transport layer of the IPS                                                                             |
| UDP                                              | 768        | Connectionless transport layer of the IPS                                                                                  |
| DNS                                              | 1034, 1035 | Distributed database used to map between hostnames and IP addresses                                                        |
| ARP                                              | 826        | Provides address mapping IP and the link layer (e.g., Ethernet)                                                            |
| BOOTP                                            | 951        | Basic service allowing hosts to query for their IP address                                                                 |
| DHCP                                             | 2131       | Service allowing hosts to query for their IP address and other initial parameters at startup from a server. Replaces BOOTP |
| —                                                | 1918       | Address allocation for private internets                                                                                   |
| —                                                | 1006       | ISO Transport service on top of the TCP                                                                                    |
| <b>Legend</b>                                    |            |                                                                                                                            |
| <b>ARP:</b> Address resolution protocol          |            |                                                                                                                            |
| <b>BOOTP:</b> Bootstrap Protocol                 |            |                                                                                                                            |
| <b>DHCP:</b> Dynamic host configuration protocol |            |                                                                                                                            |
| <b>DNS:</b> Domain name system                   |            |                                                                                                                            |
| <b>IP:</b> Internet protocol                     |            |                                                                                                                            |
| <b>IPS:</b> Internet protocol suite              |            |                                                                                                                            |
| <b>ISO:</b> Internet protocol suite              |            |                                                                                                                            |
| <b>TCP:</b> Transmission control protocol        |            |                                                                                                                            |
| <b>UDP:</b> User datagram protocol               |            |                                                                                                                            |

<sup>4</sup> IETF documents are available at <http://www.ietf.org>.

## 5.1 IP layers

Figure 5 shows the various protocols in the Internet protocol suite (see Stevens [B45]<sup>5</sup> for a complete description).

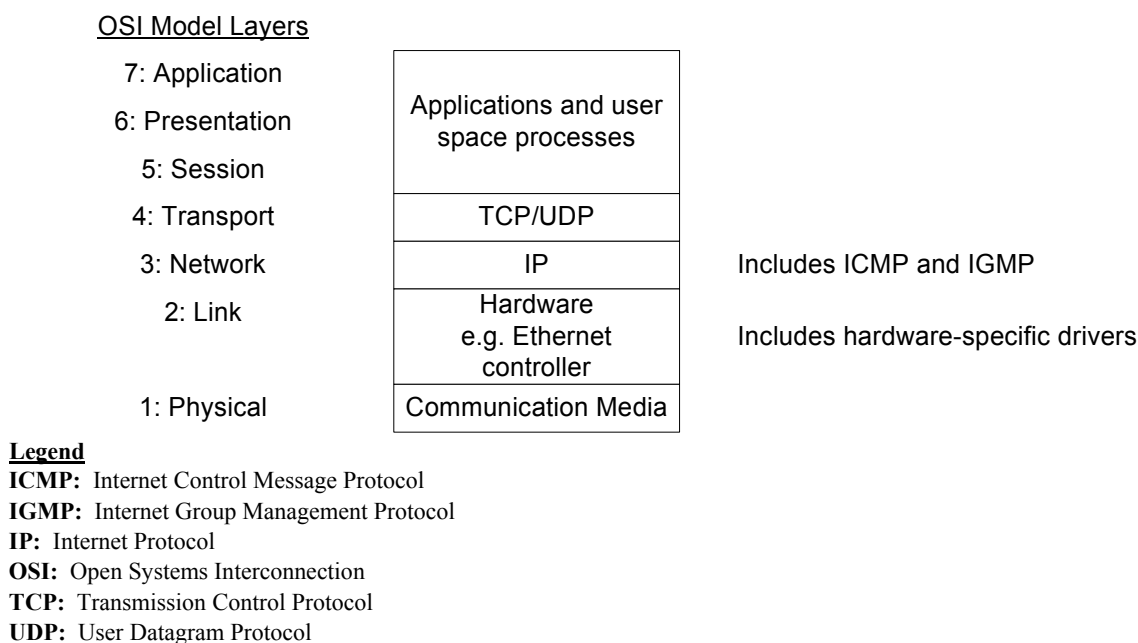


**Figure 5—IPS protocols and layers**

### 5.1.1 Link layer

The link layer is not really a part of the IPS. The link layer passes packets from the network layer of one device to the network layer of another. On one end, the link layer adds a frame header to prepare it for transmission and then transmits the frame over a physical medium. On the other end, the link layer receives data frames, strips off the frame headers, and hands the received packets to the network layer.

### 5.1.2 Network layer

The network layer solves the problem of getting packets across a single network or from the source network to the destination network. This generally involves routing the packet across a network of networks, known as an Internet.

In the IPS, IP provides the addressing and basic delivery service. An IP data packet is called a datagram. The IP layer does not maintain any state information about successive datagrams. However there is enough information in the datagrams to perform packet fragmentation in the network and reassembly at the destination. An IP datagram encapsulates transport layer data packets.

Matching the IP address to a specific network device is accomplished by the address resolution protocol (ARP). It is this protocol that links the OSI network layer to the OSI link layer. Each hardware device connected to a network is assigned a hardware address called a media access control (MAC) address. The ARP protocol “resolves” these addresses and therefore associates the IP software address with the device hardware address.

<sup>5</sup> The numbers in brackets preceded by the letter B correspond to those of the bibliography in Annex E.

### 5.1.3 Transport layer

The transport layer service allows applications to use a standard set of function calls in order to communicate on a variety of networks without worrying about different network interfaces. In the IPS this function is achieved by the connection oriented transmission control protocol (TCP) and the connectionless user datagram protocol (UDP).

#### 5.1.3.1 Connection oriented—TCP

The transmission control protocol (TCP) provides a connection-oriented transport service for the IPS. This means that two computers must negotiate a connection before data can be transferred. For TCP, one end is termed the server and it listens for connection requests. The other end is termed the client, which initiates connection requests. Once the connection is established, it may be held indefinitely or closed by either end. TCP also provides a number of mechanisms for enhancing the reliability of the data transfer. For example, TCP uses acknowledgements, sequencing, and dynamic timeout and retry of packets.

#### 5.1.3.2 Connectionless—UDP

The user datagram protocol (UDP) provides a connectionless transport service for the IPS. Two or more computers can exchange UDP datagrams without having to negotiate a connection. UDP does not provide any reliability enhancements aside from an optional checksum of the data. Any applications that utilize UDP must provide their own assurance mechanisms as necessary. UDP datagrams may be sent to multiple destinations using broadcast or multicast addressing.

#### 5.1.3.3 Ports

To facilitate a plurality of applications within a device (e.g., on a PC with a single IP address), TCP and UDP transport layer protocols have their own identifiers called ports (0–65 535). Port numbers below 1024 are reserved for standard applications such as hypertext transfer protocol (HTTP), file transfer protocol (FTP), telnet, etc. and are referred to as “well known ports.” Port numbers from 1024 through 49 151 may be used by ordinary applications. They are called “registered ports” since the Internet Assigned Numbers Authority (IANA)<sup>6</sup> allows users to register them for common knowledge. “Dynamic and/or private ports” are those from 49 152 through 65 535.

#### 5.1.3.4 TCP/UDP comparison

TCP provides features that ensure the correct delivery of messages; however it does so at the expense of increased network traffic (often by two to ten times), and the potential for increased latency (TCP can delay messages by hundreds of milliseconds). TCP is a good choice for “long term” communications such as file transfers (e.g., event records, e-mail) and data acquisition that can tolerate short delays (e.g., most SCADA data).

UDP provides a simple, low overhead message delivery service. However it does not provide any features that ensure the messages arrive at their destination. This must be handled by the application. UDP is a good choice for substation applications that require timely communications (e.g., time synchronization, switching commands) and can tolerate or compensate for network errors.

---

<sup>6</sup> See IANA information at <http://www.iana.org>.

## 5.1.4 IPS services

### 5.1.4.1 Name-to-address mapping

The domain name system (DNS) is a distributed database that is used by other applications to map between hostnames (e.g., www.ieee.org) and IP addresses. This allows users to specify human readable names of other computers when initiating data transfer and it allows users access to computers that may have dynamic IP addresses. The IPS must know the IP address of a computer before initiating a TCP connection or UDP datagram transmission. DNS uses the UDP transport layer. The DNS service must be provided on a network by a DNS server and each computer must know the address of this server to use the DNS.

### 5.1.4.2 Managed host configuration

The dynamic host configuration protocol (DHCP) provides a means for delivering host-specific configuration parameters (e.g., IP addresses at startup) and a mechanism for managing IP addresses on a network. A designated DHCP server can allocate IP addresses to other computers on the network so that the address pool for that network can be managed from a single location. Each client computer queries the server for its unique set of IP address information.

### 5.1.4.3 Bootstrapping an IP address

The Bootstrap Protocol (BOOTP), is a UDP network protocol used by a network client to automatically obtain an IP address during the booting process of computers or operating systems running on them. The BOOTP servers assign the IP address from a pool of addresses to each client. A typical use of BOOTP is to enable “diskless workstation” computers to obtain an IP address prior to loading any advanced operating system.

## 5.2 IP Addressing

Every device/computer on an IP network must have a unique IP address. For most devices, this means one unique address, as most devices have one interface to the network. For routers and gateways (devices that move data from one network to another), this requirement dictates two or more unique addresses depending on the number of networks.<sup>7</sup>

### 5.2.1 Structure

An IP address is composed of three parts (see Figure 6). The Network ID is determined by the first bytes of the address and depends on the particular range of addresses allocated for use on the global Internet. The Subnet ID allows a large network to be divided into smaller networks, thus simplifying the routing. The Host ID refers to the particular computer on this smaller network. The combination of the three parts gives each computer a unique address in the overall network.

|             |            |  |           |
|-------------|------------|--|-----------|
|             | MSB        |  | LSB       |
| IP address  | Network ID |  | Subnet ID |
| Subnet mask | all 1's    |  | all 0's   |

**Figure 6—IP address structure**

<sup>7</sup> Currently, IP addresses are 32 bits long. However, a movement is underway to slowly phase in 128-bit addresses since the number of devices connected to the global Internet continues to grow rapidly and may eventually exceed the available 32 bit address space. These efforts parallel address assignment and routing initiatives that better utilize the existing address space. The new 128-bit address scheme (termed IPv6) also provides additional features such as quality of service (QoS), autoconfiguration, and security headers.

The subnet mask is required for all computers and determines the boundary in the 32-bit address between the subnet ID and host ID. Using the host ID and subnet mask, each computer can determine whether a packet destined for another computer can be sent directly or whether it needs to be routed through another network to reach its destination. Valid subnet masks always have only ones on the left and zeroes on the right. For example, the mask 255.255.255.192 has 26 “1” bits and 6 “0” bits for a total of 64 addresses on the subnet.

Any IP address can be written with the notation AAA.BBB.CCC.DDD/NN where AAA.BBB.CCC.DDD is the IP address and NN is the number of “1” bits in the subnet mask.

### 5.2.2 Special cases

A computer on a network cannot be assigned a host ID of zero or all ones (-1). These are reserved for special use. A host ID or subnet ID of 0 can never be used as a destination address, and is typically used in network diagrams and configuration programs to refer to a range of addresses. For example, the address 192.168.5.0/24 describes all of the computers with host IDs 1 through 254 on the subnet 192.168.5 with a subnet mask of 255.255.255.0. The all-ones host ID for this network of 255 (hex FF) can never be used as a source address, and is used to indicate a broadcast packet. For example, a destination address of 192.168.5.255/24 will cause a packet to be routed to all computers on the 192.168.5 subnet (assuming broadcasting is enabled for that network).

### 5.2.3 Address allocation

There are two ways that a network device can obtain its IP address. The first is to have a discrete method for setting the value in the device (usually via a user interface). The second is for the device to query a server on the network for a pre-assigned or dynamic address. The latter type of allocation uses either BOOTP or DHCP.

For more guidance on address allocation, see IETF RFC 1918 [B37] or Mansfield [B41].

#### 5.2.3.1 Discrete address allocation

Figure 7 shows an example of a network where all of the devices have an individually-defined address.

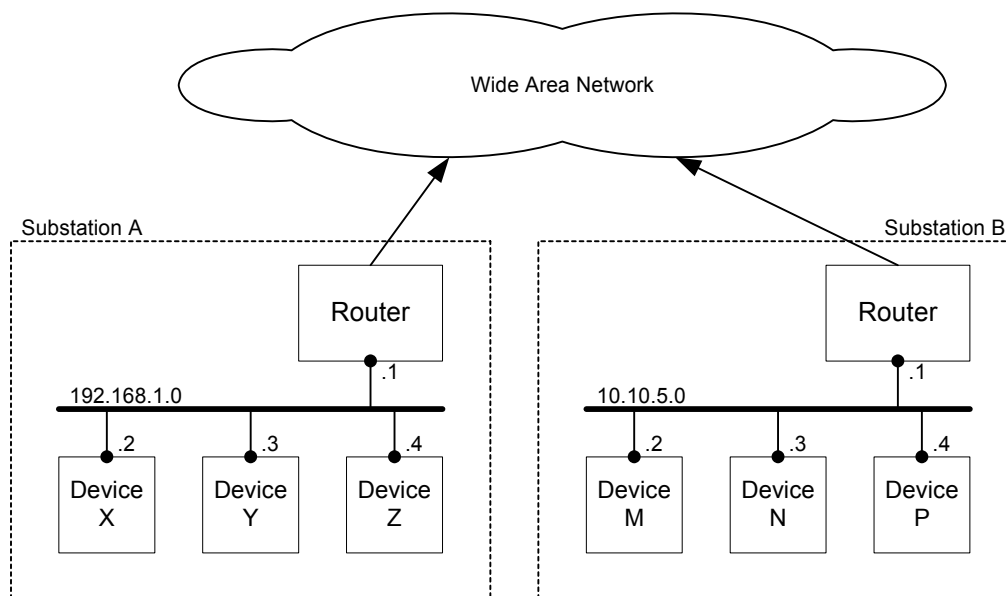


Figure 7—Discrete address allocation