

Recognized as an
American National Standard (ANSI)

IEEE Std 1379-2000(R2006)
(Revision of
IEEE Std 1379-1997)

IEEE Recommended Practice for Data Communications Between Remote Terminal Units and Intelligent Electronic Devices in a Substation

Sponsor

Substations Committee
of the
IEEE Power Engineering Society

Reaffirmed 30 March 2006
Approved 21 September 2000
IEEE-SA Standards Board

Approved 1 January 2001
American National Standards Institute

Abstract: A uniform set of guidelines for communications and interoperations of remote terminal units (RTUs) and intelligent electronic devices (IEDs) in an electric utility substation is provided. A mechanism for adding data elements and message structures to this recommended practice is described.

Keywords: IED, master station, RTU, slave, supervisory control and data acquisition (SCADA) systems

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

Copyright © 2001 by the Institute of Electrical and Electronics Engineers, Inc.
All rights reserved. Published 16 March 2001. Printed in the United States of America.

Print: ISBN 0-7381-2639-X SH94890
PDF: ISBN 0-7381-2640-3 SS94890

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.

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
P.O. Box 1331
Piscataway, NJ 08855-1331
USA

Note: 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 with respect to the existence or validity of any patent rights in connection therewith. The IEEE shall not be responsible for identifying patents for which a license may be required by an IEEE standard or for conducting inquiries into the legal validity or scope of those patents that are brought to its attention.

IEEE is the sole entity that may authorize the use of certification marks, trademarks, or other designations to indicate compliance with the materials set forth herein.

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; (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 1379-2000, IEEE Recommended Practice for Data Communications Between Remote Terminal Units and Intelligent Electronic Devices in a Substation.)

This recommended practice presents a uniform set of guidelines for specific interdevice communication details that can permit interoperation of remote terminal units (RTUs) and intelligent electronic devices (IEDs) in an electric utility substation. The data definitions and message structure can be used by product developers of both RTUs and IEDs to create nonproprietary communication interfaces, and by buyers and specifiers as a definition or reference document for data representation and transmission. The standard can also be used as a communication interface between RTUs and supervisory control and data acquisition (SCADA) master stations.

The task force that prepared this recommended practice began with the objective of providing a forum for the providers and users of (smart) devices to discuss approaches to common data interchange. As the dialogue progressed, members decided to survey, review, and evaluate existing communications protocols and standards for those protocols. Task force members, as a result of the studies, presentations, and discussions, decided that maximum progress toward interoperability would be made if existing defined protocol(s) were publicly implemented. The original trial use recommended practice was the result of that decision.

This recommended practice does not establish an underlying communication standard. It instead provides a specific implementation of two existing communication protocols already in wide scale use in the public domain (all documentation is available for a nominal fee without proprietary restriction). This document is also a template for extensions of the concept by other groups, if desired. A mechanism for adding data elements and message structures to this recommended practice is described, recognizing the rapid progress being made with IEDs of all types in all areas of the electric utility industry.

There are continuing efforts in the IEEE Power Engineering Society Committees, as well as in the IEC and CIGRE to seek further compatibility among devices through communication standards. This is being aided by the efforts of many industry groups, consultants, and suppliers who see benefits in such compatibility.

At the time this recommended practice was developed, Task Force 1 of Working Group C3 had the following membership:

H. Lee Smith, *Chair*

William J. Ackerman
Alexander Apostolov
Wayne R. Block
Ken L. Cooley
Ken Curtis
Michael J. Dood
James W. Evans
Ron J. Farquharson

Grant Gilcrest
Ameen Hamdon
Derick Hammond
Dennis K. Holstein
Marc Lacroix
Parker McCauley
Bruce Muschlitz

H. Lee Smith
Robert C. Sodergren
John T. Tengdin
Michael Thesing
Jack Verson
Tony Watson
Andrew West
David Wood

The following members of the balloting committee voted on this standard:

Hanna E. Abdallah	Donald G. Dunn	Gary L. Michel
William J. Ackerman	Ahmed Elneweihi	Bruce Muschlitz
Stan J. Arnot	Gary R. Engmann	Daniel E. Nordell
Thomas M. Barnes	James W. Evans	Shashi G. Patel
George J. Bartok	Ron J. Farquharson	Carlos O. Peixoto
Michael J. Bio	David L. Harris	Radhakrishna V. Rebbapragada
Philip C. Bolin	Dennis K. Holstein	Paulo F. Ribeiro
Stuart H. Bouchey	James Jung	David Shafer
Dennis L. Carr	George G. Karady	Yitzhak G. Shertok
James F. Christensen	Richard P. Keil	Mark S. Simon
John R. Clayton	Hermann Koch	Robert C. Sodergren
Ken L. Cooley	Luther W. Kurtz	Brian Sparling
Robert Corlew	David S. Lehman	Peter G. Stewart
Frank A. Denbrock	H. Peter Lips	Charles Sufana
W. Bruce Dietzman	John D. McDonald	John T. Tengdin
Randall L. Dotson	A. S. Mehraban	Duane R. Torgerson
Clifford Downs	A. P. Sakis Meliopoulos	Peter S. Wong
Paul R. Drum		John A. Zulaski

When the IEEE-SA Standards Board approved this standard on 21 September 2000, it had the following membership:

Donald N. Heirman, *Chair*
James T. Carlo, *Vice Chair*
Judith Gorman, *Secretary*

Satish K. Aggarwal	James H. Gurney	James W. Moore
Mark D. Bowman	Richard J. Holleman	Robert F. Munzner
Gary R. Engmann	Lowell G. Johnson	Ronald C. Petersen
Harold E. Epstein	Robert J. Kennelly	Gerald H. Peterson
H. Landis Floyd	Joseph L. Koepfinger*	John B. Posey
Jay Forster*	Peter H. Lips	Gary S. Robinson
Howard M. Frazier	L. Bruce McClung	Akio Tojo
Ruben D. Garzon	Daleep C. Mohla	Donald W. Zipse

*Member Emeritus

Also included is the following nonvoting IEEE-SA Standards Board liaison:

Alan Cookson, *NIST Representative*
Donald R. Volzka, *TAB Representative*

Noelle D. Humenick
IEEE Standards Project Editor

Contents

1.	Overview	1
1.1	Scope.....	1
1.2	Purpose.....	1
1.3	Distributed network protocol (DNP3)	2
1.4	IEC 60870-5 protocol	2
2.	References.....	2
3.	Definitions, acronyms, and abbreviations.....	3
3.1	Definitions.....	3
3.2	Acronyms and abbreviations.....	6
4.	Description of RTU-to-IED communications needs.....	6
4.1	The traditional SCADA protocol	7
4.2	Specific criteria used to select protocols for RTU/IED communication	7
5.	Recommended practice for RTU/IED communication.....	8
5.1	General application practice using DNP3	8
5.2	General application practice using IEC-60870-5 standards.....	11
5.3	Functionality of the 101 companion standard profile	11
5.4	Summary comparative description tables	14
6.	Physical layer definition (ISO/OSI layer 1).....	16
6.1	Modes of transmission	16
6.2	Local loop	16
6.3	Recommended physical layer for DNP3.....	16
6.4	Recommended physical layers for IEC 60870-5-101 (1995-11).....	17
7.	Data link layer definition (ISO/OSI layer 2).....	17
7.1	Recommended data link layer for DNP3	17
7.2	Recommended data link layer for IEC 60870-5-101 (1995-11).....	20
7.3	DNP3 pseudo-transport layer (ISO/OSI layer 4)	20
8.	Application layer definition (ISO/OSI layer 7)	21
8.1	Recommended application layer for DNP3	21
8.2	Recommended application layer for IEC 60870-5-101 (1995-11).....	25
9.	Definitions of data elements and objects	28
9.1	DNP3 data element/object definition	28
9.2	IEC 60870-5 data element definition	28
9.3	Comparative tables of defined objects and data elements	28

10. Process for addition of data elements/objects	31
10.1 Creation	31
10.2 Role of the DNP users group	31
Annex A (informative) Comparison of DNP3 and IEC 60870-5-101	32
Annex B (informative) Protocol implementation	38

IEEE Recommended Practice for Data Communications Between Remote Terminal Units and Intelligent Electronic Devices in a Substation

1. Overview

This recommended practice consists of descriptions and tabular information for implementation of common communication functions among intelligent electronic devices (IEDs) in electric utility substation applications.

1.1 Scope

This recommended practice presents a uniform set of guidelines for communications and interoperation of IEDs and remote terminal units (RTUs) in an electric utility substation. This recommended practice does not establish an underlying communication standard. Instead, it provides a specific limited subset of two existing communication protocols, to encourage understanding and timely application.

1.2 Purpose

The purpose of this standard is to illustrate a recommended practice that will eliminate the need for time-consuming and costly efforts by implementers to interface their equipment to other equipment on a project-by-project basis. It is assumed that implementers understand the basic concepts of RTU and IED communications, as well as the overall concept of the supervisory control and data acquisition (SCADA) system and its master station.

Two different protocols with many similarities are included in this recommended practice. Each is intended to satisfy the communication requirements between RTU-to-IED communications and also contain an adequate framework for most system applications. Both protocols are fully specified and cross-referenced so that users and developers can choose one or the other, based on the system or product application requirements.

1.3 Distributed network protocol (DNP3)

DNP3 is essentially a three-layer protocol using the layers 1, 2, and 7 of the ISO/OSI communications profile set. It is specifically designed for data acquisition and control applications, and focuses its application information in the area of electric utility data transmission. This recommended practice specifies the level 2 subset implementation of DNP3 as published.

DNP3 protocol was built on the framework specified by the IEC 60870-5 documents, and developed in response to market demands, including the need for early publication of a full protocol description that can be implemented in commonly available hardware. DNP3 is controlled by a DNP3 users group that includes a technical committee charged with reviewing problems, recommending enhancements, and updating the protocol documents.

1.4 IEC 60870-5 protocol

The IEC Technical Committee 57 Working Group 03 (TC57 WG03) was chartered to develop protocol standards for telecontrol, teleprotection, and associated telecommunications for electric utility systems, and it has created IEC 60870-5, a group of five utility-specific protocol standards. IEC 60870-5 specifies a number of links, frame formats, and services that may be provided at each of three layers. IEC 60870-5 uses the concept of a three-layer enhanced performance architecture (EPA) reference model for efficiency of implementation in devices such as RTUs, meters, relays, etc.

Additionally, IEC 60870-5 includes a user layer that is situated between the OSI application layer and the user's application program to add interoperability for such functions as clock synchronization and file transfers. Coded bit-serial data transmission is used to monitor and control geographically widespread processes.

IEC 60870-5-101 (1995-11) (hereinafter referred to as 101), is a companion standard (profile) that contains definitions specific to RTUs and IEDs.

Other companion standards that support the communications requirements for other utility devices are being defined, and are known as IEC 60870-5-102 (1996-06) (metering) and IEC 60870-5-103 (1997-12) (protection). Standard 103 includes parts of a protection device communication protocol originally developed for use in German protective relay systems and deals with the informative interface, exchanging only data that is not related to protection coordination.

2. References

This recommended practice is based on four sets of published documents that provide the basic definitions and underlying principles of the communication protocol. Each released document set is available from the sponsor for a nominal reproduction fee. This recommended practice should be used in conjunction with the following publications. When the following standards are superseded by an approved version, the new revision should apply.

DNP 3.0 Basic Four Document Set.¹

DNP V3.00 Subset Definitions.

DNP3-1999 Intelligent Electronic Device (IED) Certification Procedure Subset Level 2.

¹DNP publications are available from Secretary, DNP Users Group, c/o GE/Harris Canada, Inc., 4525 Manilla Rd. vS.E., Calgary, AB T2G4B6, Canada, fax (403) 243-1815.

IEC 60870-5-1 (1990-02), Telecontrol Equipment and Systems—Part 5: Transmission Protocols—Section 1: Transmission frame formats.²

IEC 60870-5-2 (1992-04), Telecontrol Equipment and Systems—Part 5: Transmission Protocols—Section 2: Link Transmission Procedures.

IEC 60870-5-3 (1992-09), Telecontrol Equipment and Systems—Part 5: Transmission Protocols—Section 3: General Structure of Application Data.

IEC 60870-5-4 (1993-08), Telecontrol Equipment and Systems—Part 5: Transmission Protocols—Section 4: Definition and Coding of Application Information Elements.

IEC 60870-5-5 (1995-06), Telecontrol Equipment and Systems—Part 5: Transmission Protocols—Section 5: Basic Application Functions.

IEC 60870-5-101 (1995-11), Telecontrol Equipment and Systems—Part 5: Transmission Protocols—Section 101: Companion Standard for Basic Telecontrol Tasks.

IEEE 100, *The Authoritative Dictionary of IEEE Standards Terms*, Seventh Edition.³

IEEE Std 1379-1997, IEEE Trial-Use Recommended Practice for Data Communications Between Intelligent Electronic Devices and Remote Terminal Units in a Substation.

IEEE Std C37.1-1994, IEEE Standard Definition, Specification, and Analysis of Systems Used for Supervisory Control, Data Acquisition, and Automatic Control.

ITU-T Recommendation V.24 (1996), List of definitions for interchange circuits between data terminal equipment (DTE) and data circuit-terminating equipment (DCE).⁴

ITU-T Recommendation V.28 (1993), Electrical Characteristics for unbalanced double-current interchange circuits.

ITU-T Recommendation X.24 (1996), List of definitions for interchange circuits between data terminal equipment (DTE) and data circuit-terminating equipment (DCE) on public data networks.

ITU-T Recommendation X.27 (1998), Electrical characteristics for balanced double-current interchange circuits operating at data signaling rates up to 10 Mbit/s.

3. Definitions, acronyms, and abbreviations

3.1 Definitions

The following definitions are for terms that are application specific to the DNP and IEC 60870-5 communication interface protocols. For the definition of other terms, consult the *The Authoritative Dictionary of IEEE*

²IEC publications are available from the Sales Department of the International Electrotechnical Commission, Case Postale 131, 3, rue de Varembe, CH-1211, Genève 20, Switzerland/Suisse (<http://www.iec.ch/>). IEC publications are also available in the United States from the Sales Department, American National Standards Institute, 11 West 42nd Street, 13th Floor, New York, NY 10036, USA.

³IEEE publications are available from the Institute of Electrical and Electronics Engineers, 445 Hoes Lane, P.O. Box 1331, Piscataway, NJ 08855-1331, USA (<http://standards.ieee.org/>).

⁴ITU-T publications are available from the International Telecommunications Union, Place des Nations, CH-1211, Geneva 20, Switzerland/Suisse (<http://www.itu.int/>).

Standards Terms, Seventh Edition. Users unfamiliar with SCADA terminology should also refer to IEEE Std C37.1-1994.

3.1.1 0x: A numerical prefix indicating that the number following is a hexadecimal number.

3.1.2 ACTTERM: A 60870-5-5 (1995-06) clause 6.8 command, the slave device message that a control action is complete (terminated).

3.1.3 application: A software program consisting of one or more processes and supporting functions.

3.1.4 ASCII (American Standard Code for Information Interchange): A seven-bit code that standardizes a set of characters representing letters and numbers for international use.

3.1.5 byte (B): A group of eight adjacent bits that function as a single unit. *See octet.*

3.1.6 char: The name of a data-type in the C programming language that stands for character, or a group of eight bits that function as a single unit.

3.1.7 C-SE: A 60870-5-101 (1995-11) setpoint (analog) command.

3.1.8 configure: To initialize a device so that it operates in a particular way. For instance, a customer may configure a device so the device never requests data link confirmations, using a variety of mechanisms (e.g., parameters in NVRAM, parameters in ROM, dip switches, or hardware jumpers).

3.1.9 configuration information: The data or information that defines the operational limits and characteristics of a particular device. Depending on the device, this information is either manually downloaded into nonvolatile random-access memory (NVRAM) or electronically erasable programmable read-only memory (EEPROM), or is preprogrammed into erasable programmable read-only memory (EPROM).

3.1.10 control direction: In 101, control direction is a transmission from the controlling station (master/RTU) to the controlled station (RTU/IED).

3.1.11 cyclic redundancy check (CRC): An error-detection scheme that checks the integrity of a transmitted message for errors introduced during transmission.

3.1.12 electronically erasable programmable read-only memory (EEPROM): A type of memory chip designed to be programmed more than once, supporting in-situ reprogrammability. The chips are functionally the same as erasable programmable read-only memories (EPROMs) but are erased using a particular electrical voltage.

3.1.13 erasable programmable read-only memory (EPROM): A type of memory chip designed to be programmed more than once, using special erasing procedures involving ultraviolet light. The processor can read but not alter the data, considered as permanent memory.

3.1.14 Hamming distance: The minimum number of incorrect bits that shall be received in order for a packet to be considered invalid. For example, the Hamming distance 4 means that all one-, two-, and three-bit errors are detectable.

3.1.15 host: The client or host station/computer, with which the RTU equipment communicates. *Syn:* **master.**

3.1.16 master: A device that initiates communications requests to gather data or perform controls.

3.1.17 master remote unit (MRU): An intelligent electronic device that acts as a data concentrator or master to other intelligent electronic devices. (That is, an MRU acquires data from and sends data to other intelligent electronic devices.) *Syn:* **submaster, remote master.**

3.1.18 monitor direction: In 101, refers to a transmission from the controlled station (RTU/IED) to the controlling station (master/RTU).

3.1.19 nonvolatile random-access memory (NVRAM): A semipermanent type of data storage (memory) that is backed up by batteries to maintain stored data even if system power is lost. Can be both read and changed by the system.

3.1.20 octet: 8-bit data object. *See:* **byte.**

3.1.21 parse: To resolve a request or response into component parts. In the context of messages, a device can break the message into pieces, each of which consists of a header and sometimes some corresponding data. If a device is able to parse a message, it can recognize each piece of a message. It does not necessarily make use of the data found in that message. However, it shall make any confirmation responses or other responses that the message requires.

3.1.22 port: An interface point connecting a communications channel and a device.

3.1.23 random-access memory (RAM): A type of temporary data storage (memory) that can be read and changed while the computer is in use. Data stored in random-access memory is lost if the system loses power.

3.1.24 read-only memory (ROM): A type of permanent data storage (memory) that can be read but not altered by the system. Data stored in read-only memory is not affected by power loss to the system.

3.1.25 remote terminal unit (RTU): A piece of equipment located at a distance from a master station to monitor and control the state of outlying power equipment and to communicate the information back to the master station or host.

3.1.26 report: The data objects/elements sent to a master device from slave devices. Used only in connection with slave devices. A slave device may parse requests for objects that it cannot generate or report.

3.1.27 slave: A device that gathers data or performs control operations in response to requests from the master and sends response messages in return. A slave device may also generate unsolicited responses.

3.1.28 source code: A piece of software that has not yet been compiled or assembled and appears in the language used by the programmer, and thus it cannot yet run on a machine.

3.1.29 submaster: *See:* **master remote unit.**

3.1.30 subremote unit (SRU): A physical device (for example, peripheral boards, RTUs, meters, or other intelligent electronic devices) that collects data, processes it in some way, and communicates it to an MRU. SRUs are able to respond to commands from MRUs. *Syn:* **slave units.**

3.1.31 telecontrol: *Syn:* **SCADA.**

3.1.32 trip/close: A type of digital output that stops or starts an action, usually affecting actual electric power circuits.

3.2 Acronyms and abbreviations

APCI	application protocol control information
APDU	application protocol data unit
ASDU	application service data unit
BCD	binary coded decimal
BS	bit string
CRC	cyclic redundancy check
CTO	common time of occurrence
DCE	data communication equipment
DFC	data flow control
DIR	direction of physical transmission
DNP	distributed network protocol
DPA	data processing application
DTE	data terminal equipment
EEPROM	electronically erasable programmable read-only memory
EPA	enhanced performance architecture (IEC)
EPROM	erasable programmable read-only memory
F	fixed point
FCB	frame control bit
FCV	frame count valid
I	integer
ID	identification
IED	intelligent electronic device
IIN	internal indications (DNP)
LAN	local area network
LPDU	link protocol data unit
LSDU	link service data unit
MRU	master remote unit
OSI	open system interconnection
PDU	protocol data unit
PSN	public switched network (telecommunications)
R	real
RESP	response
RTU	remote terminal unit
SCADA	supervisory control and data acquisition
SEQ	sequence number
UF	unsigned fixed point
UI	unsigned integer

4. Description of RTU-to-IED communications needs

The definition of a suitable substation communication protocol begins with an understanding of the technical basis for previous interdevice communication methods in the electric utility industry. The SCADA system is the most widely understood model for such communications. The functions of the RTU in the traditional SCADA protocol are well defined and not within the scope of this document. However, the capability for the RTU to communicate with increasing numbers and types of other intelligent devices in a substation is required by many users, hence the creation of RTU-to-IED communications requirements.

The substation IED may be a data acquisition device only or may have a primary function to provide control or protection. Therefore, the IED typically requires the input of configuration, setting, and command data, while it provides values, conditions, status, and results as output. Many of the data items are comparable to

SCADA data sent between the substation and master station. Therefore, the requirements of RTU-to-IED communications are very similar to SCADA communications, but on a local basis.

4.1 The traditional SCADA protocol

In a SCADA system, the RTU accepts commands to operate control points, set analog output levels, and responds to requests, and it provides status, analog, and accumulator data to the SCADA master station. The data representations sent are not identified in any fashion other than by absolute addressing. The addressing is designed to correlate with the SCADA master station database. The RTU has no knowledge of which unique parameters it is monitoring in the real world. It simply monitors certain points and stores the information in a local addressing scheme. The SCADA master station is the part of the system that should “know” that the first status point of RTU number 27 is the status of a certain circuit breaker of a given substation. This represents the predominant SCADA systems and protocols in use in the utility industry today.

Each protocol consists of two message sets or pairs. One set forms the master protocol, containing the valid statements for master station initiation or response, and the other set is the RTU protocol, containing the valid statements an RTU can initiate and respond to. In most but not all cases, these pairs can be considered a poll or request for information or action and a confirming response.

The SCADA protocol between master and RTU forms a viable model for RTU-to-IED communications, therefore, the DNP3 and 101 protocols in this recommended practice are SCADA-based protocols.

The basic function of SCADA systems, and their particular environmental conditions, also impose the following requirements for data transmission on RTU-to-IED communications:

- a) *Data security.* Correct data transmission is required in the presence of harsh environmental conditions such as electromagnetic interference, differences in earth potential, aging components, and other sources of disturbance and noise incident on the transmission path. It is necessary to provide protection of messages against undetected bit errors, undetected frame errors caused by synchronization errors, undetected loss of information, and/or gain of unintended information (i.e., simulation of valid messages by noise).
- b) *Efficient telecontrol transfer.* Efficient frame transmission protocols are needed for short information transfer times, particularly for event-initiated messages over a variety of transmission channels (e.g., twisted pair, fiber optics, radio) that have varying bandwidth and uncertain noise and interference characteristics.
- c) *Support of code transparent data transmission.* No code restrictions on user data should be imposed. The data link protocol should accept and transmit arbitrary bit sequence structures from the data source as in many cases the IED does not have extensive data processing power or memory.

4.2 Specific criteria used to select protocols for RTU/IED communication

A variety of RTUs and IEDs are already in use worldwide yielding a valuable experience base concerning the communications needed between these devices. Recognizing this, the following characteristics were determined to be important to successful communication interfacing between these devices. These formed a basis to compare candidate protocols for use in RTU/IED communications, with the understanding that no one protocol might meet all needs, and are provided in the following list:

- a) *Real time RTU/IED.* The protocol shall support direct RTU/IED communication without unnecessary delays but not necessarily peer-to-peer interoperability.
- b) *Existing protocol.* The protocol shall be fully developed and offered by a sponsor or fully described by a standards-making body.

- c) *Fully descriptive.* The protocol shall be uniquely identified by its name and support the minimum functions of data acquisition, control execution, time synchronization, accumulator control, and parameter downloading to IEDs.
- d) *Media independent.* The protocol shall be able to operate over physical layers of wire, coax, radio, and fiber optic media.
- e) *Addressable.* The protocol shall support multiple addresses of nodes and/or devices over a common channel.
- f) *Secure from errors.* The protocol shall provide a method of detection and either rejection or correction of corrupted messages.
- g) *Data selectable.* The protocol shall allow certain specified data to be requested and sent and not be restricted to a “poll-for-all-data” operation.
- h) *OSI model-compliant.* The protocol shall adhere to the layer structure of the OSI model for at least layers 1, 2, and 7. It should make maximum use of international/national standards wherever possible.
- i) *Documented.* The protocol shall be documented by at least a functional specification, data element/object definition, and three-layer definition.
- j) *Public domain.* The protocol shall be implementable by vendors and users without licensing fees or restrictions beyond a nominal fee for documentation that may be charged by the sponsor.
- k) *Easy-to-interface.* The protocol shall be implementable using an asynchronous serial port (UART like device) and be compatible with an 8-bit microprocessor using standard interface hardware/software.
- l) *Multiple sources of hardware.* Hardware needed to implement the protocol software shall be available from at least two independent vendors.
- m) *Local Area Network (LAN).* The protocol shall operate over a common communications channel for all substation devices. It is not restricted to point-to-point communication. The protocol should tolerate node/device failure on the common network.

5. Recommended practice for RTU/IED communication

The use of standardized protocols for information exchange requires that the information be identified in a specific manner and both communicating units must use the same formatting of messages.

By following the details given in this recommended practice, the user can have a reasonable confidence level that two substation devices, nominally an RTU and an IED, can exchange information, and that the transfer will occur without additional programming or custom configuration.

5.1 General application practice using DNP3

The DNP3 is specifically developed for interdevice communication involving SCADA RTUs, and provides for both RTU-to-IED and master-to-RTU/IED. It is based on the three-layer enhanced performance architecture (EPA) model contained in the IEC 60870-5 standards, with some alterations to meet additional requirements of a variety of users in the electric utility industry.

DNP3 was developed with the following goals:

- a) *High data integrity.* The DNP3 data link layer uses a variation of the IEC 60870-5-1 (1990-02) frame format FT3. Both data link layer frames and application layer messages may be transmitted using confirmed service.

- b) *Flexible structure.* The DNP3 application layer is object-based, with a structure that allows a range of implementations while retaining interoperability.
- c) *Multiple applications.* DNP3 can be used in several modes, including
 - 1) Polled only,
 - 2) Polled report-by-exception,
 - 3) Unsolicited report-by-exception (quiescent mode), and
 - 4) Mixture of modes 1) through 3).

It can also be used with several physical layers, and as a layered protocol is suitable for operation over local and some wide area networks.
- d) *Minimized overhead.* DNP3 was designed for existing wire-pair data links with operating bit rates as low as 1200 bit/s and attempts to use a minimum of overhead while retaining flexibility. Selection of a data reporting method, such as report-by-exception, further reduces overhead.
- e) *Open standard.* DNP3 is a nonproprietary, evolving standard controlled by a users group whose members include RTU, IED, and master station vendors, and representatives of the electric utility and system consulting community.

5.1.1 Data link layer

The DNP3 data link layer specification describes the frame format, services, responsibilities, and transmission procedures for the data link layer. It describes the required services to be provided by a DNP3 physical layer. DNP3 is essentially media-independent when the physical layer interface meets these requirements. For instance, if unsolicited messaging is used, the physical layer should provide an indication of whether the link is busy, which is necessary for collision avoidance. The DNP3 data link layer specification also relates the DNP3 data link layer to IEC 60870-5-1 (1990-02) and IEC 60870-5-2 (1992-04) standards. The primary difference is that DNP3 uses the FT3 frame format for asynchronous, rather than synchronous, transmission. DNP3 also adapts the IEC 60870-5 addressing to include both a source and destination address in the frame. This addition enables the use of multiple master stations and peer-to-peer communications using DNP3.

5.1.2 Transport functions

The DNP3 transport functions specification describes the format and procedures associated with a single octet of overhead used to segment application layer messages into data link layer frames. These transport functions are not a complete transport layer, nor part of the data link or application layer overhead. For more discussion of the pseudo-transport layer, refer to 7.3.

5.1.3 Application layer

The DNP3 application layer specification describes the message format, services, and procedures for the application layer. The services and functions provided are based on the basic application functions described in IEC 60870-5-5 (1995-06) documentation, although the terminology used to describe these functions differs. Distinctive DNP3 features include the following:

- a) 16-bit device addresses
- b) 8-, 16-, or 32-bit point addresses of each data type per device
- c) Broadcast addressing
- d) Configuration and file transfer
- e) Time of day and date synchronization
- f) Time-stamped event data
- g) Polling by data priority level

- h) Support for all common industry data types including binary input and output (controls), analog input and output (setpoints), counters/accumulators, binary coded decimal (BCD), and IEEE floating point (the latter two are optional data formats)
- i) Freezing and clearing counters
- j) Solicited or unsolicited reporting of exceptions such as buffer overflow, device restarted, device trouble, device in local operation mode, time synchronization required, invalid message, point on-line/off-line, analog point over-range, counter point overflow, downstream communications lost
- k) A variety of reporting mechanisms, as discussed in a) through j)
- l) A variety of control operations, including select-before-operate, direct with/without acknowledge operate, trip/close, latch on/off, pulse on/off, automatic repetition, binary output patterns, and more
- m) Remote starting/stopping of software applications (not currently addressed in this recommended practice)

5.1.4 Data object library

The DNP3 data object library document describes the format of data presented within an application layer message. A variety of qualifier codes and variations of data permit an implementation of DNP3 to make optimal use of bandwidth. DNP objects are not general-purpose objects; they are defined specifically for SCADA operation.

5.1.5 Subset definitions

The DNP3 subset definition document describes three basic levels of DNP3 objects and services that can be used to determine interoperability between devices or to specify a minimum required level of implementation in a request for proposals. The intended use of these subsets is as follows:

Level 1 (L1): a minimum implementation, intended for a simple IED

Level 2 (L2): includes L1 definitions, intended for a more sophisticated IED or a small RTU

Level 3 (L3): includes L1 and L2 definitions, intended for a larger RTU or data concentrator

To conform to a given subset, a device should act in the following ways:

- a) Be able to parse a given set of incoming messages
- b) Be configurable to transmit only a given set of outgoing messages
- c) Obey implementation rules specified in the DNP3 subset definitions
- d) Be described by a published DNP3 device profile document

This recommended practice defines a subset of the DNP3 standard corresponding to level 2 (L2) of the DNP3 subset definitions. To follow this recommended practice, the device should conform to the subset L2. Note that the subsets represent a minimum implementation. Nothing prevents a pair of devices from using features not defined in the subset, provided that the following is true:

- a) The features are valid for DNP3 as defined in the DNP 3.0 “Basic Four” document set.
- b) The vendors agree on the protocol features being used both devices.
- c) The unique devices can disable these features when communicating with other devices.

5.2 General application practice using IEC-60870-5 standards

The IEC 60870-5 standards address the basic goals of telecontrol systems and their particular environmental conditions, as summarized in Clause 4.

IEC 60870-5 specifies a number of frame formats and services that may be provided at different layers. IEC 60870-5 is based on a three-layer EPA reference model for efficient implementation within RTUs, meters, relays, and other IEDs. Additionally, IEC 60870-5 defines basic application functionality for a user layer, which is situated between the OSI application layer and the application program. This user layer adds interoperability for such functions as clock synchronization and file transfers. The following descriptions provide the basic scope of each of the five documents in the base IEC 60870-5 telecontrol transmission protocol specification set.

Standard profiles are necessary for uniform application of the IEC 60870-5 standards. Such profiles have been and are being created. The 101 profile is described in detail following the description of the applicable standards.

- IEC 60870-5-1 (1990-02) specifies the basic requirements for services to be provided by the data link and physical layers for telecontrol applications. In particular, it specifies standards on coding, formatting, and synchronizing data frames of variable and fixed lengths that meet specified data integrity requirements.
- IEC-60870-5-2 (1992-04) offers a selection of link transmission procedures using a control field and optional address field; the address field is optional because some point-to-point topologies do not require either source or destination addressing.
- IEC 60870-5-3 (1992-09) specifies rules for structuring application data units in transmission frames of telecontrol systems. These rules are presented as generic standards that may be used to support a great variety of present and future telecontrol applications. This section of IEC 60870-5 describes the general structure of application data and basic rules to specify application data units without specifying details about information fields and their contents.
- IEC 60870-5-4 (1993-08) provides rules for defining information data elements and a common set of information elements, particularly digital and analog process variables that are frequently used in telecontrol applications.
- IEC 60870-5-5 (1995-06) defines basic application functions that perform standard procedures for telecontrol systems, which are procedures that reside beyond layer 7 (application layer) of the ISO reference model. These utilize standard services of the application layer. The specifications in IEC 60870-5-5 (1995-06) serve as basic standards for application profiles that are then created in detail for specific telecontrol tasks.

Each application profile will use a specific selection of the defined functions. Any basic application functions not found in a standards document but necessary for defining certain telecontrol applications should be specified within the profile. Examples of such telecontrol functions include station initialization, cyclic data transmission, data acquisition by polling, clock synchronization, and station configuration.

5.3 Functionality of the 101 companion standard profile

This recommended practice specifically incorporates the 101 profile. IEC 60870-5-101(1995-11) (101) is a companion standard generated by the IEC TC57 for electric utility communication between master stations and RTUs. Like DNP3, 101 provides structures that are also directly applicable to the interface between RTUs and IEDs. It contains all the elements of a protocol necessary to provide an unambiguous profile definition so vendors may create products that interoperate fully.

At the physical layer, 101 additionally allows the selection of ITU-T (formerly CCITT) standards that are compatible with EIA standards RS-232 and RS-485, and also support fiber optics interfaces.

Standard 101 specifies frame format FT 1.2, chosen from those offered in IEC 60870-5-1 (1990-02) to provide the required data integrity together with the maximum efficiency available for acceptable convenience of implementation. FT 1.2 is basically asynchronous and can be implemented using standard universal asynchronous receiver/transmitters (UARTs). Formats with both fixed and variable block length are admitted. Also, the single control character I transmission is allowed.

At the data link layer, 101 specifies whether an unbalanced (include multidrop) or balanced (includes point-to-point) transmission mode is used together with which link procedures (and corresponding link function codes) are to be used. Also specified is an unambiguous number (address) for each link.

The link transmission procedures selected from IEC 60870-5-2 (1992-04) specify that SEND/NO REPLY, SEND/CONFIRM, and REQUEST/RESPOND message transactions should be supported as necessary for the functionality of the end device. Additionally, 101 defines the necessary rules for devices that will operate in the unbalanced (multidrop) and balanced (point-to-point) transmission modes.

Standard 101 defines appropriate application service data units (ASDUs) from a given general structure in IEC 60870-5-3 (1992-09). The sizes and the contents of individual information fields of ASDUs are specified according to the declaration rules for information elements defined in the document IEC 60870-5-4 (1993-08).

Type information defines structure, type, and format for information object(s), and a set has been predefined for a number of information objects. The predefined information elements and type information do not preclude the addition by vendors of new information elements and types that follow the rules defined by IEC 60870-5-4 (1993-08) and 101. Information elements in the 101 profile have been defined for protection equipment, voltage regulators, and metered values to interface these devices as IEDs to the RTU.

Standard 101 utilizes the following basic application functions, defined in IEC 60870-5-5 (1995-06), within the user layer:

- a) Station initialization
- b) Cyclic data transmission
- c) General interrogation
- d) Command transmission
- e) Data acquisition by polling
- f) Acquisition of events
- g) Parameter loading
- h) File transfer
- i) Clock synchronization
- j) Transmission of integrated totals
- k) Test procedure

Finally, 101 defines a mechanism for interoperability within a particular system. It is recognized that the companion standard defines parameters and alternatives from which subsets are chosen to implement particular telecontrol systems. Certain parameter values such as the number of bytes in the common address of ASDUs represent mutually exclusive alternatives because only one value is allowed per system. Other parameters, such as the process information elements listed in the command and monitor directions, allow the specification of either the complete set or subsets, as appropriate for an application.