

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

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

Approved 16 September 1997
IEEE Standards Board

Abstract: A uniform set of guidelines for communications and interoperations of Intelligent Electronic Devices (IEDs) and Remote Terminal Units (RTUs) 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 Engineers, Inc.

345 East 47th Street, New York, NY 10017-2394, USA

Copyright © 1998 by the Institute of Electrical and Electronics Engineers, Inc.

All rights reserved. Published 1997. Printed in the United States of America.

ISBN 1-55937-982-0

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 Technical Committees of the IEEE Societies and the Standards Coordinating Committees of the IEEE Standards Board. Members of the committees serve voluntarily and without compensation. They are not necessarily members of the Institute. The standards developed within IEEE represent a consensus of the broad expertise on the subject within the Institute as well as those activities outside of IEEE which have expressed an interest in participating in the development of the standard.

Use of an IEEE Standard is wholly voluntary. The existence of an IEEE Standard does not imply that there are no other ways to produce, test, measure, purchase, market, or provide other goods and services related to the scope of the IEEE Standard. Furthermore, the viewpoint expressed at the time a standard is approved and issued is subject to change brought about through developments in the state of the art and comments received from users of the standard. Every IEEE Standard is subjected to review at least once 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.

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.

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 all 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 technical 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 on standards and requests for interpretations should be addressed to:

Secretary, IEEE Standards Board
345 East 47th Street
New York, NY 10017
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.

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; (508) 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 1379-1997, IEEE Trial-Use Recommended Practice for Data Communications Between Intelligent Electronic Devices and Remote Terminal Units in a Substation.)

This trial-use recommended practice presents a uniform set of guidelines for specific interdevice communication details which can permit interoperation of Intelligent Electronic Devices (IEDs) and Remote Terminal Units (RTUs) in an electric utility substation. The data definitions and message structure can be used by product developers of both IEDs and RTUs to create nonproprietary interfaces, and by buyers and specifiers as a definition or reference document for data representation and transmission.

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. This trial-use recommended practice is the result of that decision.

This recommended practice does not establish an underlying communication standard. To quickly achieve industry acceptance and use, it instead provides a specific implementation of two existing communication protocols which are in the public domain (all documentation is or will be 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 as well, 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.

Publication of this trial-use standard for comment and criticism has been approved by the Institute of Electrical and Electronics Engineers. Trial-use standards are effective for 24 months from the date of publication. Comments for revision will be accepted for 18 months after publication. Suggestions for revision should be directed to the Secretary, IEEE Standards Board, 445 Hoes Lane, P.O. Box 1331, Piscataway, NJ 08855-1331, and should be received no later than 20 August 1999. It is expected that following the 24-month period, this trial-use standard, revised as necessary, shall be submitted to the IEEE Standards Board for approval as a full-use standard.

At the time this trial-use recommended practice was developed, the working group had the following membership:

Ken Jackson, Chair
John T. Tengdin, Vice Chair

William J. Ackerman
Mark Adamiak
Lawrence A. Barto
George J. Bartok
Donald Berkowitz
Hans Bjorklund
Wayne R. Block
Dennis L. Carr
William J. Cheetham
Larry Clark
Mason Clark
Richard Clark
Ken Cooley
John W. Dean
Michael Dood
Randall Ehlers
James W. Evans
Ron J. Farquharson
Thomas E. Gasparich
Floyd W. Greenway

Daniel Gregory
Glenn Harmon
G. Roger Jensen
Danny L. Johnson
Rick Joyce
Mark J. Kempker
Stanley Klein
Roderic L. Kreger
Terry L. Krummrey
Carl J. LaPlace, Jr.
Kenneth E. Lindler
Gregory L. Luri
Sioe Mak
John D. McDonald
Jeff McElray
Harish I. Mehta
Gary Michel
Gary Moore
John Newbury

Dan Nordell
Wally Prystajacky
Gregory M. Robinson
Clarence J. Sasso
Terry Saxton
George Schimmel
Russ Schoetker
Samuel C. Sciacca
Allen R. Skopp
H. Lee Smith
Robert C. Sodergren
Stanley R. Sykes
Norman Tweed
Eric Udren
Tony Watson
James A. Whatley
Joe N. Wilson
Peter S. Wong
Ray Wright
Walt Yeager

The following persons were on the balloting committee:

William J. Ackerman
Alexander P. Apostolov
Lawrence A. Barto
George J. Bartok
Michael J. Bio
Wayne R. Block
James C. Burke
Dennis L. Carr
William J. Cheetham
Frank Y. Chu
Ken L. Cooley
Robert Corlew
James G. Cupp
John W. Dean
W. Bruce Dietzman

Michael Dood
Gary R. Engmann
James W. Evans
Ron J. Farquharson
Floyd W. Greenway
Daniel C. Gregory
R. J. Hellweg
Kenneth Jackson
Danny L. Johnson
Alan E. Kollar
Roderic L. Kreger
Terry L. Krummrey
Luther W. Kurtz
Carl J. LaPlace, Jr.
H. Peter Lips

John D. McDonald
Gary L. Michel
Philip R. Nannery
James S. Oswald
Gregory M. Robinson
Samuel C. Sciacca
June Singletary, Jr.
Allen R. Skopp
H. Lee Smith
Robert C. Sodergren
Charles V. Stoll
Stanley R. Sykes
John T. Tengdin
Mark Vainberg
Tony Watson

When the IEEE Standards Board approved this trial-use recommended practice on 16 September 1997, it had the following membership:

Donald C. Loughry, *Chair*
Richard J. Holleman, *Vice Chair*
Andrew G. Salem, *Secretary*

Clyde R. Camp
Stephen L. Diamond
Harold E. Epstein
Donald C. Fleckenstein
Jay Forster*
Thomas F. Garrity
Donald N. Heirman
Jim Isaak

Ben C. Johnson
Lowell Johnson
Robert Kennelly
E. G. “Al” Kiener
Joseph L. Koepfinger*
Stephen R. Lambert
Lawrence V. McCall
L. Bruce McClung
Marco W. Migliaro

Louis-François Pau
Gerald H. Peterson
John W. Pope
Jose R. Ramos
Ronald H. Reimer
Ingo Rüsch
John S. Ryan
Chee Kiow Tan
Howard L. Wolfman

*Member Emeritus

Also included are the following nonvoting IEEE Standards Board liaisons:

Satish K. Aggarwal

Alan H. Cookson

Lisa S. Young, *IEEE Standards Project Editor*

CLAUSE	PAGE
1. Overview	1
1.1 Scope.....	1
1.2 Purpose.....	1
1.3 Distributed Network Protocol (DNP) 3.0	1
1.4 IEC 60870-5 protocol.....	2
2. References.....	2
2.1 DNP 3.0 Documents	2
2.2 IEC 60870-5 publications	3
3. Definitions.....	3
3.1 Specific DNP/IEC 60870-5 terms.....	3
3.2 Acronyms and abbreviations.....	5
4. Description of IED-to-RTU communications needs.....	6
4.1 The traditional SCADA protocol	6
4.2 Specific criteria to select protocols for IED/RTU communication.....	7
5. Recommended practice for IED/RTU communication.....	8
5.1 General application practice using DNP 3.0.....	8
5.2 General application practice using IEC-60870-5 standards.....	10
5.3 Functionality of the T101 companion standard profile.....	11
5.4 Summary comparative description tables	12
6. Physical layer definition (ISO/OSI Layer 1).....	15
6.1 Modes of transmission	16
6.2 Local loop	16
6.3 Recommended physical layer for DNP 3.0.....	16
6.4 Recommended physical layers for IEC 60870-5-101 (1995)	16
7. Data link layer definition (ISO/OSI Layer 2)	17
7.1 Recommended data link layer for DNP 3.0	17
7.2 Recommended data link layer for IEC 60870-5-T101.....	19
7.3 DNP 3.0 Pseudo-transport layer (ISO/OSI Layer 4).....	20
8. Application layer definition (ISO/OSI Layer 7)	20
8.1 Recommended application layer for DNP 3.0	20
8.2 Recommended application layer for IEC 60870-5-T101 (1995).....	24
9. Definitions of data elements and objects	27
9.1 DNP 3.0 data element/object definition.....	27
9.2 IEC 60870-5 data element definition	27
9.3 Comparative tables of defined objects and data elements	27

CLAUSE	PAGE
10. Protocol implementations	29
10.1 DNP 3.0 implementation	29
10.2 DNP 3.0 implementation examples	34
10.3 IEC-60870-5-101 Implementation	39
10.4 T101 implementation example.....	40
10.5 IEC 60870-5-T101 Example vendor device implementation	41
11. Process for addition of data elements/objects	45
11.1 Creation	45
11.2 Registration	45
11.3 Role of the DNP Users' Group	45
Annex A (informative) Comparison of DNP and IEC 60870-5-101	46
Annex B (informative) Bibliography	58

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

1. Overview

This trial-use 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 recommended practice that will eliminate the need for time-consuming and costly efforts by implementors to interface their equipment to other equipment on a project-by-project basis. It is assumed that implementors understand the basic concepts of IED and RTU 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 between them are included in this trial-use recommended practice. Each is intended for application to the IED-to-RTU communications requirements, and contains 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 requirements of a system or product application.

1.3 Distributed Network Protocol (DNP) 3.0

The DNP protocol was developed by Harris Canada (formerly Westronic, Inc.) in order to stabilize the expansion of unique protocols used to communicate between SCADA RTUs and a variety of IEDs. The DNP protocol used as its

basis several IEC 60870-5 documents that were then in development; but extended and/or modified these to accommodate North American preferences and practices.¹ Work has been done to harmonize the IEC 60870-5 documents, which were later made International Standards, with the DNP variations, but this has not been completed.

DNP 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 DNP 3.0 as published.

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, similar to the EPRI/UCA specification. 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.

Another document developed by IEC TC57 WG03 is IEC 60870-5-101 (hereinafter referred to as T101), 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 (T102) and IEC 60870-5-103 (T103). The draft T103 (as presently proposed) includes parts of a protection device communication protocol originally developed for use in German protective relay systems. T103 deals with the informative interface, exchanging only data that is not related to protection coordination. The preliminary version of T103 has received endorsement by users and vendors in the United Kingdom, Spain, and Germany.

2. References

This recommended practice is based on two 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 shall be used in conjunction with the following publications.

Users and developers should avail themselves of the most recent versions of the complete documents, which describe in detail the protocols referenced by this recommended practice. Some extracts that are relevant to the IED/RTU application are reproduced with permission in Annex A.

2.1 DNP 3.0 Documents

The following documents are essential to the application of DNP 3.0:²

- a) DNP 3.0 Protocol Functions Specification Set—"The Basic Four"
- b) DNP 3.0 Recommended Protocol Subset

¹Information on references can be found in Clause 2..

²DNP publications are available from Secretary, DNP User Group, c/o Harris Canada, Inc., 4525 Manilla Rd. S.E., Calgary, AB T2G 4B6, Canada, fax (403) 243-1815.

2.2 IEC 60870-5 publications

The following publications are essential to the application of T101:³

IEC 60870-5-1 (1990), Telecontrol equipment and systems—Part 5: Transmission protocols—Section 1: Transmission frame formats.

IEC 60870-5-2 (1992), Telecontrol equipment and systems—Part 5: Transmission protocols—Section 2: Link transmission procedures.

IEC 60870-5-3 (1992), Telecontrol equipment and systems—Part 5: Transmission protocols—Section 3: General structure of application data.

IEC 60870-5-4 (1993), Telecontrol equipment and systems—Part 5: Transmission protocols—Section 4: Definition and coding of application information elements.

IEC 60870-5-5 (1995), Telecontrol equipment and systems—Part 5: Transmission protocols—Section 5: Basic application functions.

IEC 60870-5-101 (1995), Telecontrol equipment and systems—Part 5: Transmission protocols—Section 101: Companion Standard for Basic Telecontrol Tasks.

IEEE Std 100-1996, IEEE Standard Dictionary of Electrical and Electronics Terms.⁴

3. Definitions

The following definitions are for terms that are specific in their application to the DNP and IEC 60870-5 communication interface protocols. For the definition of other terms, IEEE Std 100-1996 shall apply. Users unfamiliar with SCADA terminology should also refer to IEEE Std C37.1-1994 [B3].⁵

3.1 Specific DNP/IEC 60870-5 terms

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

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

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

3.1.4 byte: A group of eight adjacent bits that function as a single unit. *See* **octet**.

3.1.5 change of state (COS): A significant change (as defined by a particular system) in the condition of a point being monitored, for example, a change in flow rate, temperature, voltage, etc. Usually associated with dual-status (that is, alarm/normal conditions).

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.

³IEC publications are available from IEC Sales Department, Case Postale 131, 3, rue de Varembe, CH-1211, Genève 20, Switzerland/Suisse. 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.

⁴IEEE publications are available from the Institute of Electrical and Electronics Engineers, 445 Hoes Lane, P.O. Box 1331, Piscataway, NJ 08855-1331, USA.

⁵The numbers in brackets correspond to those of the bibliography in Annex B.

3.1.7 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).

3.1.8 control direction: In T101, control direction is transmission from the controlling station (master/RTU) to the controlled station (RTU/IED).

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 NVRAM or EEPROM, or is pre-programmed into EPROM.

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

3.1.11 data-collection application (DCA): A software application that acquires data from and sends data to various intelligent electronic devices.

3.1.12 EEPROM: See **electronically erasable programmable read-only memory**.

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

3.1.14 EPROM: See **erasable programmable read-only memory**.

3.1.15 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 only read but not alter the data, considered as permanent memory.

3.1.16 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.

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

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

3.1.19 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.

3.1.20 monitor direction: In T101, refers to transmission from the controlled station (RTU/IED) to the controlling station (master/RTU).

3.1.21 non-volatile random-access memory (NVRAM): A semi-permanent 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.

3.1.22 NUL: The null character ('\0').

3.1.23 octet: 8 b data object. See: **byte**.

3.1.24 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.

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

3.1.26 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.

3.1.27 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.

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

3.1.29 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.

3.1.30 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 (DNP 3.0 specific).

3.1.31 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 cannot yet run on a machine.

3.1.32 submaster: *See: master remote unit.*

3.1.33 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.

3.1.34 telecontrol: *Syn:* SCADA.

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

3.2 Acronyms and abbreviations

AC	application control
APCI	application protocol control information
APDU	application protocol data unit
APSDU	application service data unit
API	application program interface
BCD	binary coded decimal
BS	bit string
CTO	common time object
CTO	common time of occurrence
CWD	change working directory
DA	distribution automation
DC	data concentrator
DCA	data collection application
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
DUI	data unit identifiers
EPA	enhanced performance architecture (IEC)
EBCDIC	extended binary coded decimal interchange code
EXEC	execute
F	fixed point
FCB	frame control bit
FCV	frame count valid
FIFO	first-in-first-out
I	integer
ID	identification
IEC	International Electrotechnical Commission
IED	intelligent electronic device
IIN	internal indications (DNP)
IO	information objects

ISO	International Standards Organization
ITU	International Telecommunication Union
LEN	length
LPBCD	large-packed binary coded decimal
LPDU	link protocol data unit
LSDU	link service data unit
MMSM	manufacturing Messaging Specification
MPBCD	medium-packed binary coded decimal
OS	octet string
OSI	Open System Interconnection
PCB	pattern control block
PDU	protocol data unit
PRM	primary
PRN	private registration number
PRO	private registration object
PROD	private registration object description
PSN	public switched network (telecommunications)
PWD	(return to) present working directory
R	real
RESP	response
SEQ	sequence number
SPBCD	small-packed binary coded decimal
UF	unsigned fixed point
UI	unsigned integer

4. Description of IED-to-RTU communications needs

The definition of a suitable substation communication protocol could not begin without 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 RTU function in the traditional SCADA protocol is well defined and not within the scope of this document [B3] [B4]. However, the capability of 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 IED-to-RTU communications requirements.

The substation IED may be a data acquisition device only, or may also 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. Much of these data items are comparable to SCADA data sent between the substation and master station. The goals of IED-to-RTU 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 provide responses; in turn, it sends 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 a database contained in the SCADA master station, and 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 IED-to-RTU communications, therefore, the DNP 3.0 and IEC 60870-5-T101 (1995) 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 IED-to-RTU communications:

- a) *Data security*: Correct data transmission is required in the presence of harsh environmental conditions such as electromagnetic interferences, 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 shall 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 to select protocols for IED/RTU communication

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

- a) *Real time IED/RTU*: The protocol shall support direct IED/RTU 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 reject or correct corrupted messages, using "Cyclic Redundancy Check" or better error detection/correction.
- 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 3-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 b 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) *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.
- n) *UCA-compliant*: The protocol shall have a migration path to EPRI/UCA harmonization.

5. Recommended practice for IED/RTU communication

The use of standardized protocols for information exchange requires that the information be identified in a specific manner; both communicating units shall 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 IED and RTU, can exchange information, and that the transfer will occur without additional programming or custom configuration.

5.1 General application practice using DNP 3.0

The DNP 3.0 is specifically developed for interdevice communication involving SCADA RTUs, and provides for both IED-to-RTU and master-to-IED/RTU. 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.

DNP 3.0 was developed with the following goals:

- a) *High data integrity*: The DNP 3.0 Data Link Layer uses a variation of the IEC 60870-5-1 (1990) frame format FT3. Both data link layer frames and application layer messages may be transmitted using confirmed service.
- b) *Flexible structure*: The DNP 3.0 Application Layer is object-based, with a structure that allows a range of implementations while retaining interoperability.
- c) *Multiple applications*: DNP 3.0 can be used in several modes, including:
 - 1) Polled only;
 - 2) Polled report-by-exception;
 - 3) Unsolicited report-by-exception (quiescent mode);
 - 4) Mixture of the modes 1)– 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*: DNP 3.0 was designed for existing wire-pair data links, with operating bit rates as low as 1200 b/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*: DNP 3.0 is a non-proprietary, 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 DNP V3.00 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 DNP 3.0 physical layer. DNP 3.0 is essentially media-independent when the physical layer interface meets these requirements. For instance, if unsolicited messaging is used, the physical layer shall provide an indication of whether the link is busy, which is necessary for collision avoidance. The DNP V3.00 data link layer specification also relates the DNP 3.0 data link layer to IEC 60870-5-1 (1990) and IEC 60870-5-2 (1992) standards. The primary difference is that DNP 3.0 uses the FT3

frame format for asynchronous, rather than synchronous, transmission. DNP 3.0 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 DNP 3.0.

5.1.2 Transport functions

The DNP V3.00 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 proper 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 DNP V3.00 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) documentation, although the terminology used to describe these functions differs. Distinctive DNP 3.0 features include the following:

- a) 16 b device addresses;
- b) 32 b point addresses of each data type per device;
- c) Broadcast addressing;
- d) Configuration and file transfer (not currently in this trial-use recommended practice);
- 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, BCD, and IEEE floating point (the latter two are not currently addressed in this recommended practice);
- 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/immediate-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 DNP V3.00 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 DNP 3.0 to make optimal use of bandwidth. DNP objects are not general-purpose objects; they are defined specifically for RTU operation.

5.1.5 Subset definitions

The DNP V3.00 subset definitions document describes three basic levels of DNP 3.0 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): Intended for a more sophisticated IED or a small RTU;

Level 3 (3): Intended for a larger RTU or data concentrator.

These subset definitions ensure interoperability while allowing vendors to competitively provide value-added features to a minimum subset of the protocol. To conform to a given subset, a device must 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 DNP V3.00 subset definitions;
- d) Be described by a published DNP 3.0 device profile document.

This recommended practice defines a subset of the DNP 3.0 standard corresponding to Level 2 (L2) of the DNP V3.00 Subset Definitions. To follow this recommended practice, the device shall 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:

- 1) The features are valid for DNP V3.00 as defined in the DNP V3.00 “Basic Four”;
- 2) Both devices agree on the features being used;
- 3) Both devices can disable these features when communicating with other devices.

A copy of the DNP 3.0 device profile document format and instructions are included in Annex AA. It is recommended that implementors use and exchange the profile to ensure compatibility.

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 does not define one particular protocol profile; but rather like EPRI/UCA, it specifies a number of frame formats and services that may be provided at different layers. IEC 60870-5 is based on a three-layer Enhanced Performance Architecture (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 T101 profile is described in detail following the description of the applicable standards.

- IEC 60870-5-1 (1990) 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) 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) 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 describes basic rules to specify application data units without specifying details about information fields and their contents.
- IEC 60870-5-4 (1993) 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) 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) 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, cycle data transmission, data acquisition by polling, clock synchronization, and station configuration.

5.3 Functionality of the T101 companion standard profile

This recommended practice specifically incorporates the T101 profile. IEC 60870-5-101 (T101) is a companion standard generated by the IEC TC57 for electric utility communication between master stations and RTUs. Like DNP 3.0, T101 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 that vendors may create products that interoperate fully.

At the physical layer, T101 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.

T101 specifies frame format FT 1.2, chosen from those offered in IEC 60870-5-1 (1990) 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, T101 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) specify that SEND/NO REPLY, SEND/CONFIRM, and REQUEST/RESPOND message transactions shall be supported as necessary for the functionality of the end device. Additionally, T101 defines the necessary rules for devices that will operate in the unbalanced (multidrop) and balanced (point-to-point) transmission modes.

T101 defines appropriate application service data units (ASDUs) from a given general structure in IEC 60870-5-3 (1992). 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). 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) and T101. Information elements in the T101 profile have been defined for protection equipment, voltage regulators, and for metered values, to interface these devices as IEDs to the RTU.

T101 utilizes the following basic application functions, defined in IEC 60870-5-5 (1995), within the user layer:

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

Finally, T101 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.

As a guide for achieving interoperability within a system, T101 provides a checklist that a vendor can use to describe a device from a protocol perspective. Wherever choices can be made, such as baud rate, common address of ASDU field length, link transmission procedure, basic application functions, etc., there is a list that can be checked off, indicating the subset of supported services. Also contained in the checkoff list is the information which may be contained in the ASDU in both the control and monitor directions.

The T101 Application layer specifies the structure of the ASDU, as shown in Figure 1. The fields that are indicated as being optional per system will be determined by a system level parameter shared by all devices in the system. For instance, the size of the common address of ASDU is determined by a fixed system parameter, in this case one or two octets (bytes).

T101 also defines two new terms not found in the IEC 60870-5-1 through -5 base documents. The control direction refers to transmission from the controlling station to a controlled station. The monitor direction is the direction of transmission from a controlled station to the controlling station.

5.4 Summary comparative description tables

Tables 1 and 2 are provided to summarize the salient features of the two protocols in this recommended practice, and are self-explanatory.

There are other protocol development and standards-making efforts with a similar purpose being conducted at the time this document was written. Work done under the EPRI RP-3599 integrated protection project and the EPRI MRP protocol development project (“Oglethorpe”) has been sponsored for consideration by the relevant IEC technical committees, and is therefore included in tables located in Annex A as Tables A.1 and A.2 to provide further user reference and comparison.

Table 2 presents information on functions and/or messages which are applicable to the IED/RTU communication functions, using a common name to relate similar operations in each of the implementations.

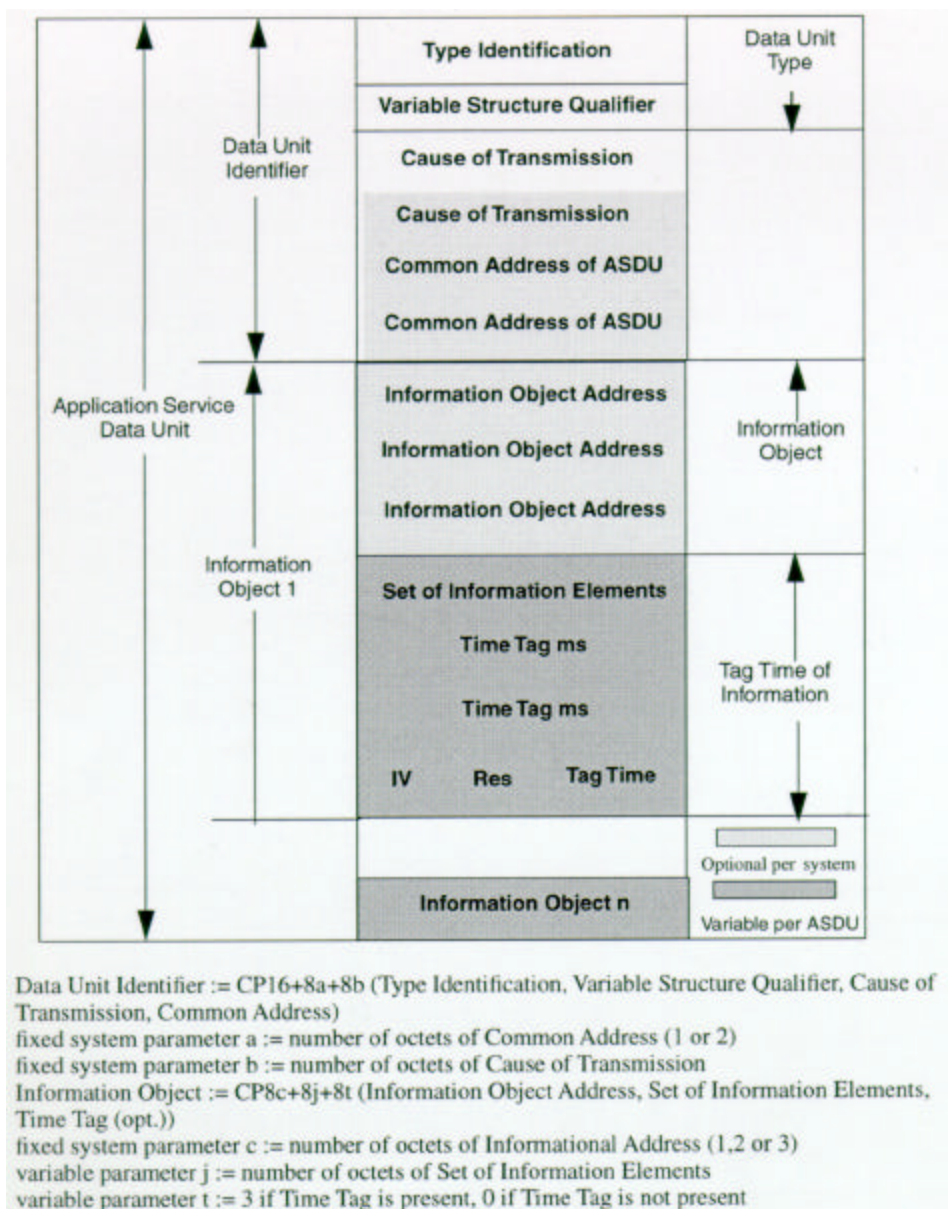


Figure 1— Structure of ASDUs in IEC 60870-5-101