IEEE Std 1379-2000
(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

Approved 21 September 2000

IEEE-SA Standards Board

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

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

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.

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	Grant Gilcrest	H. Lee Smith
Alexander Apostolov	Ameen Hamdon	Robert C. Sodergren
Wayne R. Block	Derick Hammond	John T. Tengdin
Ken L. Cooley	Dennis K. Holstein	Michael Thesing
Ken Curtis	Marc Lacroix	Jack Verson
Michael J. Dood	Parker McCauley	Tony Watson
James W. Evans	Bruce Muschlitz	Andrew West
Ron J. Farquharson		David Wood

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

Hanna E. Abdallah
William J. Ackerman
Stan J. Arnot
Thomas M. Barnes
George J. Bartok
Michael J. Bio
Philip C. Bolin
Stuart H. Bouchey
Dennis L. Carr
James F. Christensen
John R. Clayton
Ken L. Cooley
Robert Corlew
Frank A. Denbrock
W. Bruce Dietzman
Randall L. Dotson
Clifford Downs
Paul R. Drum
Donald G. Dunn
Ahmed Elneweihi
Gary R. Engmann
James W. Evans
Ron J. Farquharson
David L. Harris
Dennis K. Holstein
James Jung
George G. Karady
Richard P. Keil
Hermann Koch
Luther W. Kurtz
David S. Lehman
H. Peter Lips
John D. McDonald
A. S. Mehraban
A. P. Sakis Meliopoulos
Gary L. Michel
Bruce Muschlitz
Daniel E. Nordell
Shashi G. Patel
Carlos O. Peixoto
Radhakrishna V. Rebbapragada
Paulo F. Ribeiro
David Shafer
Yitzhak G. Shertok
Mark S. Simon
Robert C. Sodergren
Brian Sparling
Peter G. Stewart
Charles Sufana
John T. Tengdin
Duane R. Torgerson
Peter S. Wong
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
Mark D. Bowman
Gary R. Engmann
Harold E. Epstein
H. Landis Floyd
Jay Forster*
Howard M. Frazier
Ruben D. Garzon
James H. Gurney
Richard J. Holleman
Lowell G. Johnson
Robert J. Kennelly
Joseph L. Koepfinger*
Peter H. Lips
L. Bruce McClung
Daleep C. Mohla
James W. Moore
Robert F. Munzner
Ronald C. Petersen
Gerald H. Peterson
John B. Posey
Gary S. Robinson
Akio Tojo
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

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.

[1]DNP 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*

[2]IEC publications are available from the Sales Department of the International Electrotechnical Commission, Case Postale 131, 3, rue de Varembé, 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.

[3]IEEE 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/).

[4]ITU-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:

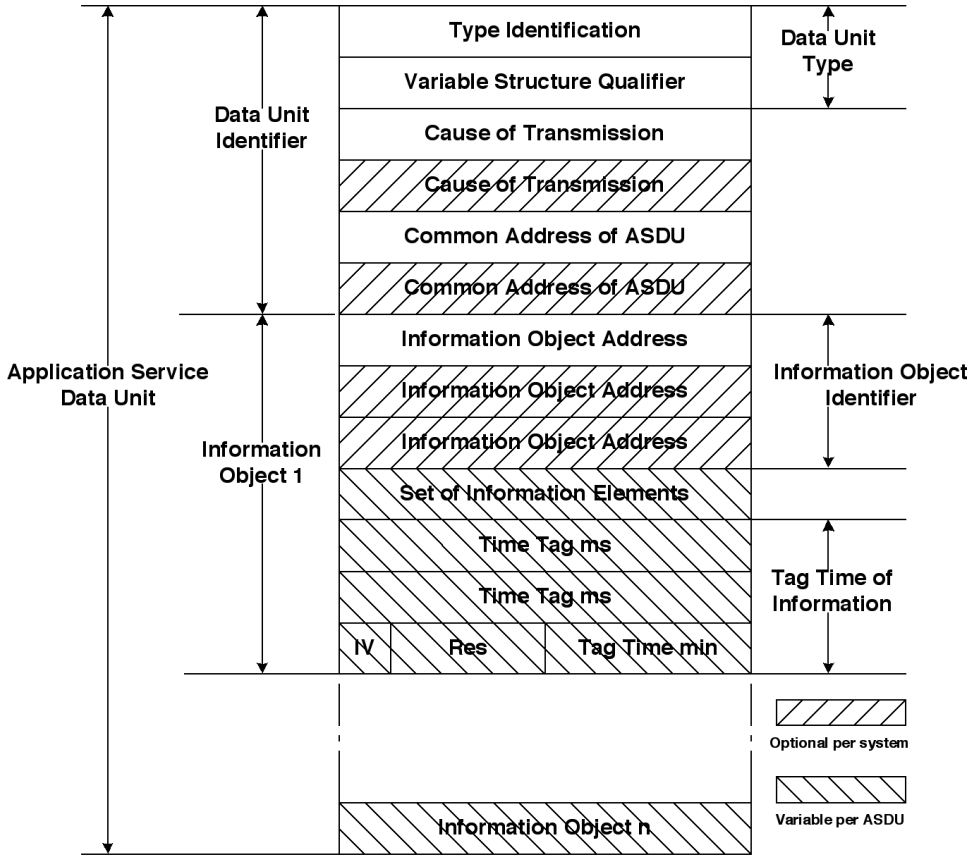
a) Station initialization
b) Cyclic data transmission
c) General interrogation
d) Command transmission
e) Data acquisition by polling
f) Acquisition of events
g) Parameter loading
h) File transfer
i) Clock synchronization
j) Transmission of integrated totals
k) Test procedure

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.

As a guide for achieving interoperability within a system, 101 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 check off list is the information that should be contained in the ASDU in both the control and monitor directions.

The 101 application layer specifies the structure of the ASDU, as shown in Figure 1. The fields 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).

Standard 101 also defines two new terms not found in the IEC 60870-5-1 through 60870-5 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.



Data Unit Identifier := CP16+8a+8b {Type Identification, Variable Structure Qualifier, Cause of Transmission, Common Address}
fixed system parameter a := number of octets of Common Address (1 or 2)
fixed system parameter b := number of octets of Cause of Transmission (1 or 2)
Information Object := CP8c+8j+8t {Information Object Address, Set of Information Elements, Time Tag (opt.)}
fixed system parameter c := number of octets of Information Address (1, 2 or 3)
variable parameter j := number of octets of Set of Information Elements
variable parameter t := 3 if Time Tag is present, 0 if Time Tag is not present

Figure 1—Structure of ASDUs in IEC 60870-5-101 (1995-11)

5.4 Summary comparative description tables

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

Table 1—Communication protocol layer structure

ISO/OSI layer	ISO/OSI layer definition	DNP3 implementation reference	101 implementation reference
1	Physical layer	Variety of asynchronous serial formats (v. 24 if modem used)	Unbalanced V.24/V 28, balanced X.24/X.27
2	Data link layer	IEC 60870-5 FT3, asynchronous with enhanced addressing	IEC 60870-*5* FTl 2
4	Transport layer	Pseudo-transport layer provides segmentation for large messages	Not applicable to 101
7	Application layer	DNP3 level 2 subset (DNP3-L2)	Selection of ASDUs from IEC-60870-5-4 (1993-08)
Not defined	User layer	Not applicable	IEC 60870-5-5 (1995-06) defines functions for clock sync and file transfer

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

Table 2—Protocol message/function types

DNP3 reference IEEE Std 1379-2000 preferred implementation			101 reference IEEE Std 1379-2000 preferred implementation	
Function code	Description	Recommended	<Type ID> or (Tx Cause)	Description
0	Confirm	Yes	(*P*/*N* = 0)	Positive confirm
			(*P*/*N* = l)	Negative confirm
1	Read	Yes	(1)	Periodic, cyclic
			<100>	Interrogation command
			<101>	Counter interrogation CMD
			<102>	Read command
			(5–6) (20)	Request General interrogation
			(2 1–36)	Group interrogation
			(38–41)	Group counter request

Table 2—Protocol message/function types (continued)

DNP3 reference IEEE Std 1379-2000 preferred implementation			101 reference IEEE Std 1379-2000 preferred implementation	
Function code	**Description**	**Recommended**	**<Type ID> or (Tx Cause)**	**Description**
2	Write	Yes	<120–126> (13)	File transfer
			<110–113>	Parameter of measured value
			<103>	Clock synch command
3 4 5 6	Select Operate Direct operate Direct operate—no ack	Yes Yes Yes Yes	<45–51> (6, 8)	Single/double command Setpoint commands Regulating step CMD Activation Deactivation
7 8 9 10 11 12	Immediate freeze Immediate freeze— no ack Freeze and clear Freeze and clear—no ack Freeze with time Freeze with time— no ack	Yes Yes Yes Yes No No	<113>	Parameter activation (parameter equals time period for periodic memorization of integrated totals)
13 14 15 16	Cold restart Warm restart Initialize data to default Initialize application	Yes No No No	(4)<70>	Initialized End of initialization
17 18	Start application Stop application	No No	<105>	Reset process command
19	Save configuration	No	<120–126> (13) <113>	File transfer Parameter activation
20	Enable unsolicited	Yes		
21	Disable unsolicited	Yes		
22	Assign to class	No	(20–41)	Group interrogations
23	Delay measurement	Yes	<103>	Clock synch command
129	Response	Yes	(11) (12) <7> <10> <1–21>	Return info—local CMD Return info—remote CMD Activation confirmation Deactivation confirmation Activation termination Process info—monitor direction
130	Unsolicited response	Yes	(1) (3) <104> <106>	Periodic, cyclic Spontaneous Test command Delay acquisition command

6. Physical layer definition (ISO/OSI layer 1)

There are two physical layer topologies used to construct both a SCADA communications network and an RTU-to-IED communications interface.

Point-to-point topology has two physical nodes with each physical node connected directly to the other. This can be a direct physical cable, a two-node radio or modem network, or a dial-up connection through a public switched network (PSN).

Multidrop topology has more than two physical nodes with each node connected to the same channel or communication line as every other node. In this configuration, one node, the master node, is deemed to be in control of the physical network. The master node transmits to multiple nodes and receives from multiple nodes. All other nodes in the network receive from the master node and transmit to the master node. In RTU/IED communication, the RTU is considered the master.

6.1 Modes of transmission

The physical layer supported by a RTU/IED protocol should transmit/receive data in a bit-serial mode. Generally, data are transferred in 8-bit octets at the most basic level. The transmission can be asynchronous, synchronous, or isochronous. Isochronous transmission allows for higher throughput when using synchronous modems. The actual mode of transmission should have no effect on the operation of the data link and higher layers of communication.

6.2 Local loop

The termination of the data communications circuit at the communicating device (not at the modem) should provide as a minimum a two-wire [one shared transmit/receive (TX/RX) pair, half duplex] or four-wire circuit (independent TX and RX pairs, full duplex). An RTU/IED protocol should support half-duplex operation with a two-wire circuit and full duplex and half-duplex operation with a four-wire circuit. The protocol should also support both full duplex and half-duplex procedures at the local loop. The different cases may be handled using different approaches, which may involve user definition of the type of circuit.

6.3 Recommended physical layer for DNP3

This subclause describes the DNP3 physical layer interface services that any physical layer should provide in order to accommodate the DNP3 data link. This recommended practice is applicable to RTU-to-IED links, which rarely utilize the PSN.

The physical layer that is recommended for DNP3 is a bit-serial oriented asynchronous physical layer supporting 8-bit data, 1-start bit, 1-stop bit, no parity, and EIA RS-232C voltage levels and control signals. The ITU-T V.24 standard (see Clause 2) describes the data terminal equipment (DTE) which is used for communication with a data communication equipment (DCE) device, often a modem. This type of circuit connection is used with either a public telephone carrier or private wire lines. In each case, the appropriate modem should be used and should conform (minimally) to the V.24 standard DCE definition.

The physical layer should provide the following five basic services: send, receive, connect, disconnect, and status.

a) The send service converts data octets into bit-serial data for transmission between the DTE and DCE. It should provide the proper signal control in order to communicate with the given DCE.

b) The receive service must be able to accept data from the DCE and therefore provide the correct signaling to the DCE in order to receive data and not noise.

c) The connect and disconnect services provide connection and disconnection from the PSN (where applicable).

d) The status service should be able to return the state of the physical medium. As a minimum, the service should indicate whether or not the medium is busy.

6.4 Recommended physical layers for IEC 60870-5-101 (1995-11)

The 101 profile provides control (RTU-to-IED) and monitor (RTU-to-IED) communications compliant with the following standards. Details are contained in the ITU-T publications referenced in Annex B.

The 101 profile is as follows:

a) *Control transmission direction*. Either an unbalanced interchange circuit per ITU-T V.24/V.28 (see Clause 2) with data rates of 300, 600, 1200, 2400, 4800, or 9600 bit/s, or balanced interchange circuit per ITU-T X.24/X.27 with data rates of 2400, 4800, 9600, 19 200, 38 400, 56 000, or 64 000 bit/s.

b) *Monitor direction*. Follows the same models, but may be selected differently.

IEC 60870-5-1 (1990-02) specifies the basic requirements for services to be provided by both the physical layer and data link layer 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.

Four basic framing formats that apply at both the data link and physical layers are defined. These formats (FT1, FT1.2, FT2, and FT3) vary in their frame transmission efficiency, data integrity class, and hardware support requirements.

The selection of frame formats allows for the protocol to be selected for a wide range of applications in diverse environments. For example, in a fairly noisy environment, FT1.2 is indicated to make use of a standard, PC-style universal asynchronous receiver/transmitter (UART) as the communication port in the RTU or IED.

Standard 101 conforms to IEC 60870-5-1 (1990-02) by including 33 idle bits (three idle characters in asynchronous mode) between each message. The receiving station can expect 33 idle bits (also called quiescent state) to exist between each message.

The ITU-T V.24 recommendation is common to both the DNP3 and the IEC 60870-5-101 (1995-11) implementations.

7. Data link layer definition (ISO/OSI layer 2)

7.1 Recommended data link layer for DNP3

This clause defines the DNP3 data link layer, link protocol data unit (LPDU), as well as data link layer services and transmission procedures. Master stations, submaster stations, RTUs, and IEDs can use this data link to pass messages between primary (originating) stations and secondary (receiving) stations.

In DNP3 protocol, master stations, submaster stations, (RTUs), and IEDs are both originators (primary stations) and receivers (secondary stations).

A data link layer accepts, performs, and controls transmission service functions required by the higher layers. The DNP data link layer shall provide transfer of information or link service data unit (LSDU) across the physical link. User data supplied by the higher layers (LSDU) shall be converted into one frame (or LPDU) and sent to the physical layer for transmission. LPDUs received by the data link layer shall be assembled into one LSDU and passed to higher layers. The DNP3 data link layer also provides for frame synchronization, link control, and indications of other events such as link status.

The OSI reference model enforces either a connection-oriented or connection-less system. However, the EPA model implies neither a connection-less system nor a connection-oriented system. The DNP3 implementation of the IEC data link handles both connection-less and connection-oriented systems (i.e., physical networks that require dial-in or log-in before data can be transmitted to the destination device) but has no need to provide connection services. The actual physical network is transparent to the application using the data link because the data link layer is responsible to connect and disconnect from any physical network without higher level interaction (i.e., the application layer). The data link (given the station destination address) will connect to the right physical circuit without control supplied from the higher layers. In this way, the physical medium is totally transparent to the link layer service user.

7.1.1 DNP3 data link functions, services, and responsibilities

This subclause describes the services offered by the data link and its functions. The communication requirements of the network layer and the pseudo-transport layer are satisfied by the data link layer service primitives.

The data link is responsible for performance of the following functions:

a) Message retries
b) Synchronizing and handling of frame control bit (FCB) in the control word
c) Setting and clearing the data flow control (DFC) bit based on buffer availability
d) Automatically establishing a connection based on the destination parameter in a dial-up environment when a directed service is requested by the user
e) Disconnection in a dial-up environment
f) Packing user data into the defined frame format and transmitting the data to the physical layer
g) Unpacking the frames that are received from the physical layer into user data
h) Controlling all aspects of the physical layer
i) Collision avoidance/detection procedures to ensure the reliable transfer of data across the physical link
j) Responding to all valid frames/function codes received from the physical layer

The data link is responsible for provision of the following services:

a) Exchange of service data units (SDUs) between peer DNP data links
b) Error notification to data link user
c) Sequencing of SDUs
d) Quality SDU delivery

SDUs are only exchanged between peer DNP data links. Quality delivery can be SEND-NO-REPLY or SEND-CONFIRM to indicate whether or not message acknowledgment is required. Error notification will be given to the data link user when a response to a request has not been received.

An FT3 frame containing the LPDU is defined as a fixed-length header block followed by optional data blocks. Each block has a 16-bit CRC appended to it. The IEC specifies that the header fields consist of two start octets, one octet length, one octet control, a destination address and an optional fixed-length user data field. In this implementation the fixed-length user data field is defined as a source address.

7.1.2 DNP3 data link layer versus IEC 60870-5

The draft versions of IEC 60870-5-1 (1990-02) and IEC 60870-5-2 (1992-04) were the basis for developing the DNP3 data link layer. The DNP3 data link supports polled and quiescent telecontrol systems and is designed to operate with connection and connection-less orientated, asynchronous or synchronous, bit-serial physical layers such as the electrical specifications RS-232C, RS-485, and fiber optic transceivers. Fully-balanced transmission procedures were adopted to support spontaneous transmissions from RTUs, IEDs, or submaster stations not designated as master stations.

The following are specific comparisons between the DNP3 protocol and the IEC 60870-5 telecontrol data link layer protocol specification:

a) *Pseudo-transport layer.* To support advanced RTU functions and messages larger than the maximum frame length as defined by IEC 60870-5-1 (1990-02), the DNP3 data link is intended to be used with a pseudo-transport layer. The pseudo-transport layer implements as a minimum message assembly and disassembly, which is not defined in IEC 60870-5. This pseudo-transport layer is described in DNP3, transport functions (P009-0PD.TF). These transport functions are not a part of the data link but are used to support advanced RTU functions and are controlled at the user layer of DNP3.

b) *Channel failover.* The DNP3 data link layer communicates with only one physical layer (or channel). In IEC 60870-5-1 (1990-02), item 13, the session layer is responsible for maintaining channel connections. In DNP3, channel failover is instead handled at the application layer.

c) *Frame format and procedures*. The DNP3 data link layer uses a variable-length frame format adapted from type FT3 defined in IEC 60870-5-1 (1990-02). For asynchronous operation, start and stop bits are appended to octets. The FT3 frame format is suited for data transmission between stations that require medium information transfer rates and low residual error probability. The basic frame format and transmission rules R1, R2, R3, and R4 from IEC 60870-5-1 (1990-02) are used. Rules R5 and R6 are adapted to make the exact time values configurable in each implementation. The frame definitions outlined in IEC 60870-5-2 (1992-04) are followed, with the condition that the address field is two octets and specifies the destination station address; the link user data field is used as a two-octet source station address.

   In full duplex channel applications, fully-balanced transmission procedures from IEC 60870-5-2 (1992-04) are used by DNP3 to handle unsolicited transmissions from stations not designated as masters. Fully balanced means that each station can act as a primary station (sending) and a secondary station (receiving) at the same time.

   In a half duplex channel environment, the same procedures will be used except that a station cannot be both a primary and secondary station at the same time. An entire data link layer transaction between stations, consisting of two transmissions, will have to be completed at both stations, before starting other transactions. In all channel configurations, it is the responsibility of each device to implement a compatible collision avoidance scheme.

d) *Length, control, and address fields*. The DNP3 data link layer uses the LENGTH field as defined in IEC 60870-5-1 (1990-02) (6.2.4). The CONTROL field used is as defined in IEC 60870-5-2 (1992-04) (6.1.2) for balanced transmission. All the function codes specified in IEC 60870-5-3 (1992-09) (Table III) are supported.

   The DNP3 data link frame header has two address fields. Each address field is 16 bits (two octets). The first field, or “A” (address) field, represents the destination station address. The second field is in the link user data field, where it is used to represent the source station address.

7.2 Recommended data link layer for IEC 60870-5-101 (1995-11)

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 point-to-point topologies do not require either source or destination addressing.

Format class FT1.2 with Hamming distance of four and format class FT2 support control systems with normal data integrity/security requirements. Format class FT3 is suited for systems with particularly high data integrity requirements.

The 101 companion standard profile specifies the FT1.2 frame format to provide the required data integrity together with the maximum efficiency available for an acceptable level of convenience of implementation. In particular

a) The FT1.2 frame format with the single character “I” (0xE5) and fixed time-out interval are used.

b) The data link transmission mode can be either balanced (half duplex for multidrop topologies) or unbalanced (for point-to-point topologies). The maximum message length “L” should be specified in octets (bytes). Appropriate function codes for the control field are specified for both modes of operation.

c) The address field can be one of the following: none (balanced transmission only), 1-octet address, 2-octet address, structured, or unstructured. The address shall be an unambiguous number for each link. Each address may be unique within a specific system, or it may be unique within a group of links sharing a common channel. The latter needs a smaller address field, but requires the controlling node to map addresses by channel number.

The transmission functions in telecontrol systems are composed of three basic types of link transmission services, namely SEND/NO REPLY, SEND/CONFIRM, and REQUEST/RESPONSE. The two services SEND/CONFIRM and REQUEST/RESPONSE consist of a sequence of non-separable dialogue elements (frames) between requesting stations and responding stations. SEND/NO REPLY is a broadcast function intended for multiple destinations.

7.3 DNP3 pseudo-transport layer (ISO/OSI layer 4)

The DNP3 layer stack includes a pseudo-transport layer, which implements (as a minimum) message assembly and disassembly functions to support advanced RTU functions and messages larger than the maximum frame length as defined by IEC 60870-5-1 (1990-02). This pseudo-transport layer is described in detail in DNP3. Pseudo-transport functions were included in the protocol stack because of the following factors:

a) Transfer of large application layer messages is demanded by complex IEDs, which are to be supported by DNP3. These messages typically contain data acquired by recording instruments, which generate large files of historical and problem analysis data examined by personnel at office and/or control centers.

b) To ensure data integrity, the DNP3 data link layer uses the IEC 60870-5-1 (1990-02) frame format FT3. This frame format has a Hamming distance of six, and therefore a maximum frame length of 292 octets, 250 of which can be user (application layer) data. This is much smaller than the size of the larger application layer messages.

Therefore, functionality was required that was not a full transport layer nor part of the FT3 frame, but that did provide a segmentation mechanism. The DNP3 transport header therefore consists of a single octet containing the following bit fields:

FIR—a single bit set if the data link frame is the FIRst frame of an application layer message

FIN—a single bit set if the data link frame is the FINal frame of an application layer message

SEQ—the sequence number of the frame

The transport header is removed by the device at each end of a physical layer, like the data link overhead, so it is not a true end-to-end transport layer. However, it is not actually part of the data link overhead but is counted as the first octet of cyclic-redundancy-checked user data carried by the data link layer. All confirmation and reliability is provided by the data link layer, not by the transport function. This function results in reduced layers and overhead and retains a high level of data integrity, yet provides a richer set of application layer functions.

8. Application layer definition (ISO/OSI layer 7)

8.1 Recommended application layer for DNP3

This clause specifies the DNP3 application layer services and message format and also the application protocol data unit (APDU), application data flow control, and any specific information pertaining to DNP application layer services. The DNP3 structure resembles the IEC 60870-5 simplified model known as enhanced performance architecture (EPA). DNP3 expands on the EPA by providing a pseudo-transport function.

Figure 2 shows the EPA structure. The user layer represents the actual RTU or IED application and makes use of the application layer to send/receive complete messages to another DNP3 compliant device.

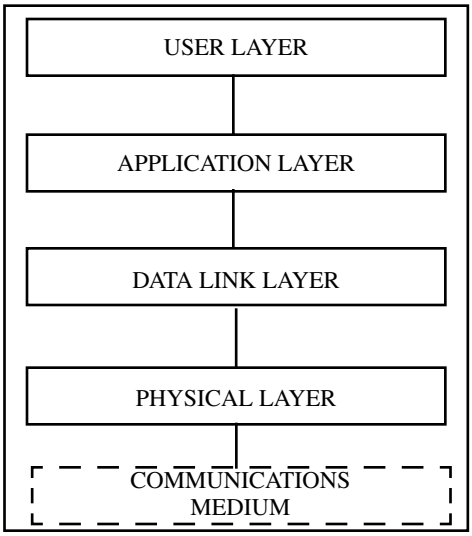


Figure 2—EPA layer organization

8.1.1 Application layer description and IEC 60870-5 comparison

The DNP3 application layer APDU is based on draft versions of IEC 60870-5-3 (1992-09) and 60870-5-4 (1993-08). Structurally, the application layer PDU (protocol data unit) fits the IEC description of an APDU. The user sends application user data to the application layer where it is converted to ASDU (application service data unit). In DNP3, the application user data is converted into multiple ASDUs. Each ASDU is then prefixed by APCI (application protocol control information), which is then packaged as an APDU.

In DNP3, each APDU that is part of the larger multi-APDU is referred to as a fragment. Each fragment shall contain only complete data objects and the function code portion of the APCI shall be identical in each fragment of the multi-APDU. There can be no fragmentation of information objects between APDUs—the same operation shall be requested of each object in the message. This ensures that each fragment can be processed on receipt and that each ASDU contains only complete data objects. In reverse, the application layer receives multiple APDUs (one at a time), removes the APCI to obtain the ASDU, and then assembles the ASDUs into the total application user data.

DNP3 also includes the concept of a class to segment data objects. Objects may be assigned to one of four classes of data. Class 0 is reserved for static data objects (static data is the current value of data in the IED or RTU). Classes 1, 2, and 3 are reserved for event data objects (objects created because of data changes within the IED or RTU, or from some input). Each event object can be assigned to Class 1, 2, or 3. Objects may be grouped in classes by priority (the priority is determined by the user), and the data classes may be polled via the SCADA system at varying rates.

The ability to assign data to classes and the degree of configurability is described in the device implementation profile. It is not required that a device have data assigned to Classes 1, 2, or 3.

Class data is used by a master station or RTU to request preassigned data objects on a demand or availability basis from a device. Therefore, a class data object header can be used only in a request (with no associate data object) to indicate to the device which data objects to return. The device will return (in the response) object headers for the actual data objects and not the class object header.

This recommended practice provides that DNP3 will be implemented using the second subset of the application layer. This implementation level is L2. This level has more features than an L1 implementation and is intended to be used between a RTU or data concentrator and an IED (e.g., meter, relay, auto-recloser, or capacitor bank controller). It is intended for use with devices whose input and output points are local to the device.

8.1.2 DNP3 application layer subset implementation table

Table 3 describes the objects, function codes, and qualifiers used in an L2 DNP3 implementation. To conform to this recommended practice, a device should also follow the implementation rules defined in the DNP3 subset definitions referenced in Clause 2. Use of a DNP device profile document provides a useful implementation checklist, as well as a concise way of exchanging details with other developers or users.

Each row of Table 3 lists a particular DNP3 object. An IED should be able to parse a request message (shown in the request column) containing the specified object variation, function codes, and qualifiers. The RTU should be able to parse a response (shown in the response) column from the IED containing the specified object variation, function codes, and qualifiers. Refer to Table 2, or the DNP3 application layer specification for the meanings of the function codes. Refer to the DNP3 application layer specification for the meanings of the qualifier fields.

NOTE—The IED does not need to support delay measurement (function code 23) or write (function code 2) of time and date (object 50, variation 1), if the IED never requests time synchronization using the time synchronization required internal indication.

Table 3—Level 2 subset implementation of DNP3 (DNP3-L2)

Object			Request (IED shall parse)		Response (RTU shall parse)	
Obj	**Var**	**Description**	**Function codes (decimal)**	**Quality codes (hex)**	**Function codes**	**Quality codes (hex)**
1	0	Binary input—all variations	1	06		
1	1	Binary input			129, 130	00, 01
1	2	Binary input with status			129, 130	00, 01
2	0	Binary input change—all variations	1	06, 07, 08		
2	1	Binary input change without time	1	06, 07, 08	129, 130	17, 28
2	2	Binary input change with time	1	06, 07, 08	129, 130	17, 28
2	3	Binary input change with relative time	1	06, 07, 08	129, 130	17, 28
10	0	Binary output—all variations	1	06		
10	2	Binary output status			129, 130	00, 01
12	1	Control relay output block	3, 4, 5, 6	17, 28	129	Echo of request
20	0	Binary counter—all variations	1, 7, 8, 9, 10	06		
20	1	32-bit binary counter			129, 130	00, 01
20	2	l6-bit binary counter			129, 130	00, 01
20	3	32-bit delta counter			129, 130	00, 01
20	4	16-bit binary counter			129, 130	00, 01
20	5	32-bit binary counter without flag			129, 130	00, 01
20	6	16-bit binary counter without flag			129, 130	00, 01
20	7	32-bit delta counter without flag			129. 130	00, 01
20	8	16-bit delta counter without flag			129, 130	00, 01
21	0	Frozen counter—all variations	1	06		
21	1	32-bit frozen counter			129, 130	00, 01
21	2	16-bit frozen counter			129, 130	00, 01
21	9	32-bit frozen counter without flag			129, 130	00, 01

Table 3—Level 2 subset implementation of DNP3 (DNP3-L2) (continued)

Object			Request (IED shall parse)		Response (RTU shall parse)	
Obj	**Var**	**Description**	**Function codes (decimal)**	**Quality codes (hex)**	**Function codes**	**Quality codes (hex)**
21	10	16-bit frozen counter without flag			129, 130	00, 01
22	0	Counter change event—all variations	1	06, 07, 08		
22	1	32-bit counter change event without time			129, 130	17, 28
22	2	16-bit counter change event without time			129, 130	17, 28
22	3	32-bit delta counter change event without time			129, 130	17, 28
22	4	16-bit delta counter change event without time			129, 130	17, 28
30	0	Analog input—all variations	1	06		
30	1	32-bit analog input			129, 130	00, 01
30	2	l6-bit analog input			129, 130	00, 01
30	3	32-bit analog input without flag			129, 130	00, 01
30	4	16-bit analog input without flag			129, 130	00, 01
32	0	Analog change event—all variations	1	06, 07, 08		
32	1	32-bit analog change event without time			129, 130	17, 28
32	2	16-bit analog change event without time			129, 130	17, 28
40	0	Analog output status—all variations	1	06		
40	2	16-bit analog output status			129, 130	00, 01
41	2	16-bit analog output block	3, 4, 5, 6	17, 28	129	Echo of request
50	1	Time and date	2 optional	07 where quantity = 1		
51	1	Time and date CTO			129, 130	07, quantity = 1
51	2	Unsynchronized time and date CTO			129, 130	07, quantity = 1
52	1	Time delay coarse			129	07, quantity = 1

Table 3—Level 2 subset implementation of DNP3 (DNP3-L2) (continued)

Object			Request (IED shall parse)		Response (RTU shall parse)	
Obj	**Var**	**Description**	**Function codes (decimal)**	**Quality codes (hex)**	**Function codes**	**Quality codes (hex)**
52	2	Time delay fine			129	07, quantity = 1
60	1	Class 0 data	1	06		
60	2	Class 1 data	1	06, 07, 08		
60	3	Class 2 data	1	06, 07, 08		
60	4	Class 3 data	1	06, 07, 08		
80	1	Internal indications	2	00 index = 7		
No object			13			
No object			23 optional			

8.2 Recommended application layer for IEC 60870-5-101 (1995-11)

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.

In this recommended practice, it is appropriate to admit application-specific or system-specific choices of data presentation, address structures, and chaining mechanisms for information objects in a frame. In most cases, the corresponding arrangements can be assumed to be known by the communicating stations and thus, need not burden the transmission frame.

The 101 companion standard defines appropriate ASDUs from the general structure in IEC 60870-5-3 (1992-09) as follows:

a) The common ASDU address may be one or two octets.

b) The information object address may be one, two, or three octets and may be structured or unstructured.

c) Cause of transmission may be one octet or two octets with originator address.

d) Station initialization may be remote or not remote.

e) General interrogations may be global or reference groups numbered 1 through 16. Addresses in each group should be defined.

f) Clock synchronization may be provided or not provided.

g) Commands of any of the following types may be transmitted:

   1) Direct command

   2) Direct set-point command

   3) Select and execute

   4) Select and execute set-point

   5) General—without additional definition

6) Use of C-SE ACTTERM is optional
7) Short pulse duration (determined by system parameter)
8) Long pulse duration (determined by system parameter)

h) Commands requesting transmission of integrated totals (e.g., metering)
1) Counter request
2) Counter freeze without reset
3) Counter freeze with reset
4) Counter reset
5) General request counter
6) Request counter by group (select from group 1 through 4); addresses in group should be defined

i) Parameter loading (download to device) may include the following:
1) Threshold values
2) Smoothing factor
3) Limit on transmission of measured value

j) Parameter activation (direct device to start/stop cyclic transmission)

k) Activate/deactivate persistent cyclic or periodic transmission of the addressed object

l) The selection of standard ASDUs is made from Table 4. The necessary ASDUs are limited to this list, but the user may implement others as needed

Table 4—Selected ASDUs for IEC 60870-5-101 (1995-11)

ASDU number	Definition	Label used
Process information in monitor direction		
<1> =	Single-point information	M_SP_NA_1
<2> =	Single-point information with time tag	M_SP_TA_1
<3> =	Double-point information	MDP_NA_1
<4> =	Double-point information with time tag	M_DP_TA_1
<5> =	Step position information	M_ST_NA_1
<6> =	Step position information with time tag	M_ST_TAJ
<7> =	Bitstring of 32 bit	M_BO_NA_1
<8> =	Bitstring of 32 bit with time tag	M_BO_TA_1
<9> =	Measured value, normalized value	M_ME_NA_1
<10> =	Measured value, normalized value with time tag	M_ME_TA_1
<11> =	Measured value, scaled value	M_ME_NB_1
<12> =	Measured value, scaled value with time tag	M_ME_TBJ
<13> =	Measured value, short floating point value	M_ME_NC_1
<14> =	Measured value, short floating point value with time tag	M_ME_TC_1

Table 4—Selected ASDUs for IEC 60870-5-101 (1995-11) (continued)

ASDU number	Definition	Label used
<15> =	Integrated totals	M_IT_NA_1
<16> =	Integrated totals with time tag	M_IT_TA_1
<17> =	Event of protection equipment with time tag	M_EP_TA_1
<18> =	Packed start events of protection equipment with time tag	M_EP_TB_1
<19> =	Packed output circuit information of protection equipment with time tag	MEP_TB_1
<45> =	Single command	CSC_NA_1
<46> =	Double command	C_DCNA_1
<47> =	Regulating step command	C_RC_NA_1
<48> =	Set point command, normalized value	C_SE_NA_1
<49> =	Set point command, scaled value	C_SE_NB_1
<50> =	Set point command, short floating point value	C_SE_NC_1
System information in monitor direction		
<70> =	End of initialization	M_EI_NA_1
System information in control direction		
<100> =	Interrogation command	C_IC_NA_1
Process information in monitor direction		
<101> =	Counter interrogation command	C_CI_NA_1
<102> =	Read command	C_RD_NA_1
<103> =	Clock synchronization command	C_CS_NA_1
<104> =	Test command	C_TS_NA_1
<105> =	Reset process command	C_RP_NA_1
Parameter in control direction		
<110> =	Parameter of measured value, normalized	P_ME_NA_1
<111> =	Parameter of measured value, scaled	P_ME_NB_1
<112> =	Parameter of measured value, short floating point value	P_ME_NC_1
<113> =	Parameter activation	PAC_NA_1
File transfer		
<120> =	File ready	F_FR_NA_1

Table 4—Selected ASDUs for IEC 60870-5-101 (1995-11) (continued)

ASDU number	Definition	Label used
<121> =	Section ready	F_SR_NA_1
<122> =	Call directory, select file, call file, call section	F_SC_NA_1
<123> =	Last section, last segment	F_LS_NA_1
<124> =	Ack file, ack section	F_AF_NA_1
<125> =	Segment	F_SG_NA_1
<126> =	Directory	F_DR_TA_1

9. Definitions of data elements and objects

Data elements, or objects, populate the protocol structure with defined information that has a specific form and meaning. The provision of elements or objects allows implementers of the protocol to reduce development time and prevents duplication of work already completed. The data elements allow the various devices that use the protocol to quickly recognize information that is needed for further processing or response.

9.1 DNP3 data element/object definition

The DNP3 objects are defined in Table 3. These are derived from the level 2 subset implementation of DNP, as generated and documented by the DNP user's group. Implementers may provide more functionality than the subset, per guidelines discussed in the DNP3 subset definitions and in 5.1.5 of this recommended practice.

9.2 IEC 60870-5 data element definition

IEC 60870-5-4 (1993-08) provides rules for defining information data elements. It presents a common set of information elements, in particular about digital and analog process variables, which are frequently used in telecontrol applications. Syntactic rules are presented for defining application-specific information elements as well as basic data type definitions. These basic data types are then subtyped by applying the syntactic rules.

A minimal set of standard information elements is defined for those typically found in telecontrol applications. These recommendations are not part of the standard. The standard allows definition of application elements in companion profiles. Standard 101 provides most of the definitive information elements necessary for the specific IED and RTU applications covered by this recommended practice.

9.3 Comparative tables of defined objects and data elements

Table 5 and Table 6 provide summaries of known data objects suitable for use in this recommended practice. As with Table 1 and Table 2, a further comparison is given in Table A.3 and Table A.4 in Annex A.

Table 5—Data objects—primitive

Generic data element	DNP3 reference			IEC 60870-5-101 (1995-11) reference	
	Name	Obj, var	L2	Name	APDU type
Binary inputs	Binary input	1,1	Y	Single-point information	1
	Binary input with status	1,2	Y		
Binary input history	Binary input change with time	2,1	Y	Single-point information with time tag	2
	Binary input change with release time	2,2	Y		
Double-point inputs	No corresponding data type			Double-point information	3
				Double-point information with time tag	4
Bit string	Binary input	1,1	Y	Bit string of 32 bits	7
	Pattern mask	12,3		Bit string of 32 bits with time tag	8
Binary output	Binary output	10,1		Single command	45
	Binary output status	10,2	Y	Double command	46
	Control relay output block	12,1	Y	Regulating step command	47
Bit string output	Pattern control block	12,2		Bit string of 32 bits	51
	Pattern mask	12,3			
Unsigned integer input	16-bit binary counter	20,2	Y	Integrated totals	15
	32-bit binary counter	20,1			
Unsigned integer history	16-bit counter change	22,2	Y	Integrated totals with time tag	16
	32-bit counter change	22,1	Y		
	16-bit counter change with time	22,6			
	32-bit counter change with time	22,5			
	16-bit frozen counter	21,2	Y		
	32-bit frozen counter	21,1	Y		
	16-bit frozen counter event with time	23,6			
	32-bit frozen counter event with time	23,5			
Signed integer input	16-bit analog input	30,2	Y	Step position information	5
	32-bit analog input	30,1	Y	Measured value—normalized	9
				Measured value—scaled	11

Table 5—Data objects—primitive (continued)

Generic data element	DNP3 reference			IEC 60870-5-101 (1995-11) reference	
	Name	Obj, var	L2	Name	APDU type
Signed integer history	16-bit analog input change	32,2	Y	Step position information with time tag	6
	32-bit analog input change	32,1	Y	Measured value—normalized value with time tag	10
	16-bit analog input change with time	32,4		Measured value—scaled value with time tag	12
	32-bit analog input change with time	32,3			
Floating-point input	Short floating-point analog	30,5		Measured value—short floating point	13
	Long floating-point analog	30,6			
Floating-point input history	Short floating-point change	32,5		Measured value—short floating point with time tag	14

Table 6—Meter implementation, one vendor—example

Meter functions	Register		DNP3 implementation			
	Size	Flag	Object	Size	Flag	Point
Phase A volts	12 bit	Yes	Analog	16 bit	Yes	0
Phase B volts	12 bit	Yes	Analog	16 bit	Yes	1
Phase C volts	12 bit	Yes	Analog	16 bit	Yes	2
Phase A amps	12 bit	Yes	Analog	16 bit	Yes	3
Phase B amps	12 bit	Yes	Analog	16 bit	Yes	4
Phase C amps	12 bit	Yes	Analog	16 bit	Yes	5
A phase angle	12 bit	Yes	Analog	16 bit	Yes	6
B phase angle	12 bit	Yes	Analog	16 bit	Yes	7
C phase angle	12 bit	Yes	Analog	16 bit	Yes	8
Kilowatthours in	16 bit	No	Accumulator	16 bit	No	0
Kilowatthours out	16 bit	No	Accumulator	16 bit	No	1
Kilovarhours in	16 bit	No	Accumulator	16 bit	No	2
Kilovarhours out	16 bit	No	Accumulator	16 bit	No	3
Manual reset	—	Yes	Status	1 bit	No	0
Acknowledge	—	—	—	1 bit	No	0

10. Process for addition of data elements/objects

Given the high level of ongoing activity regarding standardized communications, there will be substantial additions to the implementation data contained in this recommended practice on a regular basis. It is useful for this updated information to be made available to those who are using this recommended practice. It is also an obligation of users of this recommended practice to supply additions they make to the protocol, as well as to consult the working groups to obtain the latest information before creating duplicate implementations that may not be interoperable.

10.1 Creation

The tabular formats utilized in this document are adequate for definitions of most new implementations. Suppliers of equipment as well as specifiers and users can represent a variety of devices directly from the information contained herein. The maximum interoperability is obtained when common definitions are used for as much of the communications as possible.

However, there will be many additional specific functions and data elements that will be needed as new and novel devices and systems are created. These device models and messaging requirements should use the primitive level definitions herein. The additional data should be described in adequate detail that provides all parameters noted in the protocol standards documents. The additional definitions should also be provided to the sponsoring bodies of the protocol so they may be worked in to the basic protocol documents and shared with other implementers.

For IEC 60870-5, new information elements can be added in accordance with the rules described in IEC 60870-5-4 (1993-08).

ISO provides formal requirements for object registration as part of the open systems interconnection process.

10.2 Role of the DNP users group

DNP3 has an independent users group that administers DNP3. A function of this users group is to voluntarily register DNP3 implementations and to serve as an unbiased mediator to develop DNP3 implementations for various classes of devices (i.e., meter, regulator, relay, et al.). IED vendors, prior to beginning any DNP3 development, may contact the users group to see what developments already exist and which features should be supported for the IED device in question. The users group embodies a number of users and vendors who represent an experience base and market expertise that may allow a DNP3 development to be available to the largest body of potential users.

Annex A

(informative)

Comparison of DNP3 and IEC 60870-5-101 (1995-11)

This annex provides reference tables that compare DNP3 and IEC 60870-5-101 (1995-11). The purpose is to provide comparison of both structure and defined data contents of each protocol.

A.1 Communication protocol layer structure

Each of the referenced protocols makes use of the ISO/OSI layer structure model. Implementation of each protocol consists of a selected set of layer definitions, as illustrated in Table A.1.

Table A.1—Communication protocol layer structure for IEEE Std 1379-2000

ISO/OSI model layer	Layer name definition	DNP3 implementation	IEC 60870-5-101 (1995-11) implementation
1	Physical layer	Asynchronous, bit-serial, 8 data bits, 1 stop, no parity	Unbalanced V24/V.28 balanced X.24/X 27
2	Data link layer	IEC 60870-5 FT3	IEC 60870-5 FT1.2
4	Transport layer	DNP-specific pseudo-transport layer for long message segmentation	Not implemented
7	Application layer	Generally organized as arrays of data elements with support for files and other objects	APDUs as defined in IEC 60870-5-101 (1995-11) from IEC 60870-5-4 (1993-08)
Not defined	User layer	Device, unit, or system-specific data representation	Device, unit, or system-specific data representation

A.2 Message/function types

Table A.2 presents information on functions and/or messages that are applicable to the RTU/IED communication functions. Where similar operations exist in each of the implementations, equivalent messages/operators are shown.

Table A.2—Message/function types for IEEE Std 1379-2000

Function or message	DNP3 implementation			IEC 60870-5-101 (1995-11) implementation	
	Function code	Description	Recommended	<Type ID> or (Tx Cause)	Description
					Send
Confirm	0	Confirm	Yes	(P/N=0)	Positive confirm
Read	1	Read	Yes	(1)	Periodic, cyclic
				<100>	Interrogation command
				<101>	Counter interrogation command
				<102>	Read command
				(5–6)	Request
				(20)	General interrogation
				(21–36)	Group interrogation
				(38–41)	Group counter request
Write	2	Write	Yes		
				<120–126> (13)	File transfer
				<110–113>	Parameter of measured value
		Send time Synchronize object		<103>	Clock synchronize command
Select	3	Select	Yes	<45–51> (6, 8)	Single/double commands Setpoint command Regulating command Step command Activation command
Operate	4	Operate	Yes	<45–51> (6, 8)	Single/double commands Setpoint command Regulating command Step command Activation command
	5	Direct operate	Yes	<45–51> (6, 8)	Single/double commands Setpoint command Regulating command Step command Activation command
	6	Direct operate no ack	Yes		

Table A.2—Message/function types for IEEE Std 1379-2000 (continued)

Function or message	DNP3 implementation			IEC 60870-5-101 (1995-11) implementation	
	Function code	Description	Recommended	<Type ID> or (Tx Cause)	Description
	7	Immediate freeze	Yes	<101>	Counter interrogation
	8	Immediate freeze no ack	Yes		
	9	Freeze and clear	Yes		
	10	Freeze and clear no ack	Yes		
	11	Freeze with time	No		
	12	Freeze with time no ack	No		
	13	Cold start	Yes	(4) <70>	Initialized End of initialization
	14	Warm restart	No		
	15	Initialize data to default	No		
	16	No			
Run program	17	Start application	No	<105>	Reset process command
Stop program	18	Stop application	No		
	19	Save configuration	No	<120–126> (13)	File transfer
				<113>	Parameter activation
Start unsolicited	20	Enable unsolicited	Yes		
Stop unsolicited	21	Disable unsolicited	Yes		
Set priority	22	Assign to class	No		
	23	Delay measurement	Yes	<106>	Delay acquisition command
Response with data	129	Response	Yes	<1–21>	Process information–monitor direction
	130	Unsolicited response	Yes		
Test				<104>	Test command

A.3 Data objects—primitive

The protocols compared in Table A.3 use similar basic data representations that carry the "numbers" identified in the object or element definitions of the protocol. Table A.3 shows the variety of primitive representations that are available in the two protocols. Not all primitive types will map to a data object or element.

Table A.3—Data objects for IEEE Std 1379-2000 implementation—primitive

Parameter equal generic data element	DNP# implementation		IEC 60870-5-101 (1995-11) implementation	
	Notation	Typical use in an object		
Bit notation	BSn[pos]	*n* = number of bits pos = bit position in word		
Bit	BS1	Binary input, control relay output block, binary output status		
Bit string	BSn	(not in DNP3-L2)		BITSTRING (size)
Pattern mask	UI	To be defined		
Integer 8-bit unsigned	UII6	16-bit binary counter		
16-bit frozen counter				Integer 16 U
Integer 16-bit signed	I16	16-bit analog input		
16-bit analog output				Integer 16 S
Integer 32-bit unsigned	UI32	32-bit binary counter		
32-bit frozen counter				Integer 32 U
Floating point number—32 bit	R32			
(IEEE)	Short floating point	(Not in DNP30-L2)		
Floating point number—64 bit	R64			
(IEEE)	Long floating point	(Not in DNP3-L2)		

A.4 Data elements with utility specific definitions

Many forms of lED and RTU data need to be represented by known objects that have a defined place in the protocol used. Depending on the protocol, the object can be very specific or is very general, being related to the precise quantity represented only in the context of the protocol structure. Table A.4 is intended to compare the representations of two relevant protocols.

Table A.4—Data elements with utility-specific definitions

Utility-specific data element	DNP3 implementation	IEC 60870-5-101 (1995-11) implementation
Analog input		
Sensor value	16/32-bit analog input Floating point analog input *	Measured value
Transducer value		
Amps (Kamps)		
Volts (Kvolts)		
Power factor		
Watt (kwatt)		
VA (kVA)		
VAR (kVAR)		
Frequency—Hz		
Phasors		
Ambient conditions		
Temperature (units °C)	16/32-bit analog input Floating point analog input *	Measured value
Humidity (%)		
Wind (knots)		
Operating conditions		
Impedance (ohms)	16/32-bit analog input Floating point analog input*	Measured value
Ground fault (current)		
Ground fault (status)	Binary input	Single-point info
Transformer temp (units °C)	16/32-bit analog input Floating point analog input*	Measured value
Xformer fans (on/off)	Binary input	Single/double point info
Xfmr oil pumps on/off	Binary input	Single/double point into
Communications SNR (dB SINAD)	16/32-bit analog input Floating point analog input*	Measured value
Status/counters		
Breaker open/close	Binary input	Single/double point info
	16/32-bit binary counter	Integrated totals
Reclosing on/off	Binary input	Single/double point info
	16/32-bit binary counter	Integrated totals
Fast trip relay in/out	Binary input	Single/double point info
	16/32-bit binary counter	Integrated totals
Operation counter	16/32-bit binary counter	Integrated totals
Tap position	16/32-bit analog input	Step position info
Controls		
Command	Control relay output block	Single command, double command, regulating step command

Table A.4—Data elements with utility-specific definitions (continued)

Utility-specific data element	DNP3 implementation	IEC 60870-5-101 (1995-11) implementation
Limit settings	16/32-bit analog output Float analog output* 16/32-bit analog input reporting deadband*	Parameter activation
Trigger settings	16/32-bit analog output Float analog output *	Parameter activation
Operating set points	16/32-bit analog output Float analog output*	Setpoint command
Regulation setting	16/32-bit analog output Float analog ouput*	Setpoint command
Alarms		
Faults (Status and point ID only)	Binary input change	Event of protection equipment single/double point info
Device operation	Binary input change	Event of protection equipment single/double point info
Station lockout	Binary input change	Event of protection equipment single/double point info
Feeder lockout	Binary input change	Event of protection equipment single/double point info
Sequence of events	Binary input change with time	Event of protection equipment single/double point info
Device programming		
Configuration (File transfer download)	File identifier* Octet strings	Parameter activation
Database (Read or write data)	File identifier* Device profile (read)*	File transfer
Fault records		
Event data Fault/unit ID Event profile Event detail data Target information	File identifier* Private registration object**	File transfer
Time		
Time sync command	Time and date	Clock synch command
Time stamp of event (day, hh:mm:ss:msec)	Binary input change with time 16-bit/32-bit/float analog input change with time* 16-32/32-bit/float frozen analog input with time of freeze* 16-bit/32-bit/float frozen analog change event with time* 16/32-bit frozen counter with time of freeze*	Event of protection equipment with time tag single/double-point info with time tag step position info with time tag integrated totals with time tag output circuit info with time tag
Duration of event (hh:mm:ss:msec)	16/32-bit analog input with time* Delay coarse Time delay fine	Measured value

Annex B

(informative)

Protocol implementation

Information that relates the abstract protocol structure to actual applications in an electric utility system is given in B.1 for the benefit of product developers, end users, and systems integrators.

B.1 DNP3 implementation

DNP3 protocol implements request-reply transactions. The master side of the protocol issues request for data or control, and the slave device responds with the requested data or the control feedback.

In most cases, an implementer will either be designing the master side of the protocol (referred to as the client) or the slave/remote side of the protocol (referred to as the server). In the scope of this recommended practice, the RTU will generally be the client, and the lED will be the server.

In order to logically implement DNP3, the device vendor will decide on the appropriate answer to the following questions:

a) Will the device use the client or the server side of DNP3?

b) Which commands will the device need to have implemented?

c) What will the database mapping of the device be?

To assist in this process, the DNP user's group has generated specific implementation subsets applicable to RTU-to-IED interfaces. This recommended practice uses the subset level 2 to define support of particular message and data elements to achieve interoperation. The procedure that follows explains the process of applying the DNP3 protocol subset to a product or products.

B.1.1 Selection of client or server

DNP3 is hierarchical, and each device needs to implement either the client or server side of the protocol. The implementer is advised to use the explanation below to select the implementation wisely:

a) *Client*. A device or software that issues request for data or control actions is a client implementation. The RTU is the client in RTU to IED transactions.

b) *Server.* A device or software process that contains data or controls that another device wants to retrieve or activate. The IED is the server in RTU-to-IED transactions. The IED acquires data by measurement or computation and some are able to effect real or pseudo control operations. The client (RTU) requests this data from the server (IED) or issues control requests to it.

c) *Combination devices*. Occasionally, a device will implement both the server and the client side of the protocol. As an example, an RTU connected to an intelligent meter and a SCADA master station would need both client and server. The RTU would gather data from the meter using the client and respond to the master station using the server. In such a case, two separate serial communication ports or communication networking schemes would typically be used.

B.1.2 Command selection

DNP3 is a comprehensive protocol with an extensive range of services and functions. However, not all functions need to be implemented in the device. Only those functions that make sense to the device are required.

For example, DNP3 accommodates 16-bit and 32-bit accumulators. However, if the server device only maintains 16-bit values, it can report those counts using 16-bits. Similarly, the client can interrogate the server for its data in a nonspecific size or variation, thus allowing the server to report data in the most efficient manner.

DNP3 server devices do not need to support all functions and data variations if it does not make sense for the particular device. The protocol provides error indications when a client issues a request for a function or object that the server does not support.

B.1.3 Database mapping

In the final step of implementation, the server establishes or configures a mapping of its data to a sequential, 0-based point number. Only the data desired by the system integrator need be mapped, although some IED implementers map all of their data whether wanted or not.

The client can request data from specific points or it can request all data and filter data from those points of interest.

Server device vendors are obligated to provide documentation indicating the commands, responses, and point mapping in their device.

The complementary client function should correspond to an IED server. This means when multiple, non-similar servers are connected in a multidrop configuration to an RTU, the RTU client must support all of them. All devices will use standard DNP3 messages.

B.1.4 Maximizing interoperability using the subset definitions

The DNP3 level 2 subset defined in this recommended practice is designed to avoid a situation in which a given client (RTU) implementation must be tailored to a specific server (IED) implementation and vice versa

The DNP3 level 2 subset limits the client to issuing requests that use wild card specifiers or to only a few of the many possible point variation and range specifiers. Likewise, the server may only respond with a few of the many possible options available in DNP3. This minimizes device complexity but allows substantial flexibility, while still guaranteeing interoperability.

Vendors who wish to make use of additional, more powerful, features of DNP on their devices can choose to do so, as long as the devices can be configured to limit output to the subset when needed.

B.1.5 DNP implementation process example

For illustrative purposes, the reader is asked to consider the steps that a vendor of an intelligent meter might take to implement DNP3 on the meter to communicate with an RTU. The RTU then sends the meter data to the master station along with other directly connected I/O points. In all cases, the functionality of the DNP3 server is chosen by the vendor, and the complexity of the vendor's DNP3 server is governed by the capability of the device and the functionality sought by the vendor's customers.

a) *Meter server.* Since the meter will be interrogated for information, the meter vendor should implement the server side of the protocol. Assume that the meter performs the following functions:

1) Monitors/reports three real-time single-phase voltages, currents, and phase angles
2) Registers kWh and kVArh in two directions
3) Resets the accumulator registers to zero upon command
4) Sends a status message that the meter has been manually reset in the field, on request

b) *Object definition*. The vendor's first step is to decide which data objects to use to report the data. This is an important concept. The vendor decides which DNP data objects to use. This can be determined by looking at the DNP3 data object library and matching the appropriate object to the meter's capability.

As an illustration, DNP3 has 18 types of analog input object definitions, four static analog objects (Obj30 Var 1–4), six frozen analog objects (Obj31 Var 1–6), four analog event objects (Obj32 Var 1–4), and four frozen analog event objects (Obj33 Var 1–4). Frozen analogs, static or event type are included in the list of acceptable objets with a level 2 implementation. Vendors may include frozen analogs as long as this feature may be disabled to limit the device to level 2 acceptable objects where required. Assuming the IED vendor is building the device to be subset level 2, the number of analog objects are limited to four static types and four event types. However, there will be only one static type and one event type used for this meter. The meter has 12-bit resolution, therefore, it can use the 16-bit format, and use leading zeros to fill the frame. Secondly, the meter can set a flag on analog values to indicate an out-of-range situation, so the vendor further chooses 16-bit value with flag. Finally, assume this meter does not support time stamping of analog changes. As a result, for this meter the two objects selected are Obj30 Var02 and Obj32 Var02. For this meter, these are the only analog object definitions required. There is no need to implement other analog objects if the meter cannot develop the appropriate information for them. Similarly, the meter vendor chooses the appropriate status and accumulator freeze objects.

Also assume that the vendor chooses to define all analog events as class 2 events (Obj60 Var03).

c) *Mapping:* The next step is to set up the DNP3 object definition and mapping. Two types of point mapping schemes are typical in IEDs: configurable point map and fixed point map devices. More complex and advanced IEDs have a configurable point map. These devices allow the user to configure the DNP3 point map via a configuration utility. Configurable point map devices typically allow the user to configure specific points into the DNP3 point map and their order occurrence. Fixed point map devices have a vendor defined map that can not be changed by the user. For this example, assume the meter vendor elects to use the following fixed point mapping of actual values to the objects which are communicated by the meter:

Object	Actual value definition
DNP3 analog point 00	Phase A volts
DNP3 analog point 01	Phase B volts
DNP3 analog point 02	Phase C volts
DNP3 analog point 03	Phase A amps
DNP3 analog point 04	Phase B amps
DNP3 analog point 05	Phase C amps
DNP3 analog point 06	Phase A phase angle
DNP3 analog point 07	Phase B phase angle
DNP3 analog point 08	Phase C phase angle
DNP3 accumulator point 00	Kilowatthours in
DNP3 accumulator point 01	Kilowatthours out
DNP3 accumulator point 02	Kilovarhours in
DNP3 accumulator point 03	Kilovarhours out
DNP3 Status Point 00	Meter has been manually reset

d) *Developing the data format/function code responses*. The third step is for the meter (lED) vendor to develop the server side of the protocol. This enables the meter to recognize the appropriate DNP3

master device or client requests and respond. In other words, the meter vendor should now use the DNP3 function codes and definitions to determine what the meter will do.

If this device is to be subset level 2 conformant, the poll requests that a level 2 server must be capable of parsing are clearly defined in DNP3 subset level 2 definition (See Table 3).

Analog information is sent by the meter when it receives a request from a master device for 16-bit values corresponding to the analog data addresses. But, the DNP3-L2 subset definition (Table 3) says that the only request an lED must accept regarding its analog inputs is a wild card request for all analog input points, with no point range or object variation specified (Obj30 Var0). The lED in this example need only respond to this request with its 16-bit analog input objects, as discussed earlier. Similarly the device may return analog events via a poll for Obj60 Var03 (class 2 events) as indicated in B.1.5, item b).

To any other request, the meter returns an error response such as PARAMETER ERROR or UNKNOWN OBJECT. This tells the master it has asked for data the meter cannot provide. Similarly, the meter vendor will choose and implement responses to the appropriate accumulator and status requests.

e) *Determining internal indications and error responses*. DNP3 provides many functions for reporting errors and other conditions to the client/RTU device. Some of these are required by the protocol and the DNP3 subset definitions, but others are optional. For instance, it is required that a device set a RESTART indication in its responses to indicate that it has rebooted since it was last polled. On the other hand, the meaning of the DEVICE TROUBLE indication is device-specific. A meter vendor may choose not to use it, or may use it to indicate a fault on its inputs. The LOCAL/REMOTE indication would make no sense at all on a meter with no controls.

   For some devices, portions of an incoming message may be “don’t care.” For instance, if a meter chooses to never send unsolicited responses, it could ignore the source address of any incoming frame, and simply reply to any device that polled it**.** The destination address of an incoming frame could be “don’t care” also, although it would eliminate the ability to have multiple devices share a common link.

f) *Documenting the implementation*. The final step is to document the functions and features implemented. The DNP3 subset definitions specify a common format for providing this information, called the DNP3 device profile document. This will convey to the client developer(s) the specific functions the IED will respond to and the data that will be returned.

   Given the device profile document of the lED, the RTU vendor can then choose the appropriate request messages to send to the IED that will gather the information the SCADA master station or other users require. A simpler RTU may choose to limit its requests to those found in the DNP3-L2 subset, using the same request messages for all IEDs. A more complex RTU may make specific requests to different IED types to conserve bandwidth.

B.1.6 Interchangeability and impact on DNP3 implementation

The use of the DNP subset definitions and device profile documents will ensure interoperability between devices at the protocol level. The goal of many users, however, is to reach interchangeability between devices, so that different DNP3 devices with the same functionality (e.g., meters) could be mixed and matched without changing the databases at the RTU or the SCADA master. The realization of this goal will not occur because of the protocol but will be instead driven by market factors. To explore this idea, consider the situation of the example meter vendor developing the server.

When the meter vendor (now called Vendor A) begins development, it is found that the Meter Company B has already implemented DNP3. Upon inspection of the implementation, Meter Vendor A discovers that the Meter B implementation performs the following:

a) Monitors and reports on real-time three single-phase voltage, current, and phase angle

b) Also reports three-phase watts and volt-amps reactive (VArs)

c) Registers kilowatthours and kilovarhours in two directions

Meter Vendor A has some decisions to make. To implement the same exact server, Vendor A's meter will have to create the 3-phase watts and VArs function, perhaps requiring product development. Alternately, zeros can be sent for the 3-phase watts and VArs values whenever requested. As for functions of the accumulator values and the status point, these features of Vendor A's product will go unused by DNP3. It is a market-driven decision when a vendor determines the functions to be supported by a DNP3-compatible device as a trade-off with the user convenience of having two or more product sources for the identical data.

Table 6 shows the implementation of the single meter server. Table B.1 shows a common DNP3 implementation, and the variations possible where two vendor IEDs have different capabilities and do not necessarily contain all functions of the common implementation.

Table B.1—Meter implementation, two vendors—example

Meter B functions	Register		DNP3 implementation				Meter A functions	Register	
	Size	Flag	Object	Size	Flag	Point		Size	Flag
Phase A volts	12 bit	Yes	Analog	16 bit	Yes	0	Phase A volts	12 bit	Yes
Phase B volts	12 bit	Yes	Analog	16 bit	Yes	1	Phase B volts	12 bit	Yes
Phase C volts	12 bit	Yes	Analog	16 bit	Yes	2	Phase C volts	12 bit	Yes
Phase A amps	12 bit	Yes	Analog	16 bit	Yes	3	Phase A amps	12 bit	Yes
Phase B amps	12 bit	Yes	Analog	16 bit	Yes	4	Phase B amps	12 bit	Yes
Phase C amps	12 bit	Yes	Analog	16 bit	Yes	5	Phase C amps	12 bit	Yes
A Phase angle	12 bit	Yes	Analog	16 bit	Yes	6	A Phase angle	12 bit	Yes
B Phase angle	12 bit	Yes	Analog	16 bit	Yes	7	B Phase angle	12 bit	Yes
C Phase angle	12 bit	Yes	Analog	16 bit	Yes	8	C Phase angle	12 bit	Yes
NO OP			Analog	16 bit	No	9	3-phase kilowatt-hours	16 bit	No
NO OP			Analog	16 bit	No	10	3-phase kilovar-hours	16 bit	No
Kilowatthours in	16 bit	No	Counter	16 bit	No	0	NO OP		
Kilowatthours out	16 bit	No	Counter	16 bit	No	1	NO OP		
Kilovarhours in	16 bit	No	Counter	16 bit	No	2	NO OP		
Kilovarhours out	16 bit	No	Counter	16 bit	No	3	NO OP		
Manual reset		Yes	Status	1 bit	No	0	NO OP		
Acknowledge				1 bit	No	0	NO OP		

B.1.7 Implementation rules and recommendations

There are several constraints on the presently defined subset implementation of DNP3 that are in addition to those described in the DNP 3.0 "Basic 4 Document Set." There are rules regarding those parts of the protocol that devices should satisfy in order to conform to any DNP3 implementation level. Also, recommendations are given regarding further behavior that a device may choose to implement. The purpose of these additional rules and recommendations is to limit the possible variations of implementation and encourage standardization. These rules are summarized in Annex A. Table B.2 lists the function codes for clients and servers.

Table B.2—RTU device implementation A—function code summary function codes supported from server to client

Code	Definition
0	Confirm
1	Read
2	Write
3	Select
4	Operate
5	Direct operate (ack)
6	Directe operate (no ack)
7	Immediate freeze (ack)
8	Immediate freeze (no ack)
13	Cold restart
20	Enable spontaneous (unsolicited) messages
21	Disable spontaneous (unsolicited) messages
22	Assign classes
23	Delay measurement
Function codes supported from server to client	
0	Confirm
129	Response
130	Spontaneous message (unsolicited function code)

NOTE—All objects do not support all function codes. In addition, objects only support the functions specified in this table.

B.2 DNP3 implementation examples

Table B.3 through Table B.5 are taken from actual examples of implementations of DNP3 in RTUs and IEDs. The information was supplied by the implementers and is for illustration only, with strict DNP3 protocol subset level 2 rules not used.

The following DNP3 function request codes are supported. Use of other function codes by the host will cause Bit 0 ("Function code not implemented") to be set in the second octet of the IIN of the response.

Table B.3—RTU device implementation A—objects summary

Object description	Number	Variation	Type	Functions supported
Binary input change—all variations	02	00	Event	Read
Binary input change without time	02	01	Event	Read
Binary input change with time	02	02	Event	Read
Binary input change with relative time	02	03	Event	Read
Control relay output block	12	01	Static	Select operate direct operate direct operate no ack
Binary counter—all variations	20	00	Static	Read freeze freeze—no ack freeze and clear freeze and clear no ack
Frozen counter—all variations	21	00	Frozen static	Read
Counter change event—all variations	22	00	Event	Read
Analog input—all variations	30	00	Static	Read
Analog change event—all variations	32	00	Event	Read
Analog output status—all variations	40	1	Static	Read
16-bit analog output block	41	2	Static	Select operate direct operate direct operate no ack
Time and date	50	01		Write
Class 0	60	01		Read
Class 1	60	02		Read
Class 2	60	03		Read
Class 3	60	04		Read
Internal indications	80	1		Write

NOTE—The following DNP function request codes are supported. Use of other function codes by the host will cause Bit 0 (“Function code not implemented”) to be set in the second byte of the response.

Table B.4.a—IED device implementation

Function codes	
Code	Meaning
0	Confirm
1	Read
2	Write
13	Cold restart
14	Warm restart

Table B.4.b—IED device implementation B—DNP3 IIN response codes

Byte	Bit	Description
1	1	Class 1 data available—always zero
1	2	Class 2 data available—always zero
1	3	Class 3 data available—always zero
1	4	Time-synchronization required—always zero
1	5	Outputs off-line—always zero
1	6	Device trouble—always zero
2	3	Buffer overflow—frame data received or generated exceeds *65* bytes total, reset by host NOTE—This an inappropriate use of buffer overflow.
2	4	Request in process—always zero
2	5	Configuration corrupt—always zero

B.2.1 Implementation of a different IED functionality

Table B.4.c describes application level responses to external requests, as a DNP IED responding to external DNP master requests. Table B.5 describes each object processed by the IED.

Table B.4.c—IED device implementation B—DNP3 object types (This device has only analogs and does not do change processing DNP3 object types)

DNP type	Object	Variation	Description
Not installed	2	0	Returns null response
Not installed	2	1	Returns null response
Not installed	2	2	Returns null response
Not installed	2	3	Returns null response
Not installed	22	0	Returns null response
S-32-R	30	0	32-bit analog input
S-32-R	30	1	32-bit analog input
S-16-R*	30	2	16-bit analog input
S-32-R	30	3	32-bit analog input without flag
S-16-R	30	4	16-bit analog input without flag
S-32-R	32	0	Returns null response
—	52	1	Time delay, coarse (in response to restart function)
RS	60	1	Class 0 returns all static data
RS	60	2	Class 1 (Returns null response)
RS	60	3	Class 2 (Returns null response)
RS	60	4	Class 3 (Returns null response)
W	80	1	Internal indications

NOTE—The following object types are supported. Use of other object types will cause Bit 1 (“Requested object(s) unknown”) to be set in the second byte of the IIN of the response.

Table B.5—IED device implementation C—DNP3 application messages

Object			Request		Response	
Obj.	Var.	Description	Function code	Qualifier codes	Function code	Qualifier code
N/A	N/A	Confirm (for cold/warm restart)	0	N/A	N/A	N/A
10	0	Binary output—any	1	00, 01, 06	N/A	N/A
10	2	Binary output status	1	00, 01, 06	129	00, 01
12	1	Control relay output block	3, 4, 5	17, 28	129	00, 01
12	1	Control relay output block	6	17, 28	None	N/A

Table B.5—IED device implementation C—DNP3 application messages (continued)

Object			Request		Response	
Obj.	Var.	Description	Function code	Qualifier codes	Function code	Qualifier code
20	0	Counter—any	1	00, 01, 06	N/A	N/A
20	1	32-bit binary counter (with flag)	1	00, 01, 06	129	00, 01
20	2	16-bit binary counter(with flag)	1	00, 01, 06	129	00, 01
20	5	32-bit binary counter (without flag)	1	00, 01, 06	129	00, 01
20	6	16-bit binary counter (without flag)	1	00, 01, 06	129	00, 01
30	0	Analog input—any	1	00, 01, 06	N/A	N/A
30	1	32-bit analog input (with flag)	1	00, 01, 06	129	00, 01
30	2	16-bit analog input (with flag)	1	00, 01, 06	129	00, 01
30	3	32-bit analog input (without flag)	1	00, 01, 06	129	00, 01
30	4	16-bit analog input (without flag)	1	00, 01, 06	129	00, 01
40	0	Analog output status—any	1	00, 01, 06	N/A	N/A
40	1	Analog output status 32 bit	1	00, 01, 06	129	00, 01
40	2	Analog output status 16 bit	1	00, 01, 06	129	00, 01
41	2	Analog output block	3, 4, 5	17, 28	129	00, 01
41	2	Analog output block	6	17, 28	None	N/A
N/A	N/A	Cold restart (responds obj. 52-2)	13	N/A	129	7
N/A	N/A	Warm restart (responds obj. 52-2)	14	N/A	129	7
60	0	Class-undefined by DNP	1	06	N/A	N/A
60	1	Class 0 (static objects)	1	06	N/A	N/A
60	2	Class 1 (high-priority events)	1	06	N/A	N/A
60	3	Class 2 (medium-priority events)	1	06	N/A	N/A
60	4	Class 3 (low-priority events)	1	06	N/A	N/A
80	1	Internal indications (point 7 only)	2	00, 01	129	N/A

B.3 IEC 60870-5-101 (1995-11) implementation

B.3.1 System-level implementation

Fixed-system parameters should be agreed to before devices can interoperate. To insure interconnectivity (all devices using the same media), a decision about the number of bytes (one or two) in the address field of the ASDU should be selected. For purposes of satisfying this recommended practice, two bytes will be used as the length of the address field, allowing up to 65 534 devices to be addressed. Another system parameter

that should be fixed is the length of the information object address, with lengths of one, two, or three bytes permissible.

Another system parameter variable, the number of octets in the cause of transmission, can be set to either one or two.

B.3.2 Device-level implementation

IEC 60870-5-101 (1995-11) provides data elements and services to suit a wide number of device domains. Therefore, a number of questions should be answered before beginning a 101 implementation. Some of the more important decisions facing a vendor are

a) Will the device operate in master or slave mode?
b) Which 101 commands will be supported?
c) Which 101 information (data) elements will the device's data map into?
d) Which basic application services are necessary?

B.3.3 Master or slave?

Whether or not a device will act as a master unit or a slave unit will determine which type identifiers (function codes) are supported and what information elements will be supported in both the control and monitor directions. Depending upon device functionality a subset of the allowed type identifiers may be appropriate.

B.3.4 101 information (data) elements

Valid information elements are defined in 101 and include single-point (single-bit binary) and double-point (two-bit binary) scaled values, short floating point (IEEE Std 754-1985), binary counter, single and start events for protection equipment, normalized values, single and double commands, regulating step command (for tap-changing voltage regulators), 2-, 3- and 7-byte binary time, and many others. New information elements can be added in accordance with the rules described in IEC 60870-5-4 (1993-08).

B.3.5 Basic application services

The complexity and functionality of the device will determine which basic application services need to be implemented. Will file transfers be necessary? Are frozen counters and frozen counters with reset valid information elements (data types) for the device? Can the device be remotely initialized? A number of command transmissions, clock synchronization, parameter loading, and parameter activation are also permissible using 101. The device vendor should select those that are appropriate for his application. All of these basic application services are described fully in IEC 60870-5-5 (1995-06).

B.3.6 Network topologies

The topologies are defined in IEC 60870-5-1 (1990-02) as follows:

a) *Point-to-point*. This is the simplest topology that connects two nodes, in this case a controlling station (equivalent to master station or RTU) with one link to a controlled station (equivalent to an RTU or IED).
b) *Multiple point-to-point*. The controlling station is connected to controlled stations by multiple point-to-point links. Each link would use a separate data communications port at the control center at any

time, all controlled stations are allowed to transmit data to the controlling station, which in turn may transmit messages to one or more controlled stations simultaneously.

c) *Multipoint-party line star arrangement*. The controlling station is connected to more than one controlled station by one common port at the controlling station. The lines are presumably connected together electrically at the controlling station and fed into the controlling station via a common port. At any time, only one controlled station is allowed to transmit data to the controlling station. The controlling station may transmit data either to one or more selected controlled stations or broadcast messages to all controlled stations simultaneously.

d) *Multipoint-party line bus arrangement*. The controlling station is connected to more than one controlled station by a common path. The restrictions on data transmission are the same as in the multi-point-star configuration.

e) *Multipoint-ring (party-line ring)*. The multipoint ring is not defined in detail, and it is not clear from the protocol definitions how this could be used, but it is stated that this is the preferred method of communication because of the improved availability. It assumes a break in the line anywhere will not prevent communications with the controlling station

f) *Composite*. A meshed network configuration comprising a combination of all the types described in a) through e).

For the specific scope of the recommended practice, the controlling station would be the submaster, or RTU, and the controlled station would be the IED.

For unbalanced transmission, all the above types of networks are permitted—there are no specific constraints identified. This would result in a master-slave type of operation with polling from the controlling station. However, even though LAN types of networks are envisioned, it is permitted by the 101 profile to use the application layer with typical LAN physical and data link layers. The lower two layers should be IEC 60870-5 compliant. This means that 101 does not permit use with standard LAN protocols, such as Ethernet, Token Ring, Token Bus, or EDDI. Therefore, 101 really cannot operate as a LAN, but only as a multipoint party line.

For balanced transmission, only the point-to-point and multiple point-to-point networks are permitted. Therefore, peer-to-peer operation is not possible except on point-to-point links. This is because IEC 60870-5 protocol does not define any type of media access protocol in L2, so only the controlling station can initiate communications.

B.4 101 implementation example

As an example of 101 implementation, a vendor might go through the following process for a tap-changing voltage regulator controller IED. This implementation could be used to send commands to a voltage regulator controller for remote tap-changing, communicate regulator information to an RTU for further data processing, or communicate information straight to a SCADA master station that incorporates 101, thereby bypassing an RTU. This example follows the 101 profile document step-by-step to select options for the controller implementation. Using a bottom-up approach yields the appropriate data link layer.

B.4.1 Data link layer

The data link layer transmission mode can be either balanced (full duplex) or unbalanced (half duplex) For a multidrop topology with a single master, unbalanced transmission should be used for master-slave polling. In a star network topology, the RTU is connected point-to-point with each IED, and balanced transmission is desirable so that the IEDs may act as masters by sending data without a request. For flexibility, the voltage regulator controller example offers both balanced and unbalanced transmission modes.

B.4.2 Application layer

The application layer provides the interface to the communication stack. This interface includes both the services provided and information elements supported by the communication protocol. The application layer defines the information elements that the application data maps into and which services the device supports.

Table B.6 provides a basic data list as a guide to determining how to map data to the information elements defined in IEC 60870-5-4 (1993-08) and 101.

Table B.6—IEC 60870-5-101 (1995-11) information elements

Device element	101 information element (definition)[a]
Tap position	Value with transient state indication (7.2.6.5)
Source voltage	Scaled value (7.2.6.7)
Load voltage	Scaled value (7.2.6.7)
Load current	Scaled value (7.2.6.7)
Total operations (for regulator)	Binary counter reading (7.2.6.9)
Change tap command	Regulating step command (7.2.6 17)

[a]"Definition" is the section of 101 where the information element is defined.

Other information elements and ASDUs can be defined according to the rules set forth in IEC 60870-5-4 (1993-08) and 60870-5-3 (1992-09) respectively, however their use requires agreement between the vendor and the system user. This agreement stems from the fact that another vendor may choose to implement a new ASDU using the same type identification, but the ASDU does not match a user's with the same type identifier and the user should incorporate the new ASDU(s) into the master system or RTU if taking advantage of the new information available is desired.

B.5 IEC 60870-5-101 (1995-11)—example vendor device implementation

A master station to RTU type implementation that illustrates the IEC 60870-5-101 (1995-11) profile is given in Table B.7, which consists of a function and parameter definition table. This tabular example was provided by the implementer. In the table, all parameters are listed according to a specific topic, and the specific settings chosen by the implementer within the profile are listed. A separate configuration system was furnished to allow parameter settings to be input or changed to suit applications.

Table B.7—Implementation of IEC 60870-5-101(1995-11)—parameter overview

Topic	Parameter	Settings
Bit transmission	Channel assignment	Depending on the device configuration
	Transmission rate for the command and monitoring directions together	100, 200, 300, 600, 1200, 2400, 4800, 9600, 19 200, or 38 400 bit/s
	Set RTS signal	Before transmitting or continuously
	Send delay after RTS signal	None or 1–65 535 ms
	Use of the clear to send (CTS) signal	Do not use, or use as CTS, or data carrier detect (DCD)
	Number of idle characters in monitoring direction	1–3
	Number of idle characters in command direction	1–3
	Number of receive buffers	3–20
	Maximum telegram length (including header and trailer) in command direction	10–261 characters
Link layer		
Balanced mode	DIR bit in send direction	0 or 1
	Link address	No link address, 1 octet 0–254, or 2 octets unstructured 0–65 534
	Use of individual character E5 hex	Not as positive acknowledgment instead of a short telegram with C = 00 hex or as negative acknowledgment instead of a short telegram with C = 09 hex
	Response to receiving NACK	Repeat or reject telegram to be sent
	Time-out for acknowledgments from the other station	50–10 000 ms
	Number of transmission attempts on time-out	2–225
	Channel time-out	No time-out or 1–255 s
	Pause between status scans	0–65 535 ms
	Dual channel transmission	Yes or no
	Time window for dual channel redundancy	100–65 535 ms
	—Processing of two different telegrams within the time window	Reject or transfer
	Assignment of the second channel	Channel number
Unbalanced mode	Distinction between class 1 and class 2 in the request telegram	Yes or no
	Link address	1 octet, 0–254, or 2 octets unstructured, 0–65 534
	Use of single character E5 hex	Not as positive acknowledgment instead of a short telegram with C = 00 hex or as negative acknowledgment instead of a short telegram with C = 09 hex
	Cycle time-out	No monitoring, or 1–255

Table B.7—Implementation of IEC 60870-5-101(1995-11)—parameter overview (continued)

Topic	Parameter	Settings
General	Transmission in nonspontaneous mode and information status “not topical”	Transmit or do not transmit
	Transmission in nonspontaneous mode and information status “blocked”	Transmit or do not transmit
	End of command telegram (termination)	With or without terminator
	Originator	No originator, or 0–255
	Common ASDU address	1 octet. 0–254, 2 octets unstructured, 0–65 534, or 2 octets structured, 0–255 each
	Information object address	1 octet 1–255.2 octets unstructured, 1–65 535.2 octets structured, 0–255 each, 3 octets unstructured, 1–16, 777, 215, or 3 octets structured, 0–255 each
	Test command cycle time	No test command, or 1–65 535 s
Resource management	Number of commands that can be managed simultaneously	1–32
	Maximum number of parallel halt times	0–64
	Maximum number of monitored intermediate positions	0–32
	Maximum number of fault locations held	0–16
Image presetting	Single indication	0 or 1
	Double indication	00, 01 10, or 11 binary–32 767 to 32 767
	Analog value (standardized)	Per IEEE Std 754-1985
	Analog value (conditioned value IEEE floating point)	
	Transformer tap position	0–255
	Metered value	0–2 147 483 647
	Sequence number for metered value	0–2 147 483 647
	Bit pattern	0–7FFFFF hex
	Protection data	0 or 1
Command direction	Identifiers for private area in IEC qualifier of command	Identifiers 16–32 inactive or active
	Command output duration for each identifier	0.01–655.35 s, step 0.01 s
One- or two-bit-command with switching direction from telegram	Address of the information object	(See under general)
	Switching direction	Takeover or invert
	Command output duration	
	No additional definition	0.01–655.35 s, step 0.01 s
	Short pulse duration	0.01–655.35 s, step 0.01 s
	Long pulse duration	0.01–655.35 s, step 0.01 s
	Assignment of the command destination	Name of the command output, if necessary, with the associated feedback signal or name of the operating sequence to be executed
Setpoints	Address of the information object	(See under general)
	Type of setpoint	Analog setpoint in relative value format (unconditioned value), analog setpoint in floating point format (conditional value) or digital setpoint as bit pattern with 32 bit
	Assignment of the setpoint destination	Name of the setpoint output

Table B.7—Implementation of IEC 60870-5-101(1995-11)—parameter overview (continued)

Topic	Parameter	Settings
Monitoring direction	Types of information objects	Single indication Double indication Normalized analog value, (unconditioned value, ±15bits) Analog value in floating point format Per IEEE transformer taps, metered values, bit patterns, or protection data
Transmission lists Settings for each transmission list	Total number of transmission lists Maximum telegram length for block assembly in nonspontaneous transmission lists Assignment of information objects Transmission service	To 255 20–252 Names of the information objects send/ confirm or send/no reply
Basic cycle list (additional settings)	Priority raising Number of telegrams for priority raising Priority for priority raising	Yes or no 1–255 telegrams 1–15
Scan list (additional settings)	Priority of the list Number of telegrams per initiations Scan group Activation by operational event	1–15 All or 1–255 General scan, group 1–16, all meters, or meter group 129–132 No
Spontaneous list “telegram buffer” (additional settings)	Method for telegram buffer overflow Type of telegram buffer Priority of the list Max number of telegrams in the telegram buffer Telegram buffer warning limit Validity duration of the telegram buffer entries	Overwrite oldest entry Clear buffer content and enter current telegram, or Retain buffer content and reject current telegram With or without time stamp 1–15 10–2550, step 10 10–2550, step 10 Always valid, or 1–255 mm
Settings for each information element	Spontaneous transmission mode Assignment to nonspontaneous transmission lists Address of the information object Assignment of the source	None Via initiation buffer Via telegram buffer with real-time Via telegram buffer without real-time or double transmission (with names of the required spontaneous list) None or list names of the required scan list or basic cycle list (see under general) Information name
Single indication (additional settings)	Type of transmission Halt a raised indication in the image Halt time with time delay	Raised/cleared, pulse or transient Do not halt, halt time until command was received, or until command received or halt time 0.1–255s, step 0.1 s

Table B.7—Implementation of IEC 60870-5-101(1995-11)—parameter overview (continued)

Topic	Parameter	Settings
Analog value (additional settings)	Smoothing factor threshold Threshold reference only spontaneous (initiation for transmission to the transmission image) Halt fault locations in the images Transmit cleared fault locations	No smoothing, or 2–7 No threshold monitoring, or 0.1–100%, or step 0.1% No or yes (global for analog values) Clear immediately after transmission, do not clear, or halt for 0 1–6553 4 s, step 0.1 s Yes or no
Normalized analog value (additional settings)	Analog value format in the telegram with unconditioned value as analog value source Telegram value with rated value (100%) with conditioned value as analog value source Telegram value with rated value (100%) Rated value	Normalized or scaled 1–32 767 1–32 7 Per IEEE Std C37.1-1994
Floating point analog value (additional settings)	Scaling factor Reference value for threshold formation (absolute)	Per IEEE100 Per IEEE100
Initiation buffer (additional settings)	Priority of the list Globally for all initiation buffers if halt is parameterized for the raised state Always transient indications Always transmit raised, raised/cleared indications	1–15 No or yes No or yes