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

Sponsor

Substations Committee
of the
IEEE Power Engineering Society

Approved 16 September 1997

IEEE Standards Board

Abstract: A uniform set of guidelines for communications and interoperations of Intelligent Electronic Devices (IEDs) and Remote Terminal Units (RTUs) in an electric utility substation is provided. A mechanism for adding data elements and message structures to this recommended practice is described.
Keywords: IED, master station, RTU, slave, Supervisory Control and Data Acquisition (SCADA) systems

The Institute of Electrical Engineers, Inc.

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

ISBN 1-55937-982-0

Introduction

(This introduction is not part of IEEE Std 1379-1997, IEEE Trial-Use Recommended Practice for Data Communications Between Intelligent Electronic Devices and Remote Terminal Units in a Substation.)

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

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

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

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

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

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

Ken Jackson, *Chair*
John T. Tengdin, *Vice Chair*

William J. Ackerman
Mark Adamiak
Lawrence A. Barto
George J. Bartok
Donald Berkowitz
Hans Bjorklund
Wayne R. Block
Dennis L. Carr
William J. Cheetham
Larry Clark
Mason Clark
Richard Clark
Ken Cooley
John W. Dean
Michael Dood
Randall Ehlers
James W. Evans
Ron J. Farquharson
Thomas E. Gasparich
Floyd W. Greenway
Daniel Gregory
Glenn Harmon
G. Roger Jensen
Danny L. Johnson
Rick Joyce
Mark J. Kempker
Stanley Klein
Roderic L. Kreger
Terry L. Krummrey
Carl J. LaPlace, Jr.
Kenneth E. Lindler
Gregory L. Luri
Sioe Mak
John D. McDonald
Jeff McElray
Harish I. Mehta
Gary Michel
Gary Moore
John Newbury
Dan Nordell
Wally Prystajecky
Gregory M. Robinson
Clarence J. Sasso
Terry Saxton
George Schimmel
Russ Schoetker
Samuel C. Sciacca
Allen R. Skopp
H. Lee Smith
Robert C. Sodergren
Stanley R. Sykes
Norman Tweed
Eric Udren
Tony Watson
James A. Whatley
Joe N. Wilson
Peter S. Wong
Ray Wright
Walt Yeager

The following persons were on the balloting committee:

William J. Ackerman
Alexander P. Apostolov
Lawrence A. Barto
George J. Bartok
Michael J. Bio
Wayne R. Block
James C. Burke
Dennis L. Carr
William J. Cheetham
Frank Y. Chu
Ken L. Cooley
Robert Corlew
James G. Cupp
John W. Dean
W. Bruce Dietzman
Michael Dood
Gary R. Engmann
James W. Evans
Ron J. Farquharson
Floyd W. Greenway
Daniel C. Gregory
R. J. Hellweg
Kenneth Jackson
Danny L. Johnson
Alan E. Kollar
Roderic L. Kreger
Terry L. Krummrey
Luther W. Kurtz
Carl J. LaPlace, Jr.
H. Peter Lips
John D. McDonald
Gary L. Michel
Philip R. Nannery
James S. Oswald
Gregory M. Robinson
Samuel C. Sciacca
June Singletary, Jr.
Allen R. Skopp
H. Lee Smith
Robert C. Sodergren
Charles V. Stoll
Stanley R. Sykes
John T. Tengdin
Mark Vainberg
Tony Watson

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

CLAUSE PAGE

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

1. Overview

This trial-use recommended practice consists of descriptions and tabular information for implementation of common communication functions among Intelligent Electronic Devices (IEDs) in electric utility substation applications.

1.1 Scope

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

1.2 Purpose

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

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

1.3 Distributed Network Protocol (DNP) 3.0

The DNP protocol was developed by Harris Canada (formerly Westronic, Inc.) in order to stabilize the expansion of unique protocols used to communicate between SCADA RTUs and a variety of IEDs. The DNP protocol used as its basis several IEC 60870-5 documents that were then in development; but extended and/or modified these to accommodate North American preferences and practices.[1] Work has been done to harmonize the IEC 60870-5 documents, which were later made International Standards, with the DNP variations, but this has not been completed.

DNP is essentially a three-layer protocol using the layers 1, 2, and 7 of the ISO/OSI communications profile set. It is specifically designed for data acquisition and control applications, and focuses its application information in the area of electric utility data transmission. This recommended practice specifies the Level 2 subset implementation of DNP 3.0 as published.

1.4 IEC 60870-5 protocol

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

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

Another document developed by IEC TC57 WG03 is IEC 60870-5-101 (hereinafter referred to as T101), a companion standard (profile) that contains definitions specific to RTUs and IEDs.

Other companion standards that support the communications requirements for other utility devices are being defined, and are known as IEC 60870-5-102 (T102) and IEC 60870-5-103 (T103) . The draft T103 (as presently proposed) includes parts of a protection device communication protocol originally developed for use in German protective relay systems. T103 deals with the informative interface, exchanging only data that is not related to protection coordination. The preliminary version of T103 has received endorsement by users and vendors in the United Kingdom, Spain, and Germany.

2. References

This recommended practice is based on two sets of published documents that provide the basic definitions and underlying principles of the communication protocol. Each released document set is available from the sponsor for a nominal reproduction fee. This recommended practice shall be used in conjunction with the following publications.

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

2.1 DNP 3.0 Documents

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

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

[1]Information on references can be found in Clause 2..
[2]DNP publications are available from Secretary, DNP User Group, c/o Harris Canada, Inc., 4525 Manilla Rd. S.E., Calgary, AB T2G 4B6, Canada, fax (403) 243-1815.

2.2 IEC 60870-5 publications

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

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

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

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

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

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

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

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

3. Definitions

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

3.1 Specific DNP/IEC 60870-5 terms

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

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

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

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

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

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

[3]IEC publications are available from IEC Sales Department, Case Postale 131, 3, rue de Varembé, CH-1211, Genève 20, Switzerland/Suisse. IEC publications are also available in the United States from the Sales Department, American National Standards Institute, 11 West 42nd Street, 13th Floor, New York, NY 10036, USA.
[4]IEEE publications are available from the Institute of Electrical and Electronics Engineers, 445 Hoes Lane, P.O. Box 1331, Piscataway, NJ 08855-1331, USA.
[5]The numbers in brackets correspond to those of the bibliography in Annex B.

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

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

3.1.9 configuration information: The data or information that defines the operational limits and characteristics of a particular device. Depending on the device, this information is either manually downloaded into NVRAM or EEPROM, or is pre-programmed into EPROM.

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

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

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

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

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

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

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

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

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

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

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

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

3.1.22 NUL: The null character (‘\0’).

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

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

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

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

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

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

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

3.1.30 slave: A device that gathers data or performs control operations in response to requests from the master, and sends response messages in return. A slave device may also generate unsolicited responses (DNP 3.0 specific).

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

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

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

3.1.34 telecontrol: *Syn:* **SCADA.**

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

3.2 Acronyms and abbreviations

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

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

4. Description of IED-to-RTU communications needs

The definition of a suitable substation communication protocol could not begin without an understanding of the technical basis for previous interdevice communication methods in the electric utility industry. The SCADA system is the most widely-understood model for such communications. The RTU function in the traditional SCADA protocol is well defined and not within the scope of this document [B3] [B4]. However, the capability of the RTU to communicate with increasing numbers and types of other intelligent devices in a substation is required by many users, hence the creation of IED-to-RTU communications requirements.

The substation IED may be a data acquisition device only, or may also provide control or protection. Therefore, the IED typically requires the input of configuration, setting, and command data, while it provides values, conditions, status, and results as output. Much of these data items are comparable to SCADA data sent between the substation and master station. The goals of IED-to-RTU communications are very similar to SCADA communications, but on a local basis.

4.1 The traditional SCADA protocol

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

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

The SCADA protocol between master and RTU forms a viable model for IED-to-RTU communications, therefore, the DNP 3.0 and IEC 60870-5-T101 (1995) protocols in this recommended practice are SCADA-based protocols.

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

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

4.2 Specific criteria to select protocols for IED/RTU communication

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

a) *Real time IED/RTU:* The protocol shall support direct IED/RTU communication without unnecessary delays, but not necessarily peer-to-peer interoperability.
b) *Existing protocol:* The protocol shall be fully developed and offered by a sponsor, or fully described by a standards-making body.
c) *Fully descriptive:* The protocol shall be uniquely identified by its name, and support the minimum functions of data acquisition, control execution, time synchronization, accumulator control, and parameter downloading to IEDs.
d) *Media independent:* The protocol shall be able to operate over physical layers of wire, coax, radio, and fiber optic media.
e) *Addressable:* The protocol shall support multiple addresses of nodes and/or devices over a common channel.
f) *Secure from errors:* The protocol shall provide a method of detection, and either reject or correct corrupted messages, using “Cyclic Redundancy Check” or better error detection/correction.
g) *Data selectable:* The protocol shall allow certain specified data to be requested and sent, and not be restricted to a “poll-for-all-data” operation.
h) *OSI model-compliant:* The protocol shall adhere to the layer structure of the OSI model for at least layers 1, 2, and 7. It should make maximum use of international/national standards wherever possible.
i) *Documented:* The protocol shall be documented by at least a functional specification, data element/object definition, and 3-layer definition.
j) *Public domain:* The protocol shall be implementable by vendors and users without licensing fees or restrictions beyond a nominal fee for documentation that may be charged by the sponsor.
k) *Easy-to-interface:* The protocol shall be implementable using an asynchronous serial port (UART-like device), and be compatible with an 8 b microprocessor using standard interface hardware/software.

l) *Multiple sources of hardware:* Hardware needed to implement the protocol software shall be available from at least two independent vendors.
m) *LAN:* The protocol shall operate over a common communications channel for all substation devices. It is not restricted to point-to-point communication. The protocol should tolerate node/device failure on the common network.
n) *UCA-compliant:* The protocol shall have a migration path to EPRI/UCA harmonization.

5. Recommended practice for IED/RTU communication

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

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

5.1 General application practice using DNP 3.0

The DNP 3.0 is specifically developed for interdevice communication involving SCADA RTUs, and provides for both IED-to-RTU and master-to-IED/RTU. It is based on the three-layer Enhanced Performance Architecture (EPA) model contained in the IEC 60870-5 standards, with some alterations to meet additional requirements of a variety of users in the electric utility industry.

DNP 3.0 was developed with the following goals:

a) *High data integrity:* The DNP 3.0 Data Link Layer uses a variation of the IEC 60870-5-1 (1990) frame format FT3. Both data link layer frames and application layer messages may be transmitted using confirmed service.
b) *Flexible structure:* The DNP 3.0 Application Layer is object-based, with a structure that allows a range of implementations while retaining interoperability.
c) *Multiple applications:* DNP 3.0 can be used in several modes, including:
    1) Polled only;
    2) Polled report-by-exception;
    3) Unsolicited report-by-exception (quiescent mode);
    4) Mixture of the modes 1)– 3).

    It can also be used with several physical layers, and as a layered protocol is suitable for operation over local and some wide area networks.
d) *Minimized overhead:* DNP 3.0 was designed for existing wire-pair data links, with operating bit rates as low as 1200 b/s, and attempts to use a minimum of overhead while retaining flexibility. Selection of a data reporting method, such as report-by-exception, further reduces overhead.
e) *Open standard:* DNP 3.0 is a non-proprietary, evolving standard controlled by a users' group whose members include RTU, IED and master station vendors, and representatives of the electric utility and system consulting community.

5.1.1 Data link layer

The DNP V3.00 data link layer specification describes the frame format, services, responsibilities, and transmission procedures for the data link layer. It describes the required services to be provided by a DNP 3.0 physical layer. DNP 3.0 is essentially media-independent when the physical layer interface meets these requirements. For instance, if unsolicited messaging is used, the physical layer shall provide an indication of whether the link is busy, which is necessary for collision avoidance. The DNP V3.00 data link layer specification also relates the DNP 3.0 data link layer to IEC 60870-5-1 (1990) and IEC 60870-5-2 (1992) standards. The primary difference is that DNP 3.0 uses the FT3 frame format for asynchronous, rather than synchronous, transmission. DNP 3.0 also adapts the IEC 60870-5 addressing to include both a source and destination address in the frame. This addition enables the use of multiple master stations and peer-to-peer communications using DNP 3.0.

5.1.2 Transport functions

The DNP V3.00 transport functions specification describes the format and procedures associated with a single octet of overhead used to segment application layer messages into data link layer frames. These transport functions are not a proper transport layer, nor part of the data link or application layer overhead. For more discussion of the pseudo-transport layer, refer to 7.3.

5.1.3 Application Layer

The DNP V3.00 application layer specification describes the message format, services, and procedures for the application layer. The services and functions provided are based on the basic application functions described in IEC 60870-5-5 (1995) documentation, although the terminology used to describe these functions differs. Distinctive DNP 3.0 features include the following:

a) 16 b device addresses;
b) 32 b point addresses of each data type per device;
c) Broadcast addressing;
d) Configuration and file transfer (not currently in this trial-use recommended practice);
e) Time of day and date synchronization;
f) Time-stamped event data;
g) Polling by data priority level;
h) Support for all common industry data types including binary input and output (controls), analog input and output (setpoints), counters/accumulators, BCD, and IEEE floating point (the latter two are not currently addressed in this recommended practice);
i) Freezing and clearing counters;
j) Solicited or unsolicited reporting of exceptions such as Buffer Overflow, Device Restarted, Device Trouble, Device in Local Operation Mode, Time Synchronization Required, Invalid Message, Point On-line/Off-line, Analog Point Over-Range, Counter Point Overflow, Downstream Communications Lost;
k) A variety of reporting mechanisms, as discussed in a) through j);
l) A variety of control operations, including select-before-operate, direct/immediate-operate, trip/close, latch on/off, pulse on/off, automatic repetition, binary output patterns, and more;
m) Remote starting/stopping of software applications (not currently addressed in this recommended practice).

5.1.4 Data object library

The DNP V3.00 data object library document describes the format of data presented within an application layer message. A variety of qualifier codes and variations of data permit an implementation of DNP 3.0 to make optimal use of bandwidth. DNP objects are not general-purpose objects; they are defined specifically for RTU operation.

5.1.5 Subset definitions

The DNP V3.00 subset definitions document describes three basic levels of DNP 3.0 objects and services that can be used to determine interoperability between devices, or to specify a minimum required level of implementation in a request for proposals. The intended use of these subsets is as follows:

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

Level 2 (L2): Intended for a more sophisticated IED or a small RTU;

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

These subset definitions ensure interoperability while allowing vendors to competitively provide value-added features to a minimum subset of the protocol. To conform to a given subset, a device must act in the following ways:

a) Be able to parse a given set of incoming messages;
b) Be configurable to transmit only a given set of outgoing messages;
c) Obey implementation rules specified in the DNP V3.00 subset definitions;
d) Be described by a published DNP 3.0 device profile document.

This recommended practice defines a subset of the DNP 3.0 standard corresponding to Level 2 (L2) of the DNP V3.00 Subset Definitions. To follow this recommended practice, the device shall conform to the subset L2. Note that the subsets represent a minimum implementation. Nothing prevents a pair of devices from using features not defined in the subset, provided that the following is true:

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

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

5.2 General application practice using IEC-60870-5 standards

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

IEC 60870-5 does not define one particular protocol profile; but rather like EPRI/UCA, it specifies a number of frame formats and services that may be provided at different layers. IEC 60870-5 is based on a three-layer Enhanced Performance Architecture (EPA) reference model for efficient implementation within RTUs, meters, relays, and other IEDs. Additionally, IEC 60870-5 defines basic application functionality for a user layer, which is situated between the OSI Application Layer and the application program. This user layer adds interoperability for such functions as clock synchronization and file transfers. The following descriptions provide the basic scope of each of the five documents in the base IEC 60870-5 telecontrol transmission protocol specification set.

Standard profiles are necessary for uniform application of the IEC 60870-5 standards. Such profiles have been and are being created. The T101 profile is described in detail following the description of the applicable standards.

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

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

5.3 Functionality of the T101 companion standard profile

This recommended practice specifically incorporates the T101 profile. IEC 60870-5-101 (T101) is a companion standard generated by the IEC TC57 for electric utility communication between master stations and RTUs. Like DNP 3.0, T101 provides structures that are also directly applicable to the interface between RTUs and IEDs. It contains all the elements of a protocol necessary to provide an unambiguous profile definition so that vendors may create products that interoperate fully.

At the physical layer, T101 additionally allows the selection of ITU-T (formerly CCITT) standards that are compatible with EIA standards RS-232 and RS-485, and also support fiber optics interfaces.

T101 specifies frame format FT 1.2, chosen from those offered in IEC 60870-5-1 (1990) to provide the required data integrity together with the maximum efficiency available for acceptable convenience of implementation. FT 1.2 is basically asynchronous and can be implemented using standard Universal Asynchronous Receiver/Transmitters (UARTs). Formats with both fixed and variable block length are admitted. Also, the single control character I transmission is allowed.

At the data link layer, T101 specifies whether an unbalanced (include multidrop) or balanced (includes point-to-point) transmission mode is used together with which link procedures (and corresponding link function codes) are to be used. Also specified is an unambiguous number (address) for each link.

The link transmission procedures selected from IEC 60870-5-2 (1992) specify that SEND/NO REPLY, SEND/CONFIRM, and REQUEST/RESPOND message transactions shall be supported as necessary for the functionality of the end device. Additionally, T101 defines the necessary rules for devices that will operate in the unbalanced (multidrop) and balanced (point-to-point) transmission modes.

T101 defines appropriate application service data units (ASDUs) from a given general structure in IEC 60870-5-3 (1992). The sizes and the contents of individual information fields of ASDUs are specified according to the declaration rules for information elements defined in the document IEC 60870-5-4 (1993). Type information defines structure, type, and format for information object(s), and a set has been predefined for a number of information objects.

The predefined information elements and type information do not preclude the addition by vendors of new information elements and types that follow the rules defined by IEC 60870-5-4 (1993) and T101. Information elements in the T101 profile have been defined for protection equipment, voltage regulators, and for metered values, to interface these devices as IEDs to the RTU.

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

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

Finally, T101 defines a mechanism for interoperability within a particular system. It is recognized that the companion standard defines parameters and alternatives from which subsets are chosen to implement particular telecontrol systems. Certain parameter values such as the number of bytes in the common address of ASDUs represent mutually exclusive alternatives because only one value is allowed per system. Other parameters, such as the process information elements listed in the command and monitor directions, allow the specification of either the complete set or subsets, as appropriate for an application.

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

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

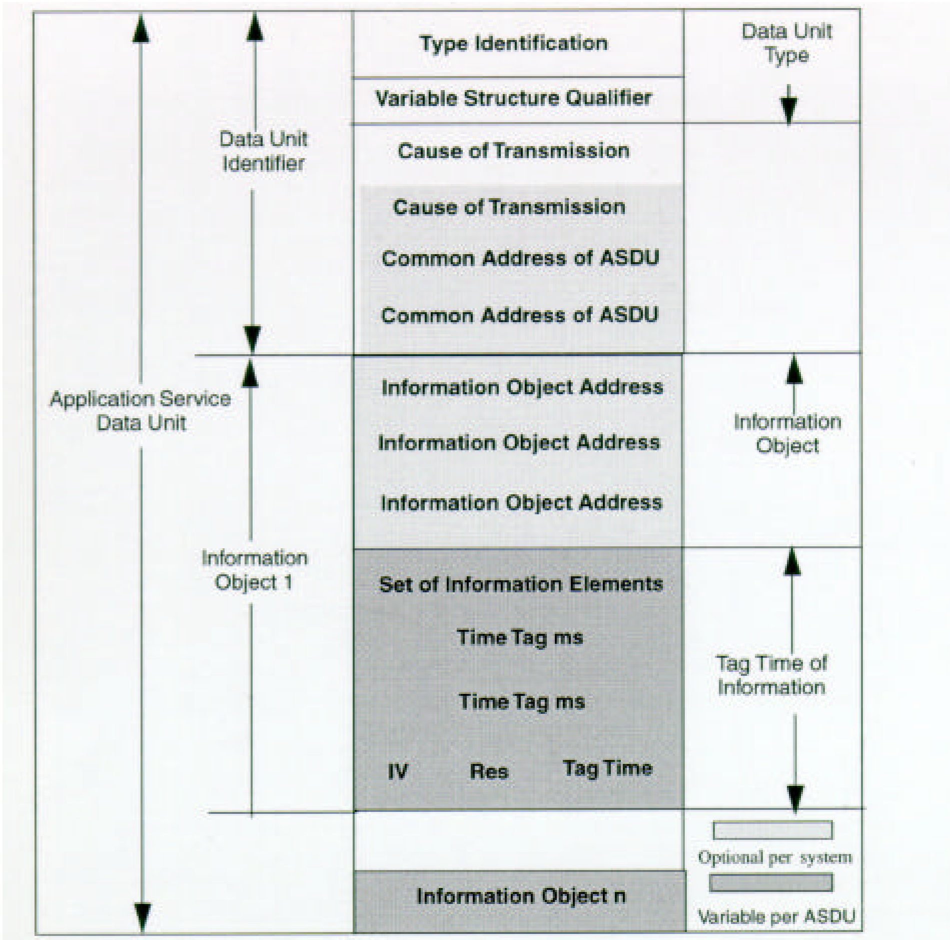
T101 also defines two new terms not found in the IEC 60870-5-1 through -5 base documents. The control direction refers to transmission from the controlling station to a controlled station. The monitor direction is the direction of transmission from a controlled station to the controlling station.

5.4 Summary comparative description tables

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

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

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



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
Information Object := CP8c+8j+8t (Information Object Address, Set of Information Elements, Time Tag (opt.))
fixed system parameter c := number of octets of Informational 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

Table 1— Communication protocol layer structure

ISO/OSI Layer	ISO/OSI Layer definition	DNP 3.0 Implementation reference	T101 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 FT1.2
4	Transport layer	Pseudo-transport layer provides segmentation for large messages	Not applicable to T101
7	Application layer	DNP V3.00 level 2 subset (DNP-L2)	Selection of ASDUs from IEC-60870-5-4
Not defined	User layer	Not applicable	IEC 60870-5-5 defines functions for clock sync. and file transfer

Table 2— Protocol message/function types

DNP V3.00 reference IEEE1379 preferred implementation			T101 reference IEEE1379 preferred implementation		
Function code	Description	Recommended	<Type ID> or (Tx Cause)	Description	Recommended
0	Confirm	Yes	(P/N=0)	Positive confirm	
			(P/N=1)	Negative confirm	
1	Read	Yes	(1)	Periodic, cyclic	
			<100>	Interrogation command	
			<101>	Counter interrogation CMD	
			<102>	Read command	
			(5–6)	Request	
			(20)	General interrogation	
			(21–36)	Group interrogation	
			(38–41)	Group counter request	
2	Write	Yes	<120–126> (13)	File transfer	
			<110–113>	Parameter of measured value	
			<103>	Clock synch command	
3	Select	Yes	<45–51> (6, 8)	Single/double command Setpoint commands Regulating step CMD activation Deactivation	
4	Operate	Yes			
5	Direct operate	Yes			
6	Direct operate– no ack	Yes			
7	Immediate freeze	Yes	<113>	Parameter activation (parameter equals time period for periodic memorization of integrated totals)	
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			

DNP V3.00 reference IEEE1379 preferred implementation			T101 reference IEEE1379 preferred implementation		
13	Cold restart	Yes	(4) <70>	Initialized End of initialization	
14	Warm restart	No			
15	Init data to default	No			
16	Initialize application	No			
17	Start application	No	<105>	Reset process command	
18	Stop application	No			
19	Save configuration	No	<120–126> (13)	File transfer	
			<113>	Parameter activation	
20	Enable unsolicited	No			
21	Disable unsolicited	No			
22	Assign to class	No	(20–41)	Group interrogations	
23	Delay measurement	Yes	<103>	Clock synch command	
129	Response	Yes	(11)	Return info—local CMD	
			(12)	Return info—remote CMD	
			<7>	Activation confirmation	
			<7>	Deactivation confirmation	
			<10>	Activation termination	
			<1–21>	Process info—monitor direction	
130	Unsolicited response	Yes	(1)	Periodic, cyclic	
			(3)	Spontaneous	
			<104>	Test command	
			<106>	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 IED-to-RTU communications interface. These are direct and serial bus topologies.

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

The serial bus or LAN topology has more than two physical nodes, with each node connected to the same channel or communication line as every other node in the serial bus network. This is often referred to as a multi-drop configuration. In this configuration, there may be one node which is deemed to be in control of the physical network. Often called the master, this node transmits to multiple nodes and receives from multiple nodes. All other nodes in the bus receive from the master node and transmit to the master node. In RTU/IED communication, the RTU is considered the master, where relevant.

In peer-to-peer communications, all devices act as slave data links and collision avoidance may be required as no single device has a higher priority, and all can transmit spontaneously.

In a multiple-master configuration, the master devices are higher priority than the slave devices.

6.1 Modes of transmission

The physical layer supported by a IED/RTU protocol shall transmit/receive data in a bit-serial mode. Generally, data are transferred in 8. b 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 IED/RTU protocol shall support half duplex operation with a two-wire circuit and full duplex and half duplex operation with a four-wire circuit. The protocol shall 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 DNP 3.0

This subclause describes the DNP 3.0 physical layer interface services that any physical layer should provide in order to accommodate the DNP 3.0 Data Link. This recommended practice is applicable to IED-to-RTU links, which rarely utilize the PSN.

The physical layer that is recommended for DNP 3.0 is a bit-serial oriented asynchronous physical layer supporting 8 b data, 1 start bit, 1 stop bit, no parity, and EIA RS-232C voltage levels and control signals. The ITU-T V.24 standard [B6] describes the DTE (Data Terminal Equipment) which is used for communication with a DCE (Data Communication Equipment) 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 shall conform (minimally) to the V.24 standard DCE definition.

The physical layer shall 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 shall 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 shall be able to return the state of the physical medium. As a minimum, the service shall indicate whether or not the medium is busy.

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

The T101 profile provides control (RTU-to-IED) and monitor (IED-to-RTU) communications compliant with the following standards. Details are contained in the ITU-T publications referenced in Annex BB. The T101 profile is as follows:

a) Control transmission direction: Either an unbalanced interchange circuit per ITU-T V.24/V.28 [B6] [B7] with data rates of 300, 600, 1200, 2400, 4800, or 9600 b/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 b/s.
b) Monitor direction: Follows the same models, but may be selected differently.

IEC 60870-5-1 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.

T101 conforms to IEC 60870-5-1 (1990) 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 [B6] recommendation is common to both the DNP 3.0 and the IEC 60870-5-101 (1995) implementations.

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

7.1 Recommended data link layer for DNP 3.0

This clause defines the DNP 3.0 Data Link layer, Link Protocol Data Unit (LPDU), as well as data link layer services and transmission procedures. Master stations, submaster stations, outstations, RTUs, and IEDs can use this data link to pass messages between primary (originating) stations and secondary (receiving) stations. In DNP 3.0 protocol, master stations, submaster stations, outstations (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 DNP 3.0 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 DNP 3.0 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 DNP 3.0 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:

1) Exchange of Service Data Units (SDUs) between peer DNP data links;
2) Error notification to data link user;
3) Sequencing of SDUs;
4) Prioritized SDU delivery;
5) Quality SDU delivery.

SDUs are only exchanged between peer DNP data links. Priority delivery can be expedited or normal to indicate a high- or low-priority request. 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 b 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 DNP 3.0 Data link layer vs. IEC 60870-5

The draft versions of IEC 60870-5-1 and IEC 60870-5-2 were the basis for developing the DNP 3.0 Data Link layer. The DNP 3.0 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 outstations, IEDs, or submaster stations not designated as master stations.

The following are specific comparisons between the DNP 3.0 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), the DNP 3.0 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 DNP V3.00, 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 DNP 3.0.

b) *Channel failover:* The DNP 3.0 data link layer communicates with only one physical layer (or channel). In IEC 60870-5-1 (1990), item 13, the session layer is responsible for maintaining channel connections. In DNP 3.0, channel failover is instead handled at the application layer.

c) *Frame format and procedures:* The DNP 3.0 data link layer uses a variable-length frame format adapted from type FT3 defined in IEC 60870-5-1 (1990). 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) 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) 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) are used by DNP 3.0 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 DNP 3.0 data link layer uses the LENGTH field as defined in IEC 60870-5-1 (1990) (6.2.4). The CONTROL field used is the as defined in IEC 60870-5-2 (1992) (6.1.2) for balanced transmission. All the function codes specified in IEC 60870-5-3(1992) (Table III) are supported. The DNP 3.0 data link frame header has two IEC address fields. Each address field is 16 b (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-T101

IEC-60870-5-2 (1992) offers a selection of link transmission procedures using a control field and optional address field; the address field is optional because 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 T101 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 “1” 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 nonseparable dialogue elements (frames) between requesting stations and responding stations. SEND/NO REPLY is a broadcast function intended for multiple destinations.

7.3 DNP 3.0 Pseudo-transport layer (ISO/OSI Layer 4)

The DNP 3.0 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). This pseudo-transport layer is described in detail in DNP V3.00. 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 DNP 3.0. 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 DNP 3.0 Data Link Layer uses the IEC 60870-5-1(1990) 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 DNP 3.0 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 DNP 3.0

This clause specifies the DNP 3.0 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 DNP 3.0 structure resembles the IEC 60870-5 simplified model known as Enhanced Performance Architecture (EPA). DNP 3.0 expands on the EPA by providing a pseudo-transport function.

Figure 2 shows the EPA structure. The user layer represents the actual IED or RTU application, and makes use of the application layer to send/receive complete messages to another DNP 3.0 compliant device.

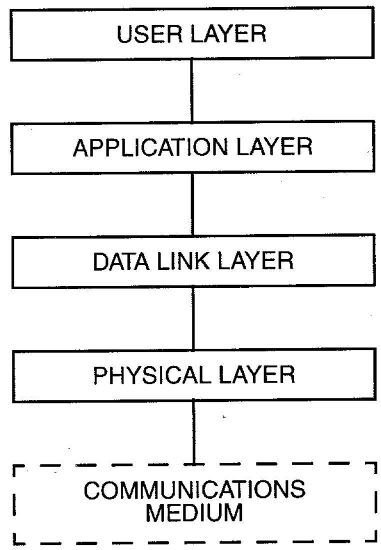


Figure 2— EPA layer organization

8.1.1 Application layer description and IEC 60870-5 comparison

The DNP 3.0 application layer APDU is based on draft versions of IEC 60870-5-3 (1992) and 60870-5-4 (1993). 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 DNP 3.0, 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 DNP 3.0, 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 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.

DNP 3.0 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 pre-assigned 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 DNP 3.0 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 (outstation) 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 DNP 3.0 application layer subset implementation table

Table 3 describes the objects, function codes, and qualifiers used in an L2 DNP 3.0 implementation. To conform to this recommended practice, a device shall also follow the implementation rules defined in the DNP V3.00 subset definitions referenced in Clause 2.. Use of a DNP device profile document as contained in Annex BB 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 DNP 3.0 object. An IED shall be able to parse a request message (shown in the request column) containing the specified object variation, function codes, and qualifiers. The RTU shall 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 DNP V3.00 application layer specification for the meanings of the function codes. Refer to the DNP V3.00 application layer specification for the meanings of the qualifier fields.

Table 3— Level 2 subset implementation of DNP 3.0 (DNP-L2)

Object			Request (IED shall parse)		Response (RTU must parse)	
Obj	Var	Description	Func Codes (dec)	Qual Codes (hex)	Func Codes	Qual 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 b binary counter			129, 130	00, 01
20	2	16 b binary counter			129, 130	00, 01
20	3	32 b delta counter			129, 130	00, 01
20	4	16 b binary counter			129, 130	00, 01
20	5	32 b binary counter without flag			129, 130	00, 01
20	6	16 b binary counter without flag			129, 130	00, 01
20	7	32 b delta counter without flag			129, 130	00, 01
20	8	16 b delta counter without flag			129, 130	00, 01
21	0	Frozen counter—all variations	1	06		
21	1	32 b frozen counter			129, 130	00, 01
21	2	16 b frozen counter			129, 130	00, 01
21	9	32 b frozen counter without flag			129, 130	00, 01
21	10	16 b frozen counter without flag			129, 130	00, 01
22	0	Counter change event— all variations	1	06, 07, 08		
22	1	32 b counter change event without time			129, 130	17, 28
22	2	16 b counter change event without time			129, 130	17, 28
30	0	Analog input—all variations	1	06		
30	1	32 b analog input			129, 130	00, 01
30	2	16 b analog input			129, 130	00, 01
30	3	32 b analog input without flag			129, 130	00,01

Object			Request (IED shall parse)		Response (RTU must parse)	
30	4	16 b analog input without flag			129, 130	00,01
32	0	Analog change event—all variations	1	06, 07, 08		
32	1	32 b analog change event without time			129, 130	17,28
32	2	16 b Analog change event without time			129, 130	17,28
40	0	Analog output status—all variations	1	06		
40	2	16 b Analog output status			129, 130	00, 01
41	2	16 b 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
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			
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.						

8.2 Recommended application layer for IEC 60870-5-T101 (1995)

IEC 60870-5-3 (1992) specifies rules for structuring application data units in transmission frames of telecontrol systems. These rules are presented as generic standards that may be used to support a great variety of present and future telecontrol applications.

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 T101 companion standard defines appropriate ASDUs from the general structure in IEC 60870-5-3 (1992) as follows:

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

b) The information object address may be 1, 2, or 3 octets, and may be structured or unstructured;
c) Cause of transmission may be 1 octet or 2 octets with originator address;
d) Station initialization may be remote or not remote;
e) General Interrogations may be global, or reference groups numbered 1–16; Addresses in each group shall 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) C_SE ACTTERM used;
    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– 4); addresses in group shall 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);
   Activate/deactivate persistent cyclic or periodic transmission of the addressed object.
k) 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)

Process information in monitor direction		
ASDU number	**Definition**	**Label used**
< 1> =	Single-point information	M_SP_NA_1
< 2> =	Single-point information with time tag	M_SP_TA_1
< 3> =	Double-point information	M_DP_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_TA_1
< 7> =	Bitstring of 32 b	M_BO_NA_1
< 8> =	Bitstring of 32 b 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_TB_1
< 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
< 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	M_EP_TB_1
< 45> =	Single command	C_SC_NA_1
< 46> =	Double command	C_DC_NA_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
<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

Process information in monitor direction		
<112> =	Parameter of measured value, short floating point value	P_ME_NC_1
<113> =	Parameter activation	P_AC_NA_1
File transfer		
<120> =	File ready	F_FR_NA_1
<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 which has a specific form and meaning. The provision of elements or objects allows implementors of the protocol to reduce development time and prevents duplication of work already completed. The data elements allow the various devices which use the protocol to quickly recognize information which is needed for further processing or response.

9.1 DNP 3.0 data element/object definition

The DNP 3.0 objects are defined in Table 3 in 8.1.2. These are derived from the Level 2 subset implementation of DNP, as generated and documented by the DNP user's group. Table 3 defines a minimum subset of the DNP objects that a device must implement. Implementors may provide more functionality than the subset, per guidelines discussed in the DNP 3.0 subset definitions and in 5.1 of this recommended practice.

9.2 IEC 60870-5 data element definition

IEC 60870-5-4 (1993) provides rules for defining information data elements. It presents a common set of information elements, in particular about digital and analog process variables, that 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. Profile T101 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

Tables 5 and 6 provide summaries of known data objects suitable for use in this recommended practice. As with Tables 1 and 2, a further comparison to other standardization efforts underway, using the same parameters, is given in Tables A.3 and A.4 in Annex A. EPRI projects are used as examples to illustrate the similarities and differences among related definition projects.

Table 5— Data objects—primitive

Parameter or generic data element	DNP 3.0 reference notation		IEC 60870-5-101 reference notation	
	Notation	Typical use in an object	Notation	Name, use
Bit notation	BSn [pos]	n = number of bits pos = bit position in word		
Bit	BS1	Binary input Control relay output block Binary output status	BS 1	
Bit string	BSn	Binary input (packed) Pattern mask (not in DNP-L2)	BS 32	
Integer 8 b unsigned	UI	To be defined		
Integer 16 b unsigned	UI16	16 b binary counter 16 b frozen counter		
Integer 16 b signed	I16	16 b analog input 16 b analog output	I16	Scaled value, 16 b analog input, 16 b analog output
Integer 32 b unsigned	UI32	32 b binary counter 32 b frozen counter	CP 40	Binary counter reading, I 32 Reading, CP 8 sequences
Floating point number—32 b	R32 (IEEE)	Short floating point (not in DNP-L2)	R32, 32	Short floating point
Boolean value	BS1	Binary input control relay output block		
Character	OS	File identifier (not in DNP-L2) Further uses to be defined; under consideration by DNP users' group		
String of characters				
Octet string				

Table 6— Meter implementation, one vendor—example

Meter Functions	Register		DNP 3.0 Implementation			
	Size	Flag	Object	Size	Flag	Point
Phase A volts	12 b	Yes	Analog	16 b	Yes	0
Phase B volts	12 b	Yes	Analog	16 b	Yes	1
Phase C volts	12 b	Yes	Analog	16 b	Yes	2
Phase A amps	12 b	Yes	Analog	16 b	Yes	3
Phase B amps	12 b	Yes	Analog	16 b	Yes	4
Phase C amps	12 b	Yes	Analog	16 b	Yes	5
A Phase angle	12 b	Yes	Analog	16 b	Yes	6
B Phase angle	12 b	Yes	Analog	16 b	Yes	7
C Phase angle	12 b	Yes	Analog	16 b	Yes	8
kilowatthours in	16 b	No	Accumulator	16 b	No	0
kilowatthours out	16 b	No	Accumulator	16 b	No	1
kilovarhours in	16 b	No	Accumulator	16 b	No	2
kilovarhours out	16 b	No	Accumulator	16 b	No	3
Manual reset	—	Yes	Status	1 b	No	0
Acknowledge	—	—	—	1 b	No	0

10. Protocol implementations

Information that relates the abstract protocol structure to actual applications in an electric utility system is given in 11.1 for the benefit of product developers, end users, and systems integrators.

10.1 DNP 3.0 implementation

The DNP protocol consists of two message sets, or pairs. The master side of the protocol contains valid statements a master device (station, RTU, or IED) can initiate or respond with, and the RTU side of the protocol contains valid statements a slave device (submaster, RTU, or IED) can initiate and respond to. In many cases (but not all), these pairs can be considered a poll or request for information/action, and a response.

In most cases, an implementer will either be designing the master side of the protocol, referred to as the data collection application (DCA) or the slave/remote side of the protocol, referred to as the data processing application (DPA). In the scope of this recommended practice, the RTU will generally be the DCA, and the IED will be the DPA.

In order to logically implement DNP 3.0, the device vendor will decide on the appropriate answer to the following questions:

a) Will the device use the DPA or DCA side of DNP 3.0?
b) Which commands will the device need to have implemented?
c) What will the data base mapping of the device be?

To assist in this process, the DNP Users' Group has generated specific implementation subsets applicable to RTU-to-IED interface. This recommended practice uses the Subset Level 2 to define support of particular message and data elements to achieve interoperation. The procedure which follows explains the process of applying the DNP 3.0 protocol subset to a product or products.

10.1.1 Selection of DCA or DPA

DNP 3.0 is hierarchical, and each device needs to implement either the DPA or DCA side of the protocol. The implementor is advised to use the explanation below to select the implementation wisely:

a) *DCA:* A device that needs to gather information from other devices on a scheduled basis for transmission upward, or is capable of sending commands to other devices, is a DCA implementation. An RTU, gathering data from an intelligent relay for transmission to the master station would be a DNP 3.0 DCA. Similarly, a PLC obtaining status and analog values from other devices for processing would also implement a DCA.
b) *DPA:* If a device provides useful data input to other devices or systems, but has no need for information from lower level systems to perform its primary function, that device should use the DPA. Meters, relays, recorders, and other devices which are to be polled for information they contain are DPA implementations.
c) *Combination devices:* Occasionally, a device will implement both the DPA and the DCA side of the protocol. As an example, an RTU connected to an intelligent meter and a SCADA master station would need both DCA and DPA. The RTU would gather data from the meter using the DCA, and respond to the master station using the DPA. In such a case, two separate serial communication ports communication or networking schemes would typically be used.

10.1.2 Command selection

DNP 3.0 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 which make sense to the device are required. This is the purpose of defined profiles or subsets of the protocol, as produced by the DNP user's group.

For example, DNP 3.0 can accommodate 16 b accumulators and 32 b accumulators. However, if the DPA device can only produce 16 b accumulator values, it need not implement the other functions. Similarly, the DCA interrogating that device need not query it for 32 accumulator values, since none exist in the device. Consequently, when implementing DNP 3.0, the implementor need only address those functions which will be applicable to the device in question. The subset definitions do require that a DPA/IED respond according to the protocol definition for all functions and objects it does not support. A meter device which does not support control operations, for instance, must respond with PARAMETER ERROR or OBJECT UNKNOWN to such requests.

10.1.3 Data base mapping

In the final step of implementation, the DPA device implementor will establish the mapping of the points. In other words, a DPA device maps the desired values to certain DNP address locations. The DCA implementor will use this mapping to determine how to take the data received from the DPA device and map the information to the proper location. In a completed DPA implementation, the vendor of the device will select and document the commands, responses and point mapping for the device.

The complementary DCA function shall correspond to the DPA of the IED. This means that an RTU connected to three different IEDs may have different DCA subset implementations. However, all devices will use the standard messages from the DNP 3.0 library.

10.1.4 Maximizing interoperability using the subset definitions

The DNP 3.0 Level 2 subset defined in this recommended practice is designed to avoid a situation in which a given DCA/RTU implementation must be tailored to a specific DPA/IED implementation and vice-versa.

The DNP 3.0 Level 2 subset limits the DCA requests to wild card requests that are simple for any DPA to parse and allow the DPA considerable flexibility in choosing what data to respond with. The subset also limits the number of object variations that a DCA must parse to about a third of the total defined in the DNP specifications. Any two devices that follow these recommended practices and conform to the L2 subset will be interoperable.

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.

10.1.5 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 DNP 3.0 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 DNP 3.0 DPA is chosen by the vendor, and the complexity of the vendor’s DNP 3.0 DPA is governed by the capability of the device and the functionality sought by the vendor's customers.

a) *Meter DPA:* Since the meter will be interrogated for information, the meter vendor should implement the DPA side of the protocol. Assume that the meter performs the following functions:
   1) Monitors/reports three real-time single phase voltages and current 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 DNP 3.0 data object library and matching the appropriate object to the meter’s capability.
   As an illustration, DNP 3.0 has 18 types of analog input object definitions. However, there will be only one type used for this meter. The meter has 12 b resolution, therefore, it can use the 16 b 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 b value with flag. For this meter, this is the only analog object

definition 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.

c) *Mapping:* The next step is to set up the DNP 3.0 object definition and mapping. For example, the meter vendor elects to use the following mapping of actual values to the objects which are communicated by the meter:

Object	**Actual value definition**
DNP 3.0 analog point 00	Phase A volts
DNP 3.0 analog point 01	Phase B volts
DNP 3.0 analog point 02	Phase C volts
DNP 3.0 analog point 03	Phase A amps
DNP 3.0 analog point 04	Phase B amps
DNP 3.0 analog point 05	Phase C amps
DNP 3.0 analog point 06	Phase A phase angle
DNP 3.0 analog point 07	Phase B phase angle
DNP 3.0 analog point 08	Phase C phase angle
DNP 3.0 accumulator point 00	kilowatthours in
DNP 3.0 accumulator point 01	kilowatthours out
DNP 3.0 accumulator point 02	kilovarhours in
DNP 3.0 accumulator point 03	kilovarhours out
DNP 3.0 status point 00	Meter has been manually reset

d) *Developing the Data Format/Function Code responses:* The third step is for the meter (IED) vendor to develop the DPA side of the protocol. This enables the meter to recognize the appropriate DNP 3.0 master device or DCA requests and respond. In other words, the meter vendor shall now use the DNP 3.0 function codes and definitions to determine what the meter will do.

Analog information is sent by the meter when it receives a request from a master device for 16 b values corresponding to the analog data addresses. But, the DNP-L2 subset definition (Table 3) says that the only request an IED must accept regarding its analog inputs is a wild card request for all analog input points, with no point range or object variation specified. The IED in this example need only respond to this request with its 16 b analog input objects, as discussed earlier. To any other request, it can return 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:* DNP 3.0 provides many functions for reporting errors and other conditions to the DCA/RTU device. Some of these are required by the protocol and the DNP 3.0 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 DNP 3.0 subset definitions specify a common format for providing this information, called the DNP 3.0 device profile document. This will convey to the DCA developer(s) the specific functions the IED will respond to and the data that will be returned.
Given the device profile document of the IED, 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 DNP-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.

10.1.6 Interchangeability and impact on DNP 3.0 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 DNP 3.0 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 DPA.

When the meter vendor (now called Vendor B) begins development, it is found that the Meter Company A has already implemented DNP V3.00. 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 DPA, 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 DNP 3.0. It is a market-driven decision when a vendor determines the functions to be supported by a DNP-compatible device as a trade-off with the user convenience of having two or more product sources for the identical data.

Table 7 shows the implementation of the single meter DPA. Table 8 shows a common DNP 3.0 implementation, and the variations possible where two vendor IEDs have different capabilities, and do not necessarily contain all functions of the common implementation.

Table 7— Meter Implementation, two vendors—example

Meter B Functions	Register		DNP 3.0 Implementation				Meter A Functions	Register	
	Size	Flag	Object	Size	Flag	Point		Size	Flag
Phase A volts	12 b	Yes	Analog	16 b	Yes	0	Phase A volts	12 b	Yes
Phase B volts	12 b	Yes	Analog	16 b	Yes	1	Phase B volts	12 b	Yes
Phase C volts	12 b	Yes	Analog	16 b	Yes	2	Phase C volts	12 b	Yes
Phase A amps	12 b	Yes	Analog	16 b	Yes	3	Phase A amps	12 b	Yes
Phase B amps	12 b	Yes	Analog	16 b	Yes	4	Phase B amps	12 b	Yes
Phase C amps	12 b	Yes	Analog	16 b	Yes	5	Phase C amps	12 b	Yes
A Phase angle	12 b	Yes	Analog	16 b	Yes	6	A Phase angle	12 b	Yes
B Phase angle	12 b	Yes	Analog	16 b	Yes	7	B Phase angle	12 b	Yes
C Phase angle	12 b	Yes	Analog	16 b	Yes	8	C Phase angle	12 b	Yes
NO OP			Analog	16 b	No	9	3-phase kilowatt-hours	16 b	No
NO OP			Analog	16 b	No	10	3-phase kilovarhours	16 b	No
kilowatthours in	16 b	No	Accumulator	16 b	No	0	NO OP		
kilowatthours out	16 b	No	Accumulator	16 b	No	1	NO OP		
kilovarhours in	16 b	No	Accumulator	16 b	No	2	NO OP		
kilovarhours out	16 b	No	Accumulator	16 b	No	3	NO OP		
Manual Reset		Yes	Status	1 b	No	0	NO OP		
Acknowledge				1 b	No	0	NO OP		

10.1.7 Implementation rules and recommendations

There are several constraints on the presently defined subset implementation of DNP V3.00 which are in addition to those described in the DNP V3.00 “Basic 4.” There are rules regarding those parts of the protocol that devices shall satisfy in order to conform to any DNP 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 8— RTU device implementation A—function code summary

Function code summary	
Function codes supported from master to outstation	
Code	Definition
0	Confirm
1	Read
2	Write
3	Select
4	Operate
5	Direct operate (ACK)
6	Direction operate (NOACK)
7	Immediate freeze (ACK)
8	Immediate freeze (NOACK)
13	Cold restart
20	Enable spontaneous (unsolicited) messages
21	Disable spontaneous (unsolicited) messages
22	Assign classes
23	Delay measurement
Function codes supported from outstation to master	
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.	

10.2 DNP 3.0 implementation examples

Tables 9 through 11 are taken from actual examples of implementations of DNP 3.0 in RTUs and IEDs. The information was supplied by the implementors, and is for illustration only, as strict DNP 3.0 L2 subset rules were not used.

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 IIN of the response.

Table 9— RTU device implementation A—objects summary

Objects summary				
Object Description	**Number**	**Variation**	**Type**	**Functions Supported**
Single-bit binary input	01	01	Static	Read
Binary input with status	01	02	Static	Read
Binary input change with time	02	02	Event	Assign class, enable spontaneous, disable spontaneous
Control relay output block	12	01	Static	Select, operate,
Direct operate				
16 b frozen counter	21	02	Frozen static	Imd Frz (Ack)
Imd Frz (NoAck),				
Read				
16 b analog input	30	02	Static	Read
16 b analog change event w/o time	32	02	Event	Assign class
Enable spontaneous,				
Disable spontaneous				
Time and date	50	01		Read, write
Time and date CTO	51	01		N/A
Un-Sync'd time & date CTO	51	02		N/A
Time delay fine	52	02		Delay measurement
Class 0	60	01		Assign class
Class 1	61	01		Assign class
Class 2	62	01		Assign class
Class 3	63	01		Assign class
File identifier	70	01		Write
Device profile	82	01		Read

Table 10.A— IED device implementation B—function codes

Function Codes	
Code	Meaning
0	Confirm
1	Read
2	Write
13	Cold restart (comm card only)
14	Warm restart (comm card only)
15	Initialize data to defaults (acknowledged but otherwise ignored)
16	Initialize application (acknowledged but otherwise ignored)
17	Start application (acknowledged but otherwise ignored)
18	Stop application (acknowledged but otherwise ignored)
22	Assign class
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 IIN of the response.	

Table 10.B— IED device implementation B—DNP 3.0 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
2	4	Request in process—always zero
2	5	Configuration corrupt—always zero
NOTE — The IIN field is fully supported.		

Table 10.C— IED device implementation B—DNP 3.0 object types

DNP 3.0 object types			
DNP Type	**Object**	**Variation**	**Description**
S-32-R	30	1	32 b analog input
S-16-R	30	2	16 b analog input
S-32-R	30	3	32 b analog input without flag
S-16-R	30	4	16 b analog input without flag
—	52	1	Time delay, coarse (in response to restart func)
RS	60	1	Class 0 (statics only)
RS	60	2	Class 1 (events only)
RS	60	3	Class 2 (events only)
RS	60	4	Class 3 (events only)
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.			

10.2.1 implementation of a different IED functionality

This table describes application level responses to external requests, as a DNP IED responding to external DNP master requests. The following table describes each object processed by the IED.

Table 11— IED device implementation C

DNP application messages						
Object			**Request**		**Response**	
Obj.	**Var.**	**Description**	**Func Code**	**Qual Codes**	**Func Code**	**Qual Codes**
N/A	N/A	Confirm (for cold/warm restart)	0	N/A	N/A	N/A
10	0	Binary output	1	6, Read	129	0,Read
10	2	Binary output status	1	6, Read	129	0,Read
12	1	Control relay output block	5	Write	5	Write
12	1	Control relay output block	6	Write	None	N/A
20	0	Counter (responds like 20-5)	1	6, Read	129	0, Read
20	1	32 b binary counter (with flag)	1	6, Read	129	0, Read
20	2	16 b binary counter (with flag)	1	6, Read	129	0, Read
20	5	32 b binary counter (without flag)	1	6, Read	129	0, Read
20	6	16 b binary counter (without flag)	1	6, Read	129	0, Read
30	0	Analog input (responds like 30-2)	1	6, Read	129	0, Read
30	1	32 b analog input (with flag)	1	6, Read	129	0, Read
30	2	16 b analog input (with flag)	1	6, Read	129	0, Read

DNP application messages						
30	3	32 b analog input (without flag)	1	6, Read	129	0, Read
30	4	16 b analog input (without flag)	1	6, Read	129	0, Read
40	0 0	Analog output sts (responds 40-2)	1	6, Read	129	0, Read
40	1	Analog output status 16 b	1	6, Read	129	0, Read
40	2	Analog output status	1	6, Read	129	0, Read
41	2	Analog output block	5	Write	5	Write
41	2	Analog output block	6	Write	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	6	129	0
60	1	Class 0 (static objects)	1	6	129	0
60	2	Class 1 (high-priority events)	1	6	None	N/A
60	3	Class 2 (medium-priority events)	1	6	None	N/A
60	4	Class 3 (low-priority events)	1	6	None	N/A
80	1	Internal indications (point 7 only)	2	Write	129	N/A

10.3 IEC-60870-5-101 Implementation

10.3.1 System-level implementation

Fixed-system parameters shall 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 shall 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 shall 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.

10.3.2 Device-level implementation

IEC 60870-5-101 (1995) provides data elements and services to suit a wide number of device domains. Therefore, a number of questions shall be answered before beginning a T101 implementation. Some of the more important decisions facing a vendor are:

a) Will the device operate in master or slave mode?
b) What T101 commands will be supported?
c) Which T101 information (data) elements will the device's data map into?
d) What basic application services are necessary?

10.3.3 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.

10.3.4 T101 Information (data) elements

Valid information elements are defined in IEC 60870-5-101 (1995) (T101) 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).

10.3.5 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 T101. The device vendor shall select those that are appropriate for his application. All of these basic application services are described fully in IEC 60870-5-5 (1995).

10.3.6 Network topologies

The topologies are defined in IEC 60870-5-1 (1990) 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 multipoint-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 T101 profile to use the application layer with typical LAN physical and data link layers. The lower two layers shall be IEC 60870-5 -compliant. This means that T101 does not permit use with standard LAN protocols, such as Ethernet, Token Ring, Token Bus, or FDDI. Therefore, T101 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.

10.4 T101 implementation example

As an example of T101 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 T101, thereby bypassing an RTU.

This example follows the T101 profile document step-by-step to select options for our controller implementation. Using a bottom-up approach yields the appropriate data link layer.

10.4.1 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.

10.4.2 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. At the application layer interface, we need to determine what information elements our application data will map into and which services our device will support.

Table 12 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) and T101.

Table 12— IEC 60870-5-101 information elements

Device element	T101 information element (definition) *
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)

* “Definition” is the section of T101 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) and 60870-5-3 (1992) 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 shall incorporate the new ASDU(s) into the master system or RTU if taking advantage of the new information available is desired.

10.5 IEC 60870-5-T101 Example vendor device implementation

A master station to RTU type implementation that illustrates the IEC 60870-5-101 (1995) profile is given in Table 13, which consists of a function and parameter definition table. This tabular example was provided by the implementor. In the table, all parameters are listed according to a specific topic, and the specific settings chosen by the implementor within the profile are listed. A separate configuration system was furnished to allow parameter settings to be input or changed to suit applications.

Table 13— Implementation of IEC 60870-5-101—parameter overview

Topic	Parameter	Settings
Bit transmission	Channel assignment Transmission rate for the command and monitoring directions together Set RTS signal Send delay after RTS signal Use of the clear to send (CTS) signal Number of idle characters in monitoring direction Number of idle characters in command direction Number of receive buffers Maximum telegram length (including header and trailer) in command direction	Depending on the device configuration 100, 200, 300, 600, 1200, 2400, 4800, 9600, 19 200, or 38 400 b/s Before transmitting or continuously None or 1–65 535 ms Do not use, or use as CTS, or data carrier detect (DCD) 1–3 1–3 3–20 10–261 characters
Link layer		
Balanced mode	DIR bit in send direction Link address Use of individual character E5 hex Response to receiving NACK Time-out for acknowledgments from the other station Number of transmission attempts on time-out Channel time-out Pause between status scans Dual channel transmission Time window for dual channel redundancy Processing of two different telegrams within the time window Assignment of the second channel	0 or 1 No link address, 1 octet 0–254, or 2 octets unstructured 0–65 534 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 Repeat or reject telegram to be sent 50–10 000 ms 2–225 No time-out or 1–255 s 0–65 535 ms Yes or no 100–65 535 ms Reject or transfer Channel number
Unbalanced mode	Distinction between class 1 and class 2 in the request telegram Link address Use of single character E5 hex Cycle time-out	Yes or no 1 octet, 0–254, or 2 octets unstructured, 0–65 534 Not as positive acknowledgment instead of a short telelgram with C = 00 hex or as negative acknowledgment instead of a short telegram with C = 09 hex No monitoring, or 1–255 s
General	Transmission in nonspontaneous mode and information status “not topical” Transmission in nonspontaneous mode and information status “blocked” End of command telegram (termination) Originator Common ASDU address Information object address Test command cycle time	Transmit or do not transmit Transmit or do not transmit With or without terminator No originator, or 0–255 1 octet, 0–254; 2 octets unstructured, 0–65 534, or 2 octets structured, 0–255 each 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 No test command, or 1–65 535 s

Topic	Parameter	Settings
Resource management	Number of commands that can be managed simultaneously Maximum number of parallel halt times Maximum number of monitored intermediate positions Maximum number of fault locations held	1–32 0–64 0–32 0–16
Image presetting	Single indication Double indication Analog value (standardized) Analog value (conditioned value IEEE floating point Transformer tap position Metered value Sequence number for metered value Bit pattern Protection data	0 or 1 00, 01, 10, or 11 binary –32 767 to 32 767 Per IEEE Std 754-1985 0–255 0–2 147 483 647 0–2 147 483 647 0–7FFFFFFF hex 0 or 1
Command direction One or two bit command with switching direction from telegram	Identifiers for private area in IEC qualifier of command Command output duration for each identifier Address of the information object Switching direction Command output durations: No additional definition Short pulse duration Long pulse duration Assignment of the command destination	Identifiers 16–32 inactive or active 0.01–655.35 s, step 0.01 s (See under general) Takeover or invert 0.01–655.35 s, step 0.01 s 0.01–655.35 s, step 0.01 s 0.01–655.35 s, step 0.01 s 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 Type of setpoint Assignment of the setpoint destination	(See under general) Analog setpoint in relative value format (unconditioned value), analog setpoint in floating point format (conditional value) or digital setpoint as bit pattern with 32 b Name of the setpoint output
Monitoring direction	Types of information objects	Single indication Double indication Normalized analog value, (unconditioned value, + 15 b) 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

Topic	Parameter	Settings
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 min
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 indictation (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 0.1–25.5 s, step 0.1 s
Double indication (additional settings)	Intermediate position suppression time	No intermediate position suppression or 1–255 s
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 1–32 767 Per IEEE Std C37.1-1994
Floating point analog value (additional settings)	Scaling factor Reference value for threshold formation (absolute)	Per IEEE Std 100-1996 Per IEEE Std 100-1996
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

11. 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 registration working group to obtain the latest information before creating duplicate implementations which may not be interoperable.

11.1 Creation

The tabular formats utilized in this document are adequate for definition 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 which 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 which provides all parameters noted in the protocol standards documents. The additional definitions shall also be provided to the registration body for this recommended practice in order that they may be given to other implementors.

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

11.2 Registration

The IEEE Substation Committee has a standing Working Group 3 (WG 3) within the Data Acquisition, Processing and Control Systems (C0) Subcommittee, which is responsible for standards applying to electric network control systems. This trial-use recommended practice designates that WG 3 shall act as a registration agent for additions to the list of objects, messages, and other implementations of this recommended practice. Such additions or changes will be available as information from the WG 3 during the trial-use period of two years.

A further level of official registration has been established for specific MMS objects which are being created in various projects both inside and outside the IEEE. ISO provides formal requirements for object registration as part of the Open Systems Interconnection process. Within IEEE, all societies shall coordinate with one designated local IEEE registration authority. Within the IEEE Power Engineering Society Communications Committee, a WG has been established to register objects, acting as the IEEE authority, with ability to coordinate registration activities directly with ISO on behalf of the IEEE.

11.3 Role of the DNP Users’ Group

DNP 3.0 has an independent User’s Group that administers DNP 3.0. A function of this User’s Group is to voluntarily register DNP 3.0 implementations by IED vendors, and to serve as an unbiased mediator to develop DNP 3.0 implementations for various classes of devices (i.e., meter, regulator, relay, et al.). IED vendors, prior to beginning any DNP 3.0 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, RTU vendors, and IED vendors, who represent an experience base and market expertise which may allow a DNP 3.0 development to be available to the largest body of potential users.

Annex A Comparison of DNP and IEC 60870-5-101

(Informative)

This annex provides reference tables which compare DNP and IEC 60870-5-101 with current draft protocols being developed in projects known as EPRI RP-3599 and EPRI MRP 1.0. 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

ISO/OSI model layer	Layer name definition	DNP 3.0 reference P1379 implementation	IEC 60870-5-101 reference - P1379 implementation	RP-3599 implementation	MRP implementation
1	Physical layer	RS-232, RS-485	Unbalanced V.24/ V.28, balanced X.24/X.27	EIA-232-D, ISO 8802/3, / 4, /5 ISO 9314	2/4 wire serial, EIA RS-485, MAS or spread-spectrum radio fiber optics, CATV carrier
2	Data link layer	IEC 60870-5 FT3	IEC 60870-5 FT1.2	CSMA/CD+LLC 1 or 3, where 8802/3 is used. Token bus + LLC 1 OR 3, where 8802/4 is used. FDDI+LLC 1, where ISO 9314 is used.	ADLC (asynchronous HDLC), with additions for message segmentation and time sync
4	Transport layer	DNP-specific pseudo-transport layer for long message segmentation	Not implemented	Not implemented IEC EPA 3-layer stack	Not implemented
7	Application layer	Application protocol data unit (APDU) for master to non-master operation	APDUs as defined in IEC 60870-5-101 from IEC 60870-5-4	RP-3599 objects and functions using a subset OF MMS services called SubMMS	MRP objects and functions using MMS services
Not defined	User layer	Device, unit, or system-specific data representation	Device, unit, or system-specific data representation	RP-3599 protection-specific implemented data: global, vendor unique, or application unique	SCADA-specific system commands and data

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. The RP-3599 and MRP are MMS implementations, and use more generic functions than DNP 3.0 or IEC 60870-5-101.

Table A.2 —Message/function types

Function or message	**DNP 3.0 Reference P1379 implementation**			**IEC 60870-5-101 reference P1379 implementation**		**RP-3599 reference utility message specification (draft)**		**MRP reference**	
	Func. code	Description	Recommended	<Type ID> or (Tx Cause)	Description	RP-3599 MMS service method	RP-3599 method description	MRP	MRP
0.00					Send	Set attribute			
0.00	0	Confirm	Yes	(P/N=0)	Positive confirm				
				(P/N=1)	Negative confirm				
Read	1	Read	Yes	(1)	Periodic, cyclic				
				<100>	Interrogation command				
				<101>	Counter interrogation cmd				
				<102>	Read command	Read getdatavalue	Retrieve data value(s)	Read data-pointname	Retrieve data having one structure or value
				(5–6)	Request	Get name list get data value names	Retrieve data value names		
				(20)	General interrogation				
				(21–36)	Group interrogation			Read datasetvalues	Retrieve a defined set of data from server.
				(38–41)	Group counter request				
						Readtime	Access the current time		
						Getvariable access atributes Getdatavalue type	Retrieve data value type		
Write	2	Write	Yes			Write Setdatavalue	Modify data values		

Function or message	DNP 3.0 Reference P1379 implementation			IEC 60870-5-101 reference P1379 implementation		RP-3599 reference utility message specification (draft)		MRP reference	
				<120–126> (13)	File transfer				
				<110 -113>	Parameter of measured value				
				<103>	Clock synch command	Write			
Timesync	Send time sync object								
Select	3	Select	Yes	<45–51> (6, 8)	Single/ double command setpoint commands regulating step cmd activation deactivation	Read select	Request access to a server device		
Operate	4	Operate	Yes			Write operate	Request operation of a device		
	5	Direct operate	Yes						
	6	Direct operate NO ACK	Yes						
	7	Immediate freeze	Yes	<113>	Parameter activation				
(parameter = Time Period for Periodic Memoriz-ation of Integrated Totals)									
	8	Immediate freeze - NO ACK	Yes						
	9	Freeze and clear	Yes						

Function or message	**DNP 3.0 Reference P1379 implementation**			**IEC 60870-5-101 reference P1379 implementation**		**RP-3599 reference utility message specification (draft)**		**MRP reference**	
	10	Freeze and clear - NO ACK	Yes						
	11	Freeze with time	No						
	12	Freeze with time-NO ACK	No						
	13	Cold restart	Yes	(4) <70>	Initialized end of initialization				
	14	Warm restart	No						
	15	Init data to default	No						
	16	Initialize application	No						
Run program	17	Start application	No	<105>	Reset process command	Start	Change program from idle to running		
Stop program	18	Stop application	No			Stop	Change program from running to stopped		
	19	Save configuration	No	<120–126> (13)	File transfer				
				<113>	Parameter activation				
Start RBE	20	Enable unsolicited	No			Write starttransfer	Set transfer parameters and cause server to begin monitoring	Write to transferset	Causes data set selections to be monitored for report by exception
Stop RBE	21	Disable unsolicited	No			Write stoptransfer	Inform server to stop monitoring for reporting		
Set priority	22	Assign to class	No	(20–41)	Group interrogations	Write			

Function or message	**DNP 3.0 Reference P1379 implementation**			**IEC 60870-5-101 reference P1379 implementation**		**RP-3599 reference utility message specification (draft)**		**MRP reference**	
Create-dataset	Create a new data set								
	23	Delay measurement	Yes	<103>	Clock synch command				
Response with data	129	Response	Yes	(11)	Return info-local cmd				
				(12)	Return info - remote cmd				
				<7>	Activation confirmation	Event notification	Server informs client of an event condition becoming true		
				<7>	Deactivation confirmation				
				<10>	Activation termination	Delete event			
Enrollment	Delete an event enrollment for client at server								
				<1–21>	Process info-monitor direction				
RBE	130	Unsolicited response	Yes	(1)	Periodic, cyclic	Transfer report	Server reports data set values when monitored conditions occur		
				(3)	Spontaneous				
				<104>	Test command				
				<106>	Delay acquisition command				

A.3 Data objects—primitive

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

Table A.3 —Data objects—primitive

eter equal ric data ment	DNP 3.0 reference designation P1379 implementation		IEC 60870-5-101 reference designation—P1379 implementation		RP-3599 reference designation		MRP reference design	
	Notation	Typical use in an object			Notation		Notation	Typic in an
tion	BSn[pos]	n = number of bits pos = bit position in word					Bitstring	Bitstr {size
	BS1	Binary input, control relay output block, binary output status				Bitstring 1	Singleswitchstatus- simplestate	
g	BSn	Binary input (packed)						
nask (not L2)				BITSTRING {size}	various			
3 b d	UI	To be defined				Integer 8 U	Switchstatusscan group - scan grouplength	
16 b d	UI16	16 b binary counter						
zen counter				Integer 16 U	Accumulator - accumulatorvalue			
16 b signed	I16	16 b analog input						
log output				Integer 16 S	Rawanalog - analogvalues			
32 b d	UI32	32 b binary counter						
zen counter				Integer 32 U	Transferset - start time			
point —32 b	R32							
	Short floating point (not in DNP-L2)				Float 32 (IEEE)	Processed Analog-PointValueFloata		
g point —64 b	R64							
	Long floating point (not in DNP-L2)				Float 64 (IEEE)	None defined boolean value	BS1	Binar contr outpu
f rs						Visible string (ASCII text)	Any object - datapointname octet string	

A.4 Data elements with utility-specific definitions

Many forms of IED and RTU data need to be represented by known objects which 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 four relevant protocols.

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

Utility-specific data element	DNP 3.0 reference P1379 implementation	IEC 60870-5-101 reference P1379 implementation	RP-3599 reference	MRP implementation
Analog input				
Sensor value	16/32 b Analog input	Measured value		RawAnalogQuality
Transducer value	16/32 b Analog input	Measured value		RawAnalogQuality
Amps (Kamps)	16/32 b Analog input	Measured value		RawAnalogQuality
Volts (Kvolts)	16/32 b Analog input	Measured value		RawAnalogQuality
Power factor	16/32 b Analog input	Measured value		RawAnalogQuality
Watt (kwatt)	16/32 b Analog input	Measured value		RawAnalogQuality
VA (kVA)	16/32 b Analog input	Measured value		RawAnalogQuality
VAR (kVAR)	16/32 b Analog input	Measured value		RawAnalogQuality
Frequency - Hz	16/32 b Analog input	Measured value		RawAnalogQuality
Phasors referenced to ?	16/32 b Analog input	Measured value		RawAnalogQuality
Ambient conditions				
Temperature (units ?)	16/32 b Analog input	Measured value		RawAnalogQuality
Humidity (%)	16/32 b analog input	Measured value		RawAnalogQuality
Wind (knots)	16/32 b analog input	Measured value		RawAnalogQuality
Operating conditions				
Impedance (ohms)	16/32 b analog input	Measured value		RawAnalogQuality
Ground fault (current) (status)	16/32 b analog input binary input	Measured value single-point info		RawAnalogQuality SwitchStatusValScanGroup
Transformer temp (units?)	16/32 b analog input	Measured value		RawAnalogQuality
Xformer fans on/off	Binary input	Single/double point info		SwitchStatusValScanGroup

Utility-specific data element	DNP 3.0 reference P1379 implementation	IEC 60870-5-101 reference P1379 implementation	RP-3599 reference	MRP implementation
Xfmr oil pumps on/off	Binary input	Single/double point info		SwichStatusValScanGroup
Communications SNR (dB SINAD)	16/32 b analog input	Measured value		RawAnalogQuality
Status/counters				
Breaker open/close	Binary input 16/32 b binary counter	Single/double point info		SwitchStatusValScanGroup
Reclosing on/off	Binary input 16/32 b binary counter	Single/double point info integrated totals		SwitchStatusValScanGroup Accumulator
Fast trip relay in/out	Binary input 16/32 b binary counter	Single/double point info integrated totals		SwitchStatusValScanGroup, Accumulator
Operations counter	16/32 b binary counter	Integrated totals		Accumulator
Tap position	16/32 b analog input	Step position info		RawAnalogQuality
Controls				
Command	Control relay output block	Single command, double command, regulating step command		SelectBinaryDevice OperateBinaryDevice SupervisoryCommand
Limit settings	16 b analog output 32 b analog output *	Parameter activation		SelectSetpointDevice OperateSetpointDevice SetpointCommand
Trigger settings	16 b analog output 32 b analog output *	Parameter activation		SelectSetpointDevice OperateSetpointDevice SetpointCommand
Operating set points	16 b analog output 32 b analog output *	Setpoint command		SelectSetpointDevice OperateSetpointDevice SetpointCommand
Regulation setting	16 b analog output 32 b analog output *	Setpoint command		SelectSetpointDevice OperateSetpointDevice SetpointCommand
Alarms				

Utility-specific data element	DNP 3.0 reference P1379 implementation	IEC 60870-5-101 reference P1379 implementation	RP-3599 reference	MRP implementation
Faults (status and point identification only)	Binary input change	Event of protection equipment Single/double point info		SwitchStatusValScanGroup, TransferSet
Device operation (identity only)	Binary input change	Event of protection equipment Single/double point info		SwitchStatusValScanGroup, TransferSet
Station lockout	Binary input change	Event of protection equipment Single/double point info		SwitchStatusValScanGroup, TransferSet
Feeder lockout	Binary input change	Event of protection equipment Single/double point info		SwitchStatusValScanGroup, TransferSet
Sequence of events (one per event)	Binary input change with time	Event of protection equipment Single/double point info		SOEStatusGroup TransferSet
Fault event record (file transfer)	File identifier * private registration object*	File transfer?		MMS domains?
Time				
Time sync command	Time and date	Clock synch command		Performed in data link
Time stamp of event (day, hh:mm:ss.msec)	Binary input change with time, 16/32 b analog input change with time *, 16/32 b counter change event with time *, 16/32 b 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 Measured value with time tag Integrated totals with time tag Output circuit info with time tag		SOEStatusGroup TransferSet
Duration of event (hh:mm:ss. msec)	16/32 b analog input time Delay coarse Time delay fine	Measured value?		n/a
Device programming				

Utility-specific data element	DNP 3.0 reference P1379 implementation	IEC 60870-5-101 reference P1379 implementation	RP-3599 reference	MRP implementation
Configuration (file transfer download)	File identifier *	Parameter activation		MMS domains?
Database (read or write data)	File identifier? *	File transfer?		MMS domains?
Settings	Control relay output block 16 b analog output 32 b analog output *	Parameter activation		Transfer set?
History log	File identifier *	File transfer?		MMS domains?
Fault records				
Event ID	Possibly file identifier * Currently under consideration by DNP User's Group	File transfer?		MMS domains?
Location/unit ID				
Event profile				
Event detail data				
Target information				

*Not defined in the DNP-L2 subset specified in these recommended practices. Listed here to show the capabilities of the protocol.

Annex B Bibliography

(Informative)

[B1] EPRI Project RP-3599 (Substation Integrated Protection, Control, and Data Acquisition) Documentation: Utility Message Specification, Preliminary Implementation Agreement, Document RP-3599-01, Pre-Release Version 14 September 1995.[6]

[B2] EPRI MRP Protocol Documentation.[7]

[B3] IEEE Std C37.1-1994, IEEE Standard Definition, Specification, and Analysis of Systems Used for Supervisory Control, Data Acquisition, and Automatic Control.

[B4] IEEE Std 999-1992, IEEE Recommended Practice for Master/Remote Supervisory Control and Data Aquisition (SCADA) Communication.

[B5] ITU-T Recommendation V.24 (1996), List of definitions for interchange circuits between data terminal equipment (DTE) and data circuit-terminating equipment (DCE).[8]

[B6] ITU-T Recommendation V.28 (1993), Electrical characteristics for unbalanced double-current interchange circuits.

[B7] ITU-T Recommendation X.24 (1996), List of definitions for interchange circuites between data terminal equipment (DTE) and data circuit-terminating equipment (DCE) on public data networks.

[B8] ITU-T Recommendation X.27 (1988), Electrical characteristics for balanced double-current interchange circuits operating at data signaling rates up to 10 Mbit/s.

[6]For information about EPRI projects and publications, contact the Power Systems Planning and Operations Program of the Power Delivery Group, Electric Power Research Institute, 3412 Hillview Avenue, Palo Alto, CA 94304.
[7]This EPRI document is in development; contact EPRI for information.
[8]ITU-T publications are available from the International Telecommunications Union, Place des Nations, CH-1211, Geneva 20, Switzerland.

