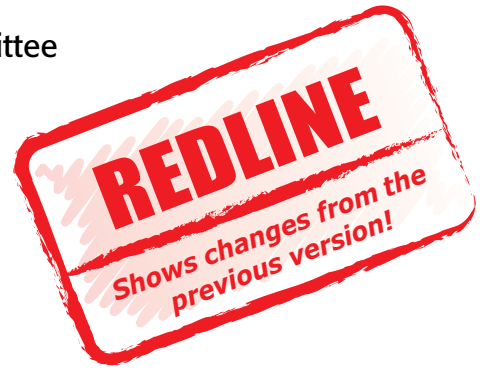
IEEE STANDARDS ASSOCIATION IEEE

IEEE Standard for Electric Power Systems Communications—Distributed Network Protocol (DNP3)

IEEE Power and Energy Society

Sponsored by the
Transmission and Distribution Committee
and
Substations Committee



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

10 October 2012

IEEE Std 1815™-2012
(Revision of
IEEE Std 1815-2010)

Documents
Document Sharing Hub

Authorized licensed use limited to: Tsinghua University. Downloaded on February 25,2026 at 01:06:46 UTC from IEEE Xplore. Restrictions apply.

Full document details: IEEE 1815-2012

Documents
Document Sharing Hub
Authorized licensed use limited to: Tsinghua University. Downloaded on February 25,2026 at 01:06:46 UTC from IEEE Xplore. Restrictions apply.
Full document details: IEEE 1815-2012

This is a Redline Document produced by Techstreet, a business of Thomson Reuters.

This document is intended to provide users with an indication of changes from one edition to the next. It includes a full-text version of the new document, plus an indication of changes from the previous version.

Redlines are designed to save time and improve efficiencies by using the latest software technology to find and highlight document changes. More professionals are using valuable new technologies like redlines, to help improve outcomes in a fastpaced global business world.

Because it may not be technically possible to capture all changes accurately, it is recommended that users consult previous editions as appropriate. In all cases, only the current base version of this publication is to be considered the official document.

Documents Document Sharing Hub

Authorized licensed use limited to: Tsinghua University. Downloaded on February 25,2026 at 01:06:46 UTC from IEEE Xplore. Restrictions apply.

Full document details: IEEE 1815-2012

Redline Processing Notes:

1. ~~**Red Text**~~ - Red strikethrough text denotes deletions.

2. **Blue Text** - Blue underlined text denotes modifications and additions.

Documents
Document Sharing Hub

Authorized licensed use limited to: Tsinghua University. Downloaded on February 25,2026 at 01:06:46 UTC from IEEE Xplore. Restrictions apply.

Full document details: IEEE 1815-2012

IEEE Std 1815™-2012
(Revision of
IEEE Std 1815-2010)

IEEE Standard for Electric Power Systems Communications—Distributed Network Protocol (DNP3)

Sponsor

Transmission and Distribution Committee

and

Substations Committee

of the

IEEE Power and Energy Society

Approved 8 June 2012
IEEE-SA Standards Board

Documents
Document Sharing Hub

Authorized licensed use limited to: Tsinghua University. Downloaded on February 25,2026 at 01:06:46 UTC from IEEE Xplore. Restrictions apply.

Full document details: IEEE 1815-2012

The Working Group thanks the International Electrotechnical Commission (IEC) for permission to reproduce information from the International Standards IEC/TS 62351-3 ed. 1.0 (2007), IEC/TS 62351-5 ed. 1.0 (2009), and IEC/TS 62351-8 ed. 1.0 (2011).

All such extracts are copyright of IEC, Geneva, Switzerland. All rights reserved. Further information on the IEC is available from www.iec.ch. IEC has no responsibility for the placement and context in which the extracts and contents are reproduced by the author, nor is IEC in any way responsible for the other content or accuracy therein.

Abstract: The DNP3 protocol structure, functions, and interoperable application options (subset levels) are specified. The simplest application level is intended for low-cost distribution feeder devices, and the most complex for full-featured systems. The appropriate level is selected to suit the functionality required in each device. The protocol is suitable for operation on a variety of communication media consistent with the makeup of most electric power communication systems.

Keywords: Distributed Network Protocol (DNP3), distribution automation, distribution feeder, electric power communication systems, IEEE 1815, master station, substation automation

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

Copyright © 2012 by The Institute of Electrical and Electronics Engineers, Inc.
All rights reserved. Published 10 October 2012. Printed in the United States of America.

IEEE is a registered trademark in the U.S. Patent & Trademark Office, owned by The Institute of Electrical and Electronics Engineers, Incorporated.

PDF: ISBN 978-0-7381-7292-7 STD97267
Print: ISBN 978-0-7381-7344-3 STDPD97267

IEEE prohibits discrimination, harassment and bullying. For more information, visit http://www.ieee.org/web/aboutus/whatis/policies/p9-26.html.
No part of this publication may be reproduced in any form, in an electronic retrieval system or otherwise, without the prior written permission of the publisher.

Documents
Document Sharing Hub

Authorized licensed use limited to: Tsinghua University. Downloaded on February 25,2026 at 01:06:46 UTC from IEEE Xplore. Restrictions apply.

Full document details: IEEE 1815-2012

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

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

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

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

In publishing and making its standards available, IEEE is not suggesting or rendering professional or other services for, or on behalf of, any person or entity. Nor is IEEE undertaking to perform any duty owed by any other person or entity to another. Any person utilizing any IEEE Standards document, should rely upon his or her own independent judgment in the exercise of reasonable care in any given circumstances or, as appropriate, seek the advice of a competent professional in determining the appropriateness of a given IEEE standard.

Translations: The IEEE consensus development process involves the review of documents in English only. In the event that an IEEE standard is translated, only the English version published by IEEE should be considered the approved IEEE standard.

Official Statements: A statement, written or oral, that is not processed in accordance with the IEEE-SA Standards Board Operations Manual shall not be considered the official position of IEEE or any of its committees and shall not be considered to be, nor be relied upon as, a formal position of IEEE. At lectures, symposia, seminars, or educational courses, an individual presenting information on IEEE standards shall make it clear that his or her views should be considered the personal views of that individual rather than the formal position of IEEE.

Comments on Standards: Comments for revision of IEEE Standards documents are welcome from any interested party, regardless of membership affiliation with IEEE. However, IEEE does not provide consulting information or advice pertaining to IEEE Standards documents. Suggestions for changes in documents should be in the form of a proposed change of text, together with appropriate supporting comments. Since IEEE standards represent a consensus of concerned interests, it is important to ensure that any responses to comments and questions also receive the concurrence of a balance of interests. For this reason, IEEE and the members of its societies and Standards Coordinating Committees are not able to provide an instant response to comments or questions except in those cases where the matter has previously been addressed. Any person who would like to participate in evaluating comments or revisions to an IEEE standard is welcome to join the relevant IEEE working group at http://standards.ieee.org/develop/wg/.

Comments on standards should be submitted to the following address:

Secretary, IEEE-SA Standards Board
445 Hoes Lane
Piscataway, NJ 08854-4141
USA

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

Documents
Document Sharing Hub
Authorized licensed use limited to: Tsinghua University. Downloaded on February 25,2026 at 01:06:46 UTC from IEEE Xplore. Restrictions apply.
Full document details: IEEE 1815-2012

Notice to users

Laws and regulations

Users of IEEE Standards documents should consult all applicable laws and regulations. Compliance with the provisions of any IEEE Standards document does not imply compliance to any applicable regulatory requirements. Implementers of the standard are responsible for observing or referring to the applicable regulatory requirements. IEEE does not, by the publication of its standards, intend to urge action that is not in compliance with applicable laws, and these documents may not be construed as doing so.

Copyrights

This document is copyrighted by the IEEE. It is made available for a wide variety of both public and private uses. These include both use, by reference, in laws and regulations, and use in private self-regulation, standardization, and the promotion of engineering practices and methods. By making this document available for use and adoption by public authorities and private users, the IEEE does not waive any rights in copyright to this document.

Updating of IEEE documents

Users of IEEE Standards documents should be aware that these documents may be superseded at any time by the issuance of new editions or may be amended from time to time through the issuance of amendments, corrigenda, or errata. An official IEEE document at any point in time consists of the current edition of the document together with any amendments, corrigenda, or errata then in effect. In order to determine whether a given document is the current edition and whether it has been amended through the issuance of amendments, corrigenda, or errata, visit the IEEE-SA Website at http://standards.ieee.org/index.html or contact the IEEE at the address listed previously. For more information about the IEEE Standards Association or the IEEE standards development process, visit IEEE-SA Website at http://standards.ieee.org/index.html.

Errata

Errata, if any, for this and all other standards can be accessed at the following URL: http://standards.ieee.org/findstds/errata/index.html. Users are encouraged to check this URL for errata periodically.

Copyright © 2012 IEEE. All rights reserved.

Documents
Document Sharing Hub

Authorized licensed use limited to: Tsinghua University. Downloaded on February 25,2026 at 01:06:46 UTC from IEEE Xplore. Restrictions apply.

Full document details: IEEE 1815-2012

Patents

Attention is called to the possibility that implementation of this standard may require use of subject matter covered by patent rights. By publication of this standard, no position is taken by the IEEE with respect to the existence or validity of any patent rights in connection therewith. If a patent holder or patent applicant has filed a statement of assurance via an Accepted Letter of Assurance, then the statement is listed on the IEEE-SA Website at http://standards.ieee.org/about/sasb/patcom/patents.html. Letters of Assurance may indicate whether the Submitter is willing or unwilling to grant licenses under patent rights without compensation or under reasonable rates, with reasonable terms and conditions that are demonstrably free of any unfair discrimination to applicants desiring to obtain such licenses.

Essential Patent Claims may exist for which a Letter of Assurance has not been received. The IEEE is not responsible for identifying Essential Patent Claims for which a license may be required, for conducting inquiries into the legal validity or scope of Patents Claims, or determining whether any licensing terms or conditions provided in connection with submission of a Letter of Assurance, if any, or in any licensing agreements are reasonable or non-discriminatory. Users of this standard are expressly advised that determination of the validity of any patent rights, and the risk of infringement of such rights, is entirely their own responsibility. Further information may be obtained from the IEEE Standards Association.

Copyright © 2012 IEEE. All rights reserved.

Documents
Document Sharing Hub

Authorized licensed use limited to: Tsinghua University. Downloaded on February 25,2026 at 01:06:46 UTC from IEEE Xplore. Restrictions apply.

Full document details: IEEE 1815-2012

Participants

At the time this standard was submitted to the IEEE-SA Standards Board for approval, the Standard for Electric Power Systems Communications—Distributed Network Protocol (DNP3) Working Group had the following membership:

H. Lee Smith, *Co-Chair*
Ron Farquharson, *Co-Chair*
Andrew West, *Vice Chair*

Bill Ackerman
Demos Andreou
Philip Aubin
Jim Baker
James Bougie
Jake Brodsky
Carlos Bustamante
Ed Cenzon
Mason Clark
Lorene Cunningham
Mike Dood
Chris Francis
Charles Freedman
Dan Friedman
Grant Gilchrist
Randy Kimura
Marc Lacroix
Bob Landman
Parker McCauley
Steve McCoy
Bruce Muschlitz
Craig Preuss
James Recchia
Craig Rodine
Samuel Sciacca
Alan Scott
Barry Shephard
Michael S. Smith
John T. Tengdin
Eric Thibodeau
Tim Tibbals
Jay Vellore
Jack Verson
David Wood

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

Bill Ackerman
Satish Aggarwal
Ali Al Awazi
Saleman Alibhay
Ficheux Arnaud
Jim Baker
Wallace Binder
Paul Bishop
Chris Brooks
William Byrd
Paul Cardinal
Edgar Cenzon
Jerry Corkran
Lorene Cunningham
Ray Davis
Muhammad Dhodhi
Mike Dood
Randall Dotson
Gary Engmann
Ron Farquharson
Dan Friedman
Grant Gilchrist
Mietek Glinkowski
Roman Graf
Stephen Grier
Randall Groves
Timothy Hayden
Gary Heuston
Gary Hoffman
Yi Hu
Noriyuki Ikeuchi
Piotr Karocki
Yuri Khersonsky
James Kinney
Stanley Klein
Joseph L. Koepfinger
Jim Kulchisky
Marc Lacroix
Chung-Yiu Lam
G. Luri
Ahmad Mahinfallah
Wayne Manges
Pierre Martin
Jeffery Masters
John McDonald
Gary McNaughton
Willam Moncrief
Jose Morales
Charles Morgan
Adi Mulawarman
R. Muprhy
Bruce Muschlitz
Pratap Mysore
Arthur Neubauer
Michael S. Newman
Charles Ngethe
Gary Nissen
Lorraine Padden
Mirko Palazzo
Donald Parker
Bansi Patel
Craig Preuss
John Randolph
Michael Roberts
Charles Rogers
Bob Saint
Steven Sano
Bartien Sayogo
Samuel Sciacca
Gil Shultz
Mark Simon
Jerry Smith
Joshua Smith
Aaron Snyder
John Spare
Wayne Stec
Gary Stoedter
Walter Struppler
Charles Sufana
William Taylor
David Tepen
Eric Thibodeau
Eric Udren
John Vergis
Jane Verner
Daniel Ward
Andrew West
Janusz Zalewski
Matthew Zeedyk

Copyright © 2012 IEEE. All rights reserved.
Documents
Document Sharing Hub
Authorized licensed use limited to: Tsinghua University. Downloaded on February 25,2026 at 01:06:46 UTC from IEEE Xplore. Restrictions apply.
Full document details: IEEE 1815-2012

When the IEEE-SA Standards Board approved this standard on 8 June 2012, it had the following membership:

Richard H. Hulett, *Chair*
John Kulick, *Vice Chair*
Robert Grow, *Past Chair*

Satish Aggarwal	Alexander Gelman	Oleg Logvinov
Masayuki Ariyoshi	Paul Houzé	Ted Olsen
Peter Balma	Jim Hughes	Gary Robinson
William Bartley	Young Kyun Kim	Jon Walter Rosdahl
Ted Burse	Joseph L. Koepfinger*	Mike Seavey
Clint Chaplin	David J. Law	Yatin Trivedi
Wael Diab	Thomas Lee	Phil Winston
Jean-Philippe Faure	Hung Ling	Yu Yuan

*Member Emeritus

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

Richard DeBlasio, *DOE Representative*
Michael Janezic, *NIST Representative*

Don Messina
IEEE Standards Program Manager, Document Development

Matthew J. Ceglia
IEEE Standards Client Services Manager, Professional Services

Copyright © 2012 IEEE. All rights reserved.

Documents
Document Sharing Hub

Authorized licensed use limited to: Tsinghua University. Downloaded on February 25,2026 at 01:06:46 UTC from IEEE Xplore. Restrictions apply.

Full document details: IEEE 1815-2012

0 Introduction

This introduction is not part of IEEE Std 1815-2012, IEEE Standard for Electric Power Systems Communications—Distributed Network Protocol (DNP3).

0.1 DNP3 purpose and history

This Introduction discusses the creation and history of DNP3. The structure and operation of the protocol may be easier to understand when taken in the context of the problems the designers of DNP3 intended to solve.

0.1.1 Addressing an impediment to automation

Westronic Incorporated developed DNP3 between 1992 and 1994, intending it to be the first truly open, truly useful protocol standard in the utility industry. Westronic was a manufacturer of remote terminal units and a system integrator based in Calgary, Canada. It had made a reputation converting between the hundreds of proprietary utility protocols in use at the time. This was not an easy task, however, and Westronic management had become frustrated with trying to make its devices compatible with so many proprietary protocols.

A proposal was made that Westronic should develop its own protocol but then release it to the industry. The new protocol would incorporate the best features of the many protocols Westronic had encountered, plus some new ideas. Westronic would place the specification under the control of an independent users' group. Both utilities and vendors would be invited to be members, including Westronic's competitors. Westronic would not receive any money for the sale and distribution of the specification.

0.1.2 Rationale for a new protocol based on standards

Westronic was not the first to propose an open standard for the utility industry, but the designers of DNP3 did not find any of the existing efforts suitable. At the time when Westronic was considering DNP3, there were two main candidates available for an open protocol:

— The Electrical Power Research Institute (EPRI) had recently released the Utility Communications Architecture (UCA) version 1.0. However, version 1.0 listed a choice of protocol profiles only and did not define any object models or services suitable for performing Supervisory Control and Data Acquisition (SCADA) functions. At that point in the development of UCA, very few utilities or vendors had provided input to the specification, and there were some serious concerns about bandwidth usage. These drawbacks and others eventually led to the development of UCA 2.0. UCA 2.0 became an IEEE technical report in 1998 and eventually evolved into IEC 61850.[a]

— The International Electrotechnical Commission (IEC) had developed the first few documents in the IEC 60870-5 series of specifications, including the specifics of the Data Link Layer and general definitions for the Application Layer. (At that time, it was called just 870-5.) Westronic had been participating in this effort but felt that it was progressing too slowly. Furthermore, the IEC had provided many options in the specification, and Westronic was worried the standard would not be restrictive enough to promote interoperability. The IEC eventually released the 60870-5-101-companion standard in 1995 to address these issues.

In 1992, the IEC work seemed to be the more complete of the two efforts and had wider industry support at the time. Westronic therefore decided to base DNP3 on the IEC work already completed. Even now, the

[a] Information on references can be found in Clause 2.

Copyright © 2012 IEEE. All rights reserved.
Documents
Document Sharing Hub
Authorized licensed use limited to: Tsinghua University. Downloaded on February 25,2026 at 01:06:46 UTC from IEEE Xplore. Restrictions apply.
Full document details: IEEE 1815-2012

feature sets of IEC 60870-5-101:2003 [B3][b] and DNP3 are very similar because the design teams built them on the same basic research.

UCA was not forgotten. Westronic (by then called Harris Distributed Automation Products) circulated versions of the DNP3 Basic 4 Document Set including a paper called "On the Road to Utility Communications Architecture." The thesis of this paper was that by standardizing on DNP3, utilities would at least be reducing from many protocols to one. This would make it easy for utilities to later change to use UCA. However, very few design elements of UCA found their way into this standard, other than a generally layered architecture.

0.1.3 Need for scalability

The designers of DNP3 built it with several goals in mind, but the one that had the most impact on the final protocol was the industry's desire to limit the amount of bandwidth used. At that time, utilities considered a link running at 1200 bits per second to be fairly quick. (Yes, there are areas where this is still true). Local area networks (LANs) were for office computing only, and the thought of trusting one's SCADA network to a third-party telecom provider was heresy.

Power utilities had heard about layered protocols and the Open System Interconnection (OSI) model, but they were unconvinced of their value in a SCADA protocol. The Internet was beginning to boom, of course, but most utilities considered those protocols for business computing only. They were not for a SCADA network. Those who followed such things may also have heard that there was a backlash against the OSI model brewing. Protocols like Asynchronous Transfer Mode (ATM) and Frame Relay promised higher performance by eliminating layers. No utility at that time would have used these protocols in their network, but they probably heard that "layers are bad."

Therefore, the designers of DNP3 gave themselves a design goal to reduce bandwidth and use as few layers as possible.

This goal combined with the desire to be compliant with IEC 60870-5 resulted in the "Transport Function" as it now exists: a header that is not quite part of the Data Link Layer and yet not quite a complete Transport Layer. A later subclause will discuss the Transport Function in more detail.

0.1.4 Emphasis on reliability

While requesting less bandwidth, utilities refused to compromise on the requirement that a SCADA protocol be extremely reliable. Early bit-oriented protocols had acquired a bad reputation because a change of a single bit could result in a device operating the wrong switch. This led to utilities requiring in bid specifications that vendors build select-before-operate, "I tell you twice," functions into all protocols. A few bad experiences made utilities paranoid about reliability to the point of writing it into contracts.

Therefore, when designing a frame format to use, the DNP3 designers chose the most reliable format they could find. The IEC had done extensive modeling on reliability and had documented the results in IEC 60870-5-1:1990 [B3]. Rather than reinvent the wheel, the designers picked the most reliable of the several formats described in that specification, Frame Type 3 (FT3).

In the years that have passed, this decision has proven to be a good one. Many vendors have cursed the calculations necessary for the many cyclic redundancy checks (CRCs). Many system engineers have cursed the extra bandwidth overhead. However, DNP3's reputation for reliability started well and has only improved with the years.

[b] The numbers in brackets correspond to those of the bibliography in Annex G.

Copyright © 2012 IEEE. All rights reserved.
Documents
Document Sharing Hub
Authorized licensed use limited to: Tsinghua University. Downloaded on February 25,2026 at 01:06:46 UTC from IEEE Xplore. Restrictions apply.
Full document details: IEEE 1815-2012

0.1.5 Feature selection

Because the designers of DNP3 were from a systems integration company, they tried to incorporate into DNP3 the best features of all the utility protocols they had encountered. These features included:

- Broadcasting. The ability to send a single message to multiple devices.
- Select-before-operate—or not. The ability to choose to use extra reliability when operating an output, or to choose not to use it.
- Time-stamped data. Some of the most popular utility protocols, such as Modbus, had no way to accurately time-stamp data. Vendors and utilities were forced to develop proprietary work-around solutions. Other protocols supported time stamps on binary data only. DNP3 permits time stamps on almost all data. This feature has become increasingly more useful as utilities progressively gather other types of historical data beyond the standard binary "sequence of events" log.
- Accurate time synchronization. Many earlier protocols had no way to account for transmission and software delays when synchronizing. The method used in DNP3 is an amalgamation of several different protocols' solutions.
- Quality flags. Representing a maker of data concentrators, the designers provided a mechanism to see whether data was valid, and why. Some protocols, designed by intelligent electronic device (IED) vendors whose data was always online, did not include this feature.
- Multiple data formats. The ability to report data in a variety of formats: 16-bit, 32-bit, with a flag, without a flag, floating-point, binary-coded decimal (BCD), packed, unpacked, and so on.
- Scan groups. The ability to define and ask for a large set of otherwise unrelated data using a single request.
- Layer separation. Separating the function of "getting the data there" from the actual SCADA functions.
- Report-by-exception. More than any other feature, the ability to reliably report only the changes in data has helped make DNP3 successful.
- Internal indications. As several protocol efforts that are more recent than DNP3 have discovered, it is extremely useful to have a global set of flags returned in each response. These flags indicate the health of the device and the results of the last request.

Most of these features had been seen elsewhere, but this was the first time an open utility protocol had attempted to do them all.

0.1.6 Rationale for DNP3 subset definitions

Unfortunately, the "best practices" approach to developing DNP3 was not perfect, causing a number of features to be added that were not really in widespread use. A number of them existed only in Westronic equipment. At various times, vendors have questioned the need for:

- So many different types of counters, particularly delta counters
- So many different types of binary output operations, especially control queuing
- So many different ways to format data (i.e., many qualifier codes)
- Pattern masks
- Binary-coded decimal analogs
- Storage objects

Copyright © 2012 IEEE. All rights reserved.

Documents
Document Sharing Hub

Authorized licensed use limited to: Tsinghua University. Downloaded on February 25,2026 at 01:06:46 UTC from IEEE Xplore. Restrictions apply.

Full document details: IEEE 1815-2012

— The ability to either write or operate an output

— So many layers of confirmation and segmentation

0.1.7 Features to support distributed capabilities

Another trend in the early 1990s was the move to put larger processors and more memory in SCADA devices. Marketing and sales people were talking about "the intelligent network." By this, they meant pushing many of the functions previously performed only by master stations into remote devices. These devices would be more independent and make more decisions on their own. Those who join the utility industry these days are sometimes confused by the term "IED" meaning intelligent electronic device. They say, "Aren't all computing devices intelligent?" Yes, but it wasn't always this way.

In terms of DNP3 design, the idea of "the intelligent network" translated to the following features:

— Spontaneous reporting. A device could transmit whenever it wanted, not just when polled by the master. On multi-drop links, this led to the need for a collision avoidance mechanism.

— Meta-data. The DNP3 designers called a spontaneous message an "Unsolicited Response," which shows the mindset in those days. Most devices only sent data in response to a poll request. Therefore, the master always knew what data was coming. For a device to send an unsolicited response, it had to include not only the SCADA data itself but also information describing the data so the master knew what it was. The term these days for such information is meta-data. It appears in such modern technologies as Extensible Markup Language (XML). At that time, though, it was a very new concept for the utility industry.

— Wild-carding. Because the remote device was more intelligent, the designers gave it more choice in the amount and format of the data it reported. A master could ask very simple questions, like "Give me all your data" or "Give me your analog changes" and get very complex answers. Again, because the answer did not exactly match the question, meta-data was required in the response.

— Self-description. The idea that a device could tell the master what data it had available, and how to present it, was already around thanks to UCA 1.0. The DNP3 designers tried to incorporate some of this ability into DNP3. The Device Profile Object and the use of floating-point with the units transmitted were considered very advanced. Perhaps they were too advanced because they appeared in very few implementations.

— Vendor-specific expansion. This standard includes the Private Registration Object, which permits vendors to add proprietary extensions to the basic standard. The Private Registration Object Descriptor permits a standard implementation to parse these extensions even though they are proprietary. These objects, too, have not been very popular, but a few vendors have used them to good effect.

— File transfer. The designers gave DNP3 file transfer capabilities so that an intelligent device could download new configuration or software, or upload oscillography files. At the time DNP3 was developed, few devices had flash memory, and only specialized fault recorder devices performed oscillography. Now both are widespread.

— Program control. The ability to start and stop individual programs and processes on a remote device was common in the factory automation industry. DNP3 provides a rudimentary mechanism to do this.

The dream of the "intelligent network" has had mixed results. Some of these features, like spontaneous reporting, meta-data, prioritization and wild-carding, have worked very well. They are probably some of the main reasons for DNP3's popularity. Other features, like self-description, file transfer, floating-point, program control, and collision avoidance, were not completely thought out. The DNP Technical Committee was forced to revise these and issue technical bulletins clarifying their use. Some features have died a death of obscurity.

Copyright © 2012 IEEE. All rights reserved.

Documents
Document Sharing Hub

Authorized licensed use limited to: Tsinghua University. Downloaded on February 25,2026 at 01:06:46 UTC from IEEE Xplore. Restrictions apply.

Full document details: IEEE 1815-2012

However, history should not be a harsh judge. Many people take such features for granted these days, but it is important to remember that DNP3 was there first.

0.1.8 Additional communications features

Because of the intense pressure to reduce bandwidth, and because the DNP3 designers had more expertise in SCADA than in general data communications, a number of common communications features were "left out" of the DNP3 definition. Many designers have subsequently mourned the absence of these features. Some of them the DNP Technical Committee has attempted to "add on" afterward. Others the Committee could only achieve now at the cost of obsoleting all existing implementations.

The following list of missing data communications features illustrates how well the DNP3 architecture works despite the limitations imposed at its birth:

— Network layer. At one point, the designers actually wrote a specification for a DNP3 network layer, but Westronic management did not approve it. In retrospect, this is just as well, because the Internet Protocol (IP) network layer now used is far more popular.

— Application Layer addresses. The ability to select a particular logical device within a physical one would have been useful. Most devices that support this feature have found a way around it through local software mechanisms that use the Data Link address and/or physical port number as a key.

— Application and Transport Layer sequence number initialization. This has caused much grief over the years and has been addressed as well as possible without causing obsolescence. Data communications experts should note, therefore, that DNP3 is not quite connection-oriented and not quite connectionless, but somewhere in between.

— Long sequence numbers. DNP3 sequence numbers are very short, which is good for bandwidth but not for detecting duplicates. This is the reason Transmission Control Protocol (TCP) is required when using DNP3 over wide area networks (WANs), which turns out to be a very robust solution.

— Sequence number in Data Link Confirms. Without a sequence number, it is impossible to determine which Data Link frame a Confirm frame is answering. On a serial point-to-point link, this is not a problem, but on a WAN, Confirm frames could arrive out of order or be lost. Using TCP in WANs addresses the issue on IP networks, but in theory, it could still cause problems in serial radio networks. In practice, it generally works anyway. This problem was inherited from IEC 60870-5 and cannot be changed without obsolescence.

— Sliding window. One constant of DNP3 has been that only one transaction can be outstanding at a time. In theory, a device could send several response fragments very quickly for a particular request, but over the years the DNP Technical Committee has decided that interoperability is best served by enforcing a confirmation between each fragment.

— Access security. The designers of DNP3 purposely avoided dealing with this issue because of its complexity. However, the flexible structure of DNP3 has permitted access security to be integrated as an optional feature. DNP3 Secure Authentication enables a DNP3 master or outstation to unambiguously determine that it is communicating with the correct device and/or authorized user.

— Version control. Most protocols tend to have an octet reserved to show the version of the protocol in use. This was not included in the original DNP3 definition due to bandwidth reasons; however, the introduction of Object Group 0 addresses this problem.

— Overall length field. Segmentation and fragmentation would have been a lot easier and more robust, and the LAN implementation would have been easier if each fragment had a length field at the beginning. It was not included for bandwidth reasons. Again, various software solutions make it work anyway, so perhaps it was the right decision.

Copyright © 2012 IEEE. All rights reserved.
Documents
Document Sharing Hub
Authorized licensed use limited to: Tsinghua University. Downloaded on February 25,2026 at 01:06:46 UTC from IEEE Xplore. Restrictions apply.
Full document details: IEEE 1815-2012

0.1.9 Compatibility with IEC protocols

As discussed earlier, there were two reasons why the DNP3 designers wanted it to be compliant with the IEC 60870-5 specifications:

— They wanted to take advantage of the excellent technical work done on reliability in the IEC 60870-5 Data Link Layer specifications.

— They wanted to increase the acceptance of the protocol by showing it was based on standards work that was already well known.

They were so successful in both efforts that even now some people are confused about whether DNP3 and IEC 60870-5 are interoperable.

The answer is that they are not interoperable, although the DNP3 Data Link Layer could be considered compliant to IEC 60870-5-1:1990 **[B3]** and IEC 60870-5-2:1992 **[B5]**. DNP3 was based on the drafts available at the time of IEC 60870-5 Parts 1 through 5. These Parts of the specification described the Data Link Layer in great detail and the Application Layer in general. There were several options specified for the Data Link Layer.

The DNP3 designers chose those options of IEC 60870-5-1:1990 **[B3]** and IEC 60870-5-2:1992 **[B5]** they thought were most appropriate. Unfortunately, when the IEC 60870-5-101:2003 **[B4]** companion standard was released with the details of the Application Layer, it specified *different* Data Link Layer options than those the DNP3 designers had chosen.

Therefore, DNP3 is considered compliant with IEC 60870-5-1:1990 **[B3]** and 60870-5-2:1992 **[B5]** but not with IEC 60870-5-101:2003 **[B4]**.

Table 0-1 shows the differences in the Data Link Layers of the two protocols.

Copyright © 2012 IEEE. All rights reserved.
Documents
Document Sharing Hub
Authorized licensed use limited to: Tsinghua University. Downloaded on February 25,2026 at 01:06:46 UTC from IEEE Xplore. Restrictions apply.
Full document details: IEEE 1815-2012

Table 0-1—Comparison of IEC 60870-5 and DNP3 Data Link Layers

Feature	Options permitted in IEC 60870-5-1:1990 [B3] and IEC 60870-5-2:1992 [B5]	Chosen by DNP3	Chosen by IEC 60870-5-101:2003 [B4]
Addressing	Single address, length system-dependent	Two-octet Source address and two-octet Destination address. Considered a single four-octet "structured" address for compliance purposes.	Single address, choice of either zero, one, or two octets in length
Frame Format	Choice of FT1.1, FT1.2, FT2, and FT3	FT3, transmitted asynchronously.	FT1.2
Reliability Mechanism	Varies per frame type	Multiple 16-bit CRCs over each 16 octets of a 255-octet frame. Start and Stop bits, but no parity.	Parity bits and one-octet checksum (not CRC) calculated over 255 octets
Hamming Distance	Varies per frame type	6 for the original FT3. Some debate about the value as currently used. See further discussion in this subclause.	4
Acknowledgments	Either fixed-length or single-octet	Fixed 10-octet only.	Either fixed-length or single-octet
Procedures	Balanced (no master) or Unbalanced (master polls)	Balanced only.	Either Balanced or Unbalanced
Method for Multi-Drop Links	Unbalanced mode	Collision avoidance.	Unbalanced mode

0.1.9.1 Hamming Distance

Some critics of DNP3 have disputed DNP3's right to claim a Hamming Distance of six. The "Hamming Distance" of a protocol is the number of bit errors required in a frame before a receiver could incorrectly identify a corrupted incoming frame as a valid frame. Critics argue that the original calculation was made assuming the FT3 frame was transmitted synchronously, while DNP3 uses the FT3 frame format asynchronously.

The main concern in this debate is inter-character gaps. If a gap is permitted between the octets of a 16-octet block, noise could be introduced that might be misinterpreted as valid data. In fact, it has been shown that there exists at least one case where an inter-character gap of exactly 1-bit time at the end of a message can be misinterpreted, thereby resulting in a Hamming distance of 2. Critics claim that this standard has never *required* that all octets of a block be transmitted together, and this reduces the theoretical reliability of the protocol to below that of the FT1.2 frame.

However, years of use in hundreds of systems have proven DNP3's reliability to be more than sufficient for utility purposes. This may be due to the fact that most DNP3 devices transmit frames without inter-character gaps, and receiving devices tend to start a timer or other mechanism that discards incoming frames when inter-character gaps appear.

The inter-character concern with the DNP3 frame is similar to a problem that occurs in some IEC 608705-101 systems. The FT1.2 frame's reliability relies on the use of parity bits in each octet. However, many utilities mistakenly use the protocol with modems that do not add, or actually remove, such parity bits. The IEC is preparing an IEC 60870-5 standard that clarifies parity bits *shall* be used.

Copyright © 2012 IEEE. All rights reserved.

Documents
Document Sharing Hub

Authorized licensed use limited to: Tsinghua University. Downloaded on February 25,2026 at 01:06:46 UTC from IEEE Xplore. Restrictions apply.

Full document details: IEEE 1815-2012

0.1.9.2 Addressing of binary outputs

The other main issue concerning DNP3 compliance to IEC 60870-5 was the structure of the address field. The IEC definition of the address field states that it is a single address, always addressing one end of the link. This is the way IEC 60870-5-101:2003 **[B4]** uses the address field.

By including both a source and a destination in every message, the DNP3 designers permitted the use of multiple masters on the same link, and peer-to-peer communications. This proved to be a powerful argument in the acceptance of DNP3. Furthermore, since IEC 60870-5-2:1992 **[B5]** did not specify a particular length of address, a four-octet address that just happened to be "structured" with two sub-addresses could still be considered compliant.

0.1.9.3 Reality today

Although it was the topic of lively debate when DNP3 was first released, the question of whether DNP3 complies with IEC 60870-5 is essentially a moot point today. DNP3 may be considered compliant to Parts 1 and 2. One could even argue that DNP3 complies with the spirit, if not the letter, of Part 5, the general Application Layer definition. However, the format of the IEC 60870-5-101 **[B2]** Application Layer is very different from that of DNP3. It is clear the two protocols could never interoperate.

It is better to consider the two protocol suites as cousins with a common family tree and leave it at that.

0.1.10 Transport Function

The naming of the Transport Function always confuses newcomers to DNP3. Is it a true Transport Layer, is it a part of the Data Link Layer, or is it something truly different?

The answer is that it really is something different, although it most closely resembles an additional field in the Data Link Layer. It does not have its own addressing or acknowledgments, as a separate layer would. There was no network layer in the original protocol definition, so the transport header was terminated at the end of each physical link, just like the data link header. It does not have the long sequence numbers and other features that would really enforce transmitting frames in sequence. Therefore, it does not seem to be a Transport Layer.

However, if it were a field of the data link header, it would be included in every data link frame, and it is not. Only those frames containing Application Layer data contain a transport header.

The reasons this strange "half-layer" exists are both political and technical. The designers of DNP3 decided they wanted the Application Layer data broken into small segments suitable for passing over noisy links. This capability would at a minimum require a new Data Link Layer field. However, they did not want to add a new field for two reasons:

a) It would eliminate DNP3's chances to be considered compliant to IEC 60870-5. As discussed earlier, this was considered critical to DNP3's acceptance by the industry.

b) Changing the structure of the FT3 frame could possibly compromise the calculated reliability of the frame.

Therefore, the transport header was placed in front of the Application Layer header, in the user data field of the Data Link Layer frame.

However, the next question was, "What to call it?" As noted in this subclause, it had some of the characteristics of a layer but not all of them. Furthermore, the designers knew there would be resistance to any additional layers in the protocol. It was bad enough that they were dedicating *a whole octet* to the segmentation and reassembly functions.

Copyright © 2012 IEEE. All rights reserved.

Documents
Document Sharing Hub

Authorized licensed use limited to: Tsinghua University. Downloaded on February 25,2026 at 01:06:46 UTC from IEEE Xplore. Restrictions apply.

Full document details: IEEE 1815-2012

Therefore, the name “Transport Function” was chosen, thus causing years of questions on hotlines, e-mails, and training presentations.

Whatever it is, it makes DNP3 distinct. Along with Application Layer fragmentation, it permits a small, low-powered device to report a nearly unlimited amount of data reliably over a noisy link.

0.1.11 DNP Users Group

One feature of DNP3 that newcomers do not always appreciate is the organization that stands behind it. Over the years, the DNP Users Group has contributed at least as much to the protocol’s success as the technical features of the protocol itself.

In roughly chronological order, here are the organizational features that helped DNP3 become popular:

- Membership that included both utilities and vendors
- Low membership fees
- Low cost of the specifications
- A structure consisting of steering, technical, and marketing committees
- The DNP3 Subset Definitions document
- Suggested wordings for utilities to specify DNP3
- Agreement that any non-backward compatible change shall be approved by the General Membership
- The DNP3 hotline, later to become an Internet chat session
- Booths at major trade shows
- Publishing membership lists so utilities could see the lists of vendors
- The DNP3 bulletin board, later to become a Web site
- The DNP3 e-mail mailing list
- The DNP Technical Committee mailing list, which can include non-committee members
- Publishing the technical committee minutes so the process remains open
- Technical bulletins clarifying areas of dispute when interoperability issues arose
- Agreement, first informal and then formal, that the president should always be from a utility
- The DNP3 IED Application Level Conformance Test Documents[c]
- The DNP3 WAN/LAN Specification

0.1.12 Summary

The following design goals, whether formally stated or not at the time, had a major impact on the structure of DNP3:

- Include the best features of the utility protocols in use at the time.
- Push the intelligence in the network toward the remote device.
- Try to comply as much as possible with existing standards efforts, especially IEC 60870-5.

[c] Refer to http//www.dnp.org.

Copyright © 2012 IEEE. All rights reserved.

Documents
Document Sharing Hub

Authorized licensed use limited to: Tsinghua University. Downloaded on February 25,2026 at 01:06:46 UTC from IEEE Xplore. Restrictions apply.

Full document details: IEEE 1815-2012

— Use as little bandwidth as possible.

— Make it more reliable than anything that came before.

It is easy to see that these goals are necessarily contradictory. The resulting protocol was not perfect and has been "patched up" over the years. However, it remains popular, open, reliable, and mostly backward-compatible.

0.1.13 Background: Origins of the name "DNP3"

Few people seem to know what to call this protocol. Everyone knows it is DNP3, but is it "DNP 3," "DNP 3.0," "DNP V3.0," or any combination of the above? Also, there are several different subset levels of implementation, and a few non-backward-compatible changes have been made over the years.

As of Technical Bulletin TB2000-003: "Change Management," the official name of the protocol is DNP3-xxxx, where xxxx is the year of release of the Test Procedures to which a device complies. The subset level is specified afterward, as in "DNP3-2000 Level 2."

This naming convention represents an evolution of the name over the years:

— The original Basic 4 documentation referred to the protocol as "DNP V3.00." No one has ever liked saying the "V" part, so that name has never caught on.

— For those who were wondering: DNP V1.00 and DNP V2.00 are proprietary Westronic protocols that were rarely used even at the time DNP3 was released.

— The user's group is called just the "DNP Users Group." That saves it from having to worry about version numbers in marketing information.

— The Subset Definitions defined the format DNP3-Lx, where x was the subset level. That never caught on either, since utilities preferred to spell out the words "Level x" in their bid specs.

— When the Test Procedures were first published in 2000, there had to be some mechanism to distinguish between an implementation that was compliant to the procedures and earlier implementations that were not. The DNP Technical Committee therefore decided to use the year in the specification, similar to the format used by the International Organization for Standardization (ISO), IEEE, and IEC.

— The intent is that there shall never be a DNP 4.0, or even a DNP 3.1. To help illustrate this commitment to backward compatibility, the DNP Users Group changed the name from "DNP V3.00" to "DNP3." The name therefore remains recognizable while eliminating the "software version" impression that the decimal point gave.

Some people rightly complain that it is redundant to say "DNP3 protocol" since the "P" in DNP3 stands for "Protocol" already. However, this truism does not seem to discourage people from using the phrase, and it is likely to be heard for years to come.

Now if one could just figure out how a protocol that originally had no network layer ended up with the name "Distributed *Network* Protocol." One long-standing DNP3 user points out that the networks in question are SCADA networks, which "bear scant resemblance to other things that people usually call networks." Perhaps this is the case.

Ah well, a protocol by any other name is just as interoperable and reliable.

Copyright © 2012 IEEE. All rights reserved.

Documents
Document Sharing Hub

Authorized licensed use limited to: Tsinghua University. Downloaded on February 25,2026 at 01:06:46 UTC from IEEE Xplore. Restrictions apply.

Full document details: IEEE 1815-2012

0.2 DNP3 overview

0.2.1 Basic messages and data flow

The document is a brief, but incomplete, overview of DNP3 messages and data flow. Its purpose is to prepare the reader for what follows in the Application Layer, Transport Function, and Data Link Layer specifications for DNP3.

NOTE—Unless otherwise noted, DNP3 makes no representation about how data is processed once it is received.[d]

This initial discussion of DNP3 uses the master–outstation model illustrated in **Figure 0-1**. This subclause purposely omits many details to keep the description straightforward.

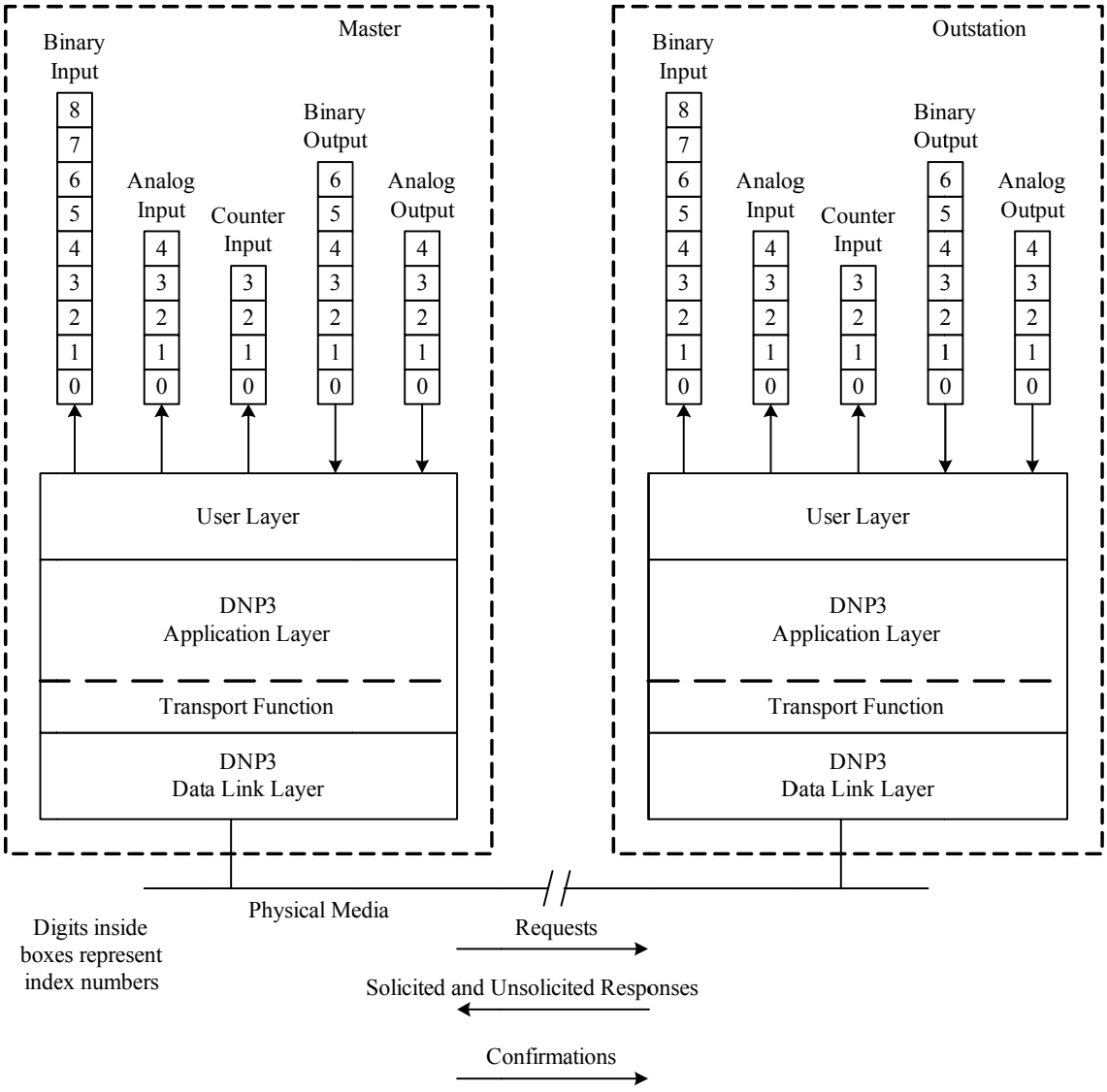


Figure 0-1—DNP3 master–outstation model

[d] Notes in text, tables, and figures of a standard are given for information only and do not contain requirements needed to implement this standard.

Copyright © 2012 IEEE. All rights reserved.
Documents
Document Sharing Hub
Authorized licensed use limited to: Tsinghua University. Downloaded on February 25,2026 at 01:06:46 UTC from IEEE Xplore. Restrictions apply.
Full document details: IEEE 1815-2012

The User Layer in the master on the left side of **Figure 0-1** initiates a data transfer by causing its Application Layer to send a request to the outstation. The request contains a function code and zero or more DNP3 objects that specify what data is wanted. The Application Layer passes the request on to the Transport Function for partitioning into transmission-sized units and then on to the Data Link Layer. The Data Link Layer adds addressing and error detection information and transmits the packet to the outstation over the physical media.

At the outstation on the right side, the Data Link Layer receives the octets from the physical layer and checks for errors that were introduced while the packet was in transit. If no errors are detected, the addressing and error detection information added by the transmitting Data Link Layer is stripped from the message, and the remaining octets are passed on to the Application Layer. If necessary, the Transport Function reassembles multiple packets into a complete request. The Application Layer then interprets the function code and DNP3 objects in the message and indicates to the User Layer what data is desired.

The User Layer in the outstation initiates a response based on what data the master requested. It fetches data, classifies it, and presents that data to the Application Layer. The Application Layer creates a message with data formatted into DNP3 objects, passes it through the Transport Function, and then on to the Data Link Layer for transmission to the master using methods similar to those employed by the master to send its request.

Upon receipt of the response at the master, the layers perform address and error checking and reassembly into a complete message for the Application Layer. This layer parses the DNP3 objects in the response and presents the information to the User Layer. The User Layer can then store or operate on that data in a way that is suitable for the end user.

The master always initiates control commands. These actuate device outputs or variables internal to the outstation. The DNP3 User-to-Application Layer interface and transmission procedures are similar to those discussed for data acquisition.

A transaction consists of a single request followed by a single response. A master sends a request and waits for the response, or a timeout, before issuing another request. Multiple transactions may simultaneously occur within a system. For example, consider the case where two masters each make requests to the same outstation.

In some systems the master does not always directly initiate data transfer. DNP3 has provision for the outstation to automatically send data when it detects a condition worthy of transmitting without a specific master request. “Unsolicited Responses” is the terminology applied to this type of operation because the request is implied.

0.2.2 Layering

0.2.2.1 General

ISO defines a communication architecture that separates functions into seven layers called the OSI reference model. DNP3 protocol is based on a simplified model termed the Enhanced Performance Architecture (EPA) that consists of only three layers: Application, Data Link, and Physical. **Figure 0-1** shows how DNP3 fits the EPA structure and communication model.

In theory, each layer in a layer stack performs a set of functions required to communicate with the same layer in another device, relying on the next lower layer for more primitive functions. At the sending device, each layer below the Application Layer receives data from the layer above for transmission. The layer adds more information that enables the equivalent layer in the receiver to properly process the message. At the receiving device, layers examine their layer specific information added by the corresponding layer at the transmission site and process the message appropriately. The layer control information is stripped, and the message is passed to the next higher layer.

Copyright © 2012 IEEE. All rights reserved.
Documents
Document Sharing Hub
Authorized licensed use limited to: Tsinghua University. Downloaded on February 25,2026 at 01:06:46 UTC from IEEE Xplore. Restrictions apply.
Full document details: IEEE 1815-2012

The Transport Function within the Application Layer performs a layer-like function of partitioning large messages into smaller messages that the Data Link Layer is capable of handling. The Transport Function is sometimes referred to as a "pseudo layer." In DNP3 the Application Layer, Transport Function, and the Data Link Layer in the transmitter add information to the message for enabling the same layer or pseudo layer in the receiver to process the message.

0.2.2.2 Fragments, segments, and frames

Figure 0-2 illustrates the partitioning of large messages at the Application Layer into smaller units and the addition of header information at each layer.

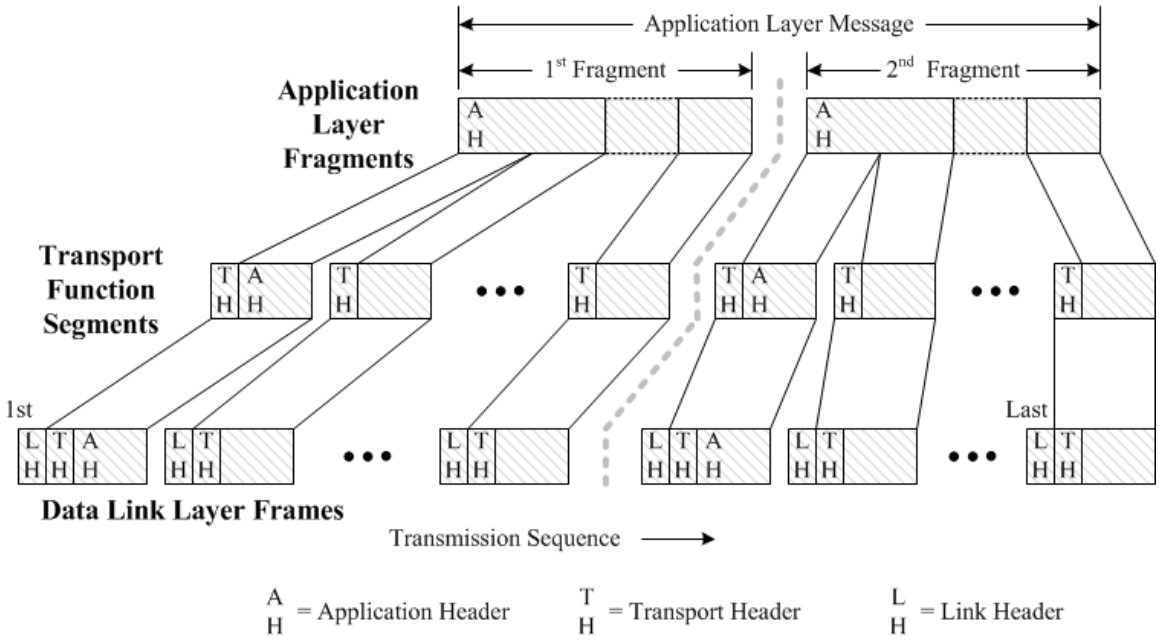


Figure 0-2—Fragmented Application Layer message

Figure 0-2 shows a fragmented Application Layer message, segmentation of each fragment by the Transport Function, and how segments fit into Data Link Layer frames. This diagram does not show timing and confirmation details but serves to demonstrate how the higher level parts nest inside the lower layer structures. It also shows the relative positions of the Application Layer headers, the Transport Function headers, and the Data Link Layer headers.

Table 0-2 provides a summary of the terminology and some brief information associated with each layer or function.

Copyright © 2012 IEEE. All rights reserved.
Documents
Document Sharing Hub
Authorized licensed use limited to: Tsinghua University. Downloaded on February 25,2026 at 01:06:46 UTC from IEEE Xplore. Restrictions apply.
Full document details: IEEE 1815-2012

Table 0-2—DNP3 layer summary

Layer or function	Unit name	Information
Application Layer	Application Fragment	Permits the setting of an upper limit on the memory requirements for message reception. Requests shall fit into a single fragment. Responses may require more than one fragment.
Transport Function	Transport Segment	Segmentation breaks a Data Link fragment into pieces that fit into a Data Link frame. Each segment contains a Transport header, but only the first segment of any fragment contains an Application header. Each segment may have a maximum of 250 octets including the Transport header.
Data Link Layer	Data Link Frame	A Frame may have as many as 292 octets including its header and CRC octets. Frames are designed for superior error detection.

0.2.3 Message sequences

Figure 0-3 illustrates a hypothetical sequence and the time relationship of fragments and frames as they move between layers, and between the master and the outstation in a **polled** environment. Readers just beginning to learn this standard are cautioned to only view the diagram as a means of gaining a general overview.

Figure 0-4 illustrates a hypothetical sequence and the time relationship of fragments and frames as they move between layers, and between the master and the outstation in an **unsolicited response** environment. Readers just beginning to learn this standard are cautioned to only view the diagram as a means of gaining a general overview. Later, after studying the details, refer back to this figure when it may be more meaningful.

Copyright © 2012 IEEE. All rights reserved.

Documents
Document Sharing Hub

Authorized licensed use limited to: Tsinghua University. Downloaded on February 25,2026 at 01:06:46 UTC from IEEE Xplore. Restrictions apply.

Full document details: IEEE 1815-2012

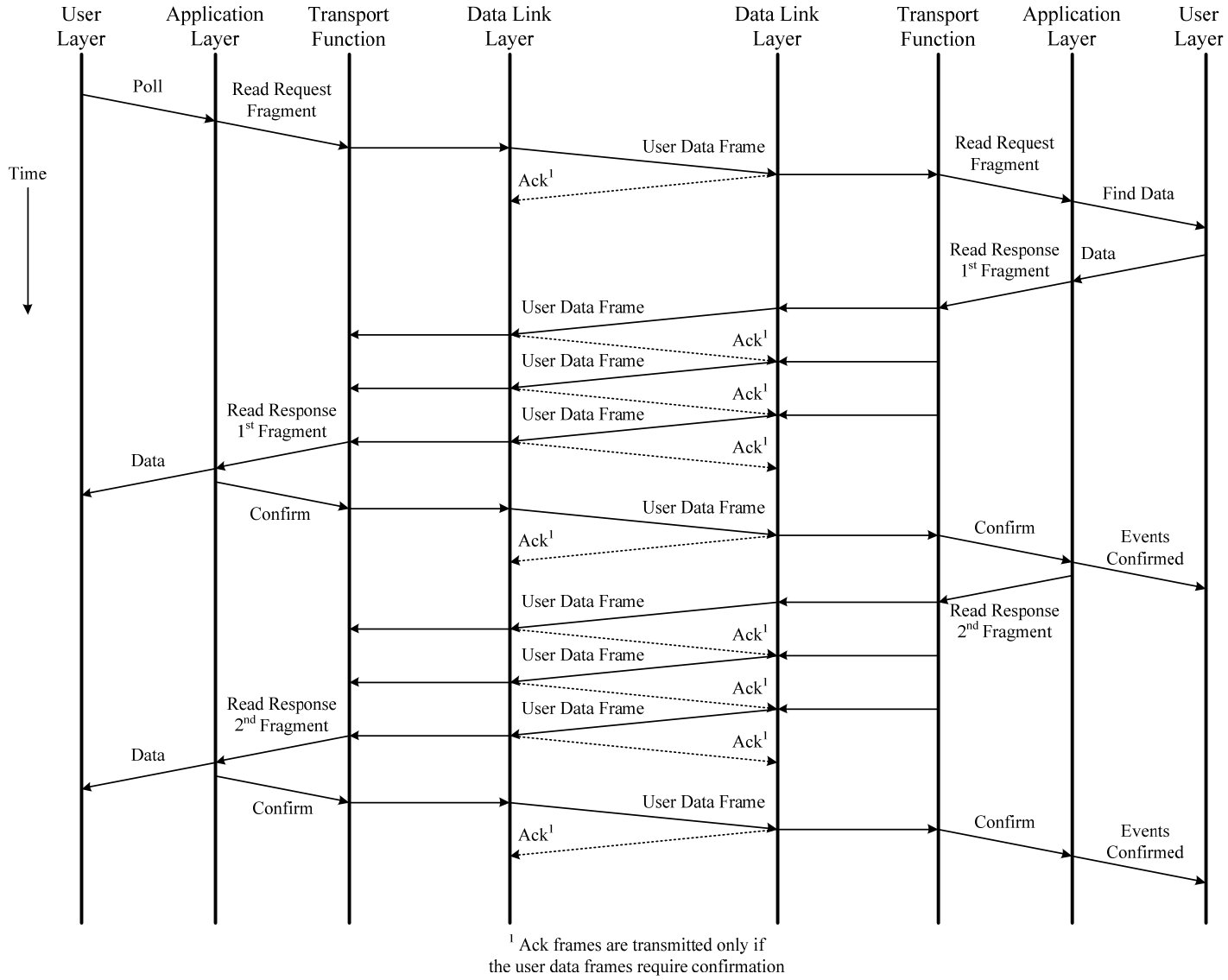


Figure 0-3—Polled sequence with Data Link Layer confirmation

Copyright © 2012 IEEE. All rights reserved.

Authorized licensed use limited to: Tsinghua University. Downloaded on February 25,2026 at 01:06:46 UTC from IEEE Xplore. Restrictions apply.

Full document details: IEEE 1815-2012

Documents
Document Sharing Hub

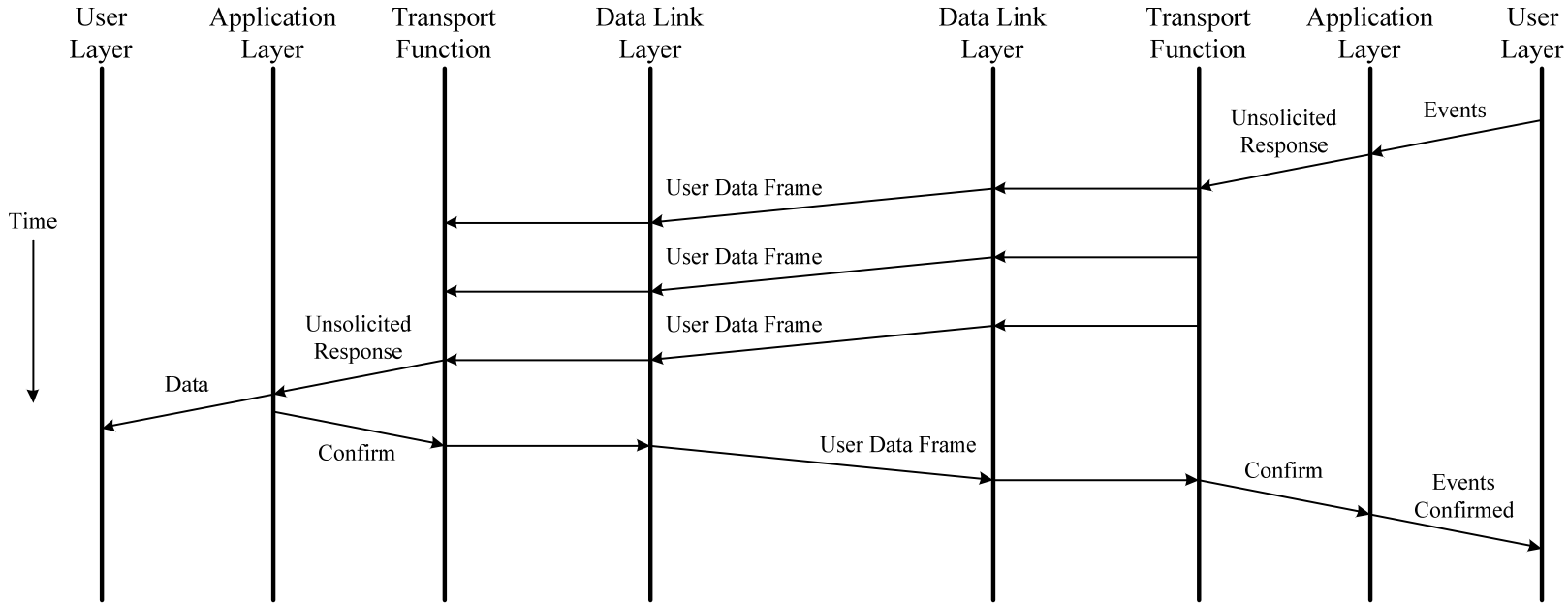


Figure 0-4—Unsolicited response sequence

Copyright © 2012 IEEE. All rights reserved.

Full document details: IEEE 1815-2012
Authorized licensed use limited to: Tsinghua University. Downloaded on February 25,2026 at 01:06:46 UTC from IEEE Xplore. Restrictions apply.
Documents
Document Sharing Hub

0.2.4 Data loss and efficiency

One of the fundamental goals of DNP3 is to prevent loss of data transferred from an outstation to the master. Of special concern is the transfer of all binary input states, in time sequence, and without missing any transitions.

To increase the efficiency, DNP3 provides for report-by-exception whereby changes are transmitted soon after they occur, and an occasional integrity poll is issued to synchronize the master and outstation databases. When an outstation transmits changes, it shall request Application Layer confirmation. Only after the master confirms receipt of the changes can the outstation assume the changes arrived at the master.

Outstation devices that are able to report all of their current data in a single frame are not required to support report-by-exception.

0.2.5 Unsolicited responses

Unsolicited responses are messages spontaneously sent from an outstation without a specific request from a master when "something of significance" occurs. The DNP3 protocol includes support for unsolicited responses.

This method of operating has advantages in some applications. In a system with a large number of outstations and a single master, changes at an outstation can reach the master often much faster because there is no delay while waiting for a master poll. The communication costs to achieve faster polling in some installations can be prohibitive, and the quickest notification of changes can occur if most of the messages contain only changes and confirmations. Unsolicited operation may reduce costs where the owners choose a "cost-per-byte" type of service.

On the other hand, equipment that implements unsolicited responses is more complex because the issues of media access and collision avoidance should be dealt with. The DNP3 specification requires that master station software is capable of accepting messages from any of its outstations at any time. Another disadvantage is that system performance may become unpredictable during periods of heavy communication.

Employing unsolicited reporting requires an engineering judgment based on numerous factors for each individual system. There are no guarantees that unsolicited reporting is universally applicable for all systems.

A description and rules for unsolicited responses are provided in Clause **4** through Clause **6** of this standard.

0.2.6 IP networking

DNP3 was originally designed for serial octet streaming, point-to-point communications over voice grade audio links, or hard-wired, multi-drop wire and fiber cabling. As IP networking evolved, users recognized a need for devices to exchange DNP3 messages over these high-speed, packet-based, digital networks. DNP3 now includes this capability.

The approach taken was to place DNP3 as the user of an IP stack and to retain all the same Application Layer, Transport Function, and Data Link Layer structures, objects, and formats as in the original DNP3. Thus, DNP3 Data Link Layer frames are passed transparently across an IP network as TCP or User Datagram Protocol (UDP) packets.

A description and special rules are described in Clause **13** and **Annex C** of this standard.

Copyright © 2012 IEEE. All rights reserved.
Documents
Document Sharing Hub
Authorized licensed use limited to: Tsinghua University. Downloaded on February 25,2026 at 01:06:46 UTC from IEEE Xplore. Restrictions apply.
Full document details: IEEE 1815-2012

0.3 Organization of DNP3 Specification

The complete DNP3 Specification is organized into separate clauses wherein details of the DNP3 protocol are documented as follows[e]:

Clause **0** through Clause **3** and **Annex A**:	DNP3 Introduction (formerly known as Volume 1)
Clause **4** through Clause **7**:	Application Layer (formerly known as Volume 2)
Clause **8**:	Transport Function (formerly known as Volume 3)
Clause **9**:	Data Link Layer (formerly known as Volume 4)
Clause **10**:	Layer Independent Topics (formerly known as Volume 5)
Clause **11**, Clause **12**, and **Annex A**:	Data Object Library (formerly known as Volume 6)
Clause **13** and **Annex C**:	IP Networking (formerly known as Volume 7)
Clause **14**:	Interoperability (formerly known as Volume 8)

0.4 Conventions used in this standard

0.4.1 Notes

NOTEs within the text are informative. They are set apart as a separate paragraph beginning with "NOTE—".

0.4.2 Examples

Examples are preceded with a box describing what is illustrated below. The number **EX 0-1** represents the example number.

EX 0-1	This example shows a request for all of the static binary inputs. Assume there are 18 binary inputs.

0.4.3 Single master, single outstation perspective

The DNP3 protocol is suitable for systems with one or more master stations, one or more outstations, and peer-to-peer arrangements. In general, this standard was written from the perspective of a single master and a single outstation to make the documents easier to understand without the additional complexities involved.

A separate subclause (**13.2.3.5**) is devoted to discussion of multi-master systems and their special considerations and requirements. Statements appear elsewhere only when it is necessary to emphasize specific characteristics or behavior for systems with multiple master or outstation devices.

[e] The DNP3 Specification was identified by volumes prior to IEEE Std 1815-2010 standardization.

Copyright © 2012 IEEE. All rights reserved.

Documents
Document Sharing Hub

Authorized licensed use limited to: Tsinghua University. Downloaded on February 25,2026 at 01:06:46 UTC from IEEE Xplore. Restrictions apply.

Full document details: IEEE 1815-2012

Contents

0 Introduction viii
0.1 DNP3 purpose and history viii
0.2 DNP3 overview xviii
0.3 Organization of DNP3 Specification xxv
0.4 Conventions used in this standard xxv

1 Overview 2
1.1 Scope 2
1.2 Purpose 2
1.3 Octet order 2

2 Normative references 3

3 Definitions, acronyms, and abbreviations 5
3.1 Definitions 5
3.2 Acronyms and abbreviations 9
3.3 Special terms 12

4 Application Layer—part 1 13
4.1 Application Layer preface 13
4.2 Message structure 19
4.3 Fragment rules 38
4.4 Detailed function code procedures 40
4.5 Detailed IIN bit descriptions 81
4.6 Unsolicited responses 88
4.7 Support for functions sent to a broadcast address 99

5 Application Layer—part 2 101
5.1 Additional details 101
5.2 Using virtual terminal objects 109
5.3 Sequential file transfer 112
5.4 Data sets 120
5.5 Device attributes 148

6 Application Layer—part 3: State tables and diagrams 155
6.1 Outstation fragment state table 155
6.2 Outstation fragment state diagram 161
6.3 Master solicited response reception state table 163
6.4 Master solicited response reception state diagram 167
6.5 Master unsolicited response reception state table 167
6.6 Master unsolicited response reception state diagram 170

7 Secure authentication 171
7.1 Purpose 171
7.2 Threats addressed 171
7.3 General principles 171
7.4 Theory of operation 173
7.5 Formal specification 186
7.6 Interoperability requirements 241
7.7 Special applications 251
7.8 Compliance with IEC/TS 62351-3 254
7.9 Compliance with IEC/TS 62351-5 258
7.10 Compliance with ISO/IEC 11770 260

Copyright © 2012 IEEE. All rights reserved.

Documents
Document Sharing Hub

Authorized licensed use limited to: Tsinghua University. Downloaded on February 25,2026 at 01:06:46 UTC from IEEE Xplore. Restrictions apply.

Full document details: IEEE 1815-2012

8 Transport Function 267
8.1 Overview 267
8.2 Transport Function description 268

9 Data Link Layer 274
9.1 Layering overview 274
9.2 DNP3 Data Link Layer description 274
9.3 State tables and diagrams 287

10 Layer-independent topics 295
10.1 Purpose of layer-independent topics 295
10.2 Confirmation and retry guidelines 295
10.3 Time synchronization 298
10.4 Handling multiple messages 305

11 Data object library—basics 307
11.1 Overview 307
11.2 Library documentation organization 307
11.3 Primitive data types 307
11.4 Object data type codes 321
11.5 DNP3 object types 321
11.6 Object flags 322
11.7 Status codes 329
11.8 Group number categories 331
11.9 Point types 331

12 DNP3 object library—parsing codes 351
12.1 Subset parsing codes 351
12.2 Parsing guidelines 362

13 IP networking 376
13.1 IP networking overview 376
13.2 Layer requirements 377
13.3 Security 390
13.4 Time synchronization 390
13.5 UML statecharts 390

14 Interoperability 393
14.1 About this clause 393
14.2 Overview 394
14.3 Level 1 DNP3 implementation (DNP3-L1) 396
14.4 Level 2 DNP3 implementation (DNP3-L2) 400
14.5 Level 3 DNP3 implementation (DNP3-L3) 404
14.6 Level 4 DNP3 implementation (DNP3-L4) 411
14.7 Conformance 427
14.8 XML representation 428
14.9 Instructions for creating a Device Profile document 436

Annex A (normative) DNP3 data object library—object descriptions 438
A.1 Object group 0: device attributes 438
A.1.1 Device attributes—secure authentication version 438
A.1.2 Device attributes—number of security statistics per association 439
A.1.3 Device attributes—identification of support for user-specific attributes 440
A.1.4 Device attributes—number of master-defined data set prototypes 443
A.1.5 Device attributes—number of outstation-defined data set prototypes 444
A.1.6 Device attributes—number of master-defined data sets 445
A.1.7 Device attributes—number of outstation-defined data sets 446

Copyright © 2012 IEEE. All rights reserved.

Documents
Document Sharing Hub

Authorized licensed use limited to: Tsinghua University. Downloaded on February 25,2026 at 01:06:46 UTC from IEEE Xplore. Restrictions apply.

Full document details: IEEE 1815-2012

A.1.8 Device attributes—maximum number of binary output objects per request 447
A.1.9 Device attributes—local timing accuracy....448
A.1.10 Device attributes—duration of time accuracy 450
A.1.11 Device attributes—support for analog output events 452
A.1.12 Device attributes—maximum analog output index 453
A.1.13 Device attributes—number of analog outputs 454
A.1.14 Device attributes—support for binary output events....455
A.1.15 Device attributes—maximum binary output index....456
A.1.16 Device attributes—number of binary outputs....457
A.1.17 Device attributes—support for frozen counter events 458
A.1.18 Device attributes—support for frozen counters....459
A.1.19 Device attributes—support for counter events 460
A.1.20 Device attributes—maximum counter index 461
A.1.21 Device attributes—number of counter points....462
A.1.22 Device attributes—support for frozen analog inputs....463
A.1.23 Device attributes—support for analog input events 464
A.1.24 Device attributes—maximum analog input index 465
A.1.25 Device attributes—number of analog input points 466
A.1.26 Device attributes—support for double-bit binary input events....467
A.1.27 Device attributes—maximum double-bit binary index 468
A.1.28 Device attributes—number of double-bit binary input points 469
A.1.29 Device attributes—support for binary input events....470
A.1.30 Device attributes—maximum binary input index....471
A.1.31 Device attributes—number of binary input points 472
A.1.32 Device attributes—maximum transmit fragment size 473
A.1.33 Device attributes—maximum receive fragment size....474
A.1.34 Device attributes—device manufacturer's software version 475
A.1.35 Device attributes—device manufacturer's hardware version 476
A.1.36 Device attributes—user-assigned location name....477
A.1.37 Device attributes—user-assigned ID code/number 478
A.1.38 Device attributes—user-assigned device name 479
A.1.39 Device attributes—device serial number....480
A.1.40 Device attributes—DNP3 subset and conformance....481
A.1.41 Device attributes—device manufacturer's product name and model 483
A.1.42 Device attributes—device manufacturer's name....484
A.1.43 Device attributes—non-specific all attributes request 485
A.1.44 Device attributes—list of attribute variations....486
A.2 Object group 1: binary inputs....488
A.2.1 Binary input—packed format 488
A.2.2 Binary input—with flags 489
A.3 Object group 2: binary input events 490
A.3.1 Binary input event—without time 490
A.3.2 Binary input event—with absolute time 491
A.3.3 Binary input event—with relative time 492
A.4 Object group 3: double-bit binary inputs 493
A.4.1 Double-bit binary input—packed format....493
A.4.2 Double-bit binary input—with flags....494
A.5 Object group 4: double-bit binary input events....495
A.5.1 Double-bit binary input event—without time....495
A.5.2 Double-bit binary input event—with absolute time 496
A.5.3 Double-bit binary input event—with relative time....497
A.6 Object group 10: binary outputs....498
A.6.1 Binary output—packed format 498
A.6.2 Binary output—output status with flags....500
A.7 Object group 11: binary output events 501
A.7.1 Binary output event—status without time 501
A.7.2 Binary output event—status with time 503

Copyright © 2012 IEEE. All rights reserved.

Documents
Document Sharing Hub

Authorized licensed use limited to: Tsinghua University. Downloaded on February 25,2026 at 01:06:46 UTC from IEEE Xplore. Restrictions apply.

Full document details: IEEE 1815-2012

A.8 Object group 12: binary output commands 505
A.8.1 Binary output command—control relay output block—also known as CROB 505
A.8.2 Binary output command—pattern control block—also known as PCB 511
A.8.3 Binary output command—pattern mask 513
A.9 Object group 13: binary output command events 514
A.9.1 Binary output command event—command status without time 514
A.9.2 Binary output command event—command status with time 516
A.10 Object group 20: counters 517
A.10.1 Counter—32-bit with flag 517
A.10.2 Counter—16-bit with flag 518
A.10.3 Counter—32-bit with flag, delta 519
A.10.4 Counter—16-bit with flag, delta 520
A.10.5 Counter—32-bit without flag 521
A.10.6 Counter—16-bit without flag 522
A.10.7 Counter—32-bit without flag, delta 523
A.10.8 Counter—16-bit without flag, delta 524
A.11 Object group 21: frozen counters 525
A.11.1 Frozen counter—32-bit with flag 525
A.11.2 Frozen counter—16-bit with flag 526
A.11.3 Frozen counter—32-bit with flag, delta 527
A.11.4 Frozen counter—16-bit with flag, delta 528
A.11.5 Frozen counter—32-bit with flag and time 529
A.11.6 Frozen counter—16-bit with flag and time 531
A.11.7 Frozen counter—32-bit with flag and time, delta 533
A.11.8 Frozen counter—16-bit with flag and time, delta 535
A.11.9 Frozen counter—32-bit without flag 537
A.11.10 Frozen counter—16-bit without flag 538
A.11.11 Frozen counter—32-bit without flag, delta 539
A.11.12 Frozen counter—16-bit without flag, delta 540
A.12 Object group 22: counter events 541
A.12.1 Counter event—32-bit with flag 541
A.12.2 Counter event—16-bit with flag 542
A.12.3 Counter event—32-bit with flag, delta 543
A.12.4 Counter event—16-bit with flag, delta 544
A.12.5 Counter event—32-bit with flag and time 545
A.12.6 Counter event—16-bit with flag and time 547
A.12.7 Counter event—32-bit with flag and time, delta 549
A.12.8 Counter event—16-bit with flag and time, delta 551
A.13 Object group 23: frozen counter events 553
A.13.1 Frozen counter event—32-bit with flag 553
A.13.2 Frozen counter event—16-bit with flag 554
A.13.3 Frozen counter event—32-bit with flag, delta 555
A.13.4 Frozen counter event—16-bit with flag, delta 556
A.13.5 Frozen counter event—32-bit with flag and time 557
A.13.6 Frozen counter event—16-bit with flag and time 559
A.13.7 Frozen counter event—32-bit with flag and time, delta 561
A.13.8 Frozen counter event—16-bit with flag and time, delta 563
A.14 Object group 30: analog inputs 565
A.14.1 Analog input—32-bit with flag 565
A.14.2 Analog input—16-bit with flag 566
A.14.3 Analog input—32-bit without flag 567
A.14.4 Analog input—16-bit without flag 568
A.14.5 Analog input—single-precision, floating-point with flag 569
A.14.6 Analog input—double-precision, floating-point with flag 570
A.15 Object group 31: frozen analog inputs 571
A.15.1 Frozen analog input—32-bit with flag 571
A.15.2 Frozen analog input—16-bit with flag 572

Copyright © 2012 IEEE. All rights reserved.

Documents
Document Sharing Hub

Authorized licensed use limited to: Tsinghua University. Downloaded on February 25,2026 at 01:06:46 UTC from IEEE Xplore. Restrictions apply.

Full document details: IEEE 1815-2012

A.15.3 Frozen analog input—32-bit with time-of-freeze 573
A.15.4 Frozen analog input—16-bit with time-of-freeze 575
A.15.5 Frozen analog input—32-bit without flag 577
A.15.6 Frozen analog input—16-bit without flag 578
A.15.7 Frozen analog input—single-precision, floating-point with flag 579
A.15.8 Frozen analog input—double-precision, floating-point with flag 580
A.16 Object group 32: analog input events 581
A.16.1 Analog input event—32-bit without time 581
A.16.2 Analog input event—16-bit without time 582
A.16.3 Analog input event—32-bit with time 583
A.16.4 Analog input event—16-bit with time 585
A.16.5 Analog input event—single-precision, floating-point without time 587
A.16.6 Analog input event—double-precision, floating-point without time 588
A.16.7 Analog input event—single-precision, floating-point with time 589
A.16.8 Analog input event—double-precision, floating-point with time 591
A.17 Object group 33: frozen analog input events 593
A.17.1 Frozen analog input event—32-bit without time 593
A.17.2 Frozen analog input event—16-bit without time 594
A.17.3 Frozen analog input event—32-bit with time 595
A.17.4 Frozen analog input event—16-bit with time 597
A.17.5 Frozen analog input event—single-precision, floating-point without time 599
A.17.6 Frozen analog input event—double-precision, floating-point without time 600
A.17.7 Frozen analog input event—single-precision, floating-point with time 602
A.17.8 Frozen analog input event—double-precision, floating-point with time 604
A.18 Object group 34: analog input reporting deadbands 606
A.18.1 Analog input reporting deadband—16-bit 606
A.18.2 Analog input reporting deadband—32-bit 607
A.18.3 Analog input reporting deadband—single-precision, floating-point 608
A.19 Object group 40: analog output status 610
A.19.1 Analog output status—32-bit with flag 610
A.19.2 Analog output status—16-bit with flag 611
A.19.3 Analog output status—single-precision, floating-point with flag 612
A.19.4 Analog output status—double-precision, floating-point with flag 613
A.20 Object group 41: analog outputs 615
A.20.1 Analog output—32-bit 615
A.20.2 Analog output—16-bit 616
A.20.3 Analog output—single-precision, floating-point 617
A.20.4 Analog output—double-precision, floating-point 618
A.21 Object group 42: analog output events 620
A.21.1 Analog output event—32-bit without time 620
A.21.2 Analog output event—16-bit without time 622
A.21.3 Analog output event—32-bit with time 623
A.21.4 Analog output event—16-bit with time 625
A.21.5 Analog output event—single-precision, floating-point without time 627
A.21.6 Analog output event—double-precision, floating-point without time 628
A.21.7 Analog output event—single-precision, floating-point with time 630
A.21.8 Analog output event—double-precision, floating-point with time 632
A.22 Object group 43: analog output command events 634
A.22.1 Analog output command event—32-bit without time 634
A.22.2 Analog output command event—16-bit without time 636
A.22.3 Analog output command event—32-bit with time 637
A.22.4 Analog output command event—16-bit with time 639
A.22.5 Analog output command event—single-precision, floating-point without time 641
A.22.6 Analog output command event—double-precision, floating-point without time 642
A.22.7 Analog output command event—single-precision, floating-point with time 644
A.22.8 Analog output command event—double-precision, floating-point with time 646
A.23 Object group 50: time and date 648

Copyright © 2012 IEEE. All rights reserved.

Documents
Document Sharing Hub

Authorized licensed use limited to: Tsinghua University. Downloaded on February 25,2026 at 01:06:46 UTC from IEEE Xplore. Restrictions apply.

Full document details: IEEE 1815-2012

A.23.1 Time and date—absolute time 648
A.23.2 Time and date—absolute time and interval 649
A.23.3 Time and date—absolute time at last recorded time 650
A.23.4 Time and date—indexed absolute time and long interval 651
A.24 Object group 51: time and date common time-of-occurrences 654
A.24.1 Time and date common time-of-occurrence—absolute time, synchronized 654
A.24.2 Time and date common time-of-occurrence—absolute time, unsynchronized 656
A.25 Object group 52: time delays 658
A.25.1 Time delay—coarse 658
A.25.2 Time delay—fine 659
A.26 Object group 60: class objects 660
A.26.1 Class objects—Class 0 data 660
A.26.2 Class objects—Class 1 data 661
A.26.3 Class objects—Class 2 data 662
A.26.4 Class objects—Class 3 data 663
A.27 Object group 70: file-control 664
A.27.1 File-control—file identifier—superseded 664
A.27.2 File-control—authentication 668
A.27.3 File-control—file command 670
A.27.4 File-control—file command status 674
A.27.5 File-control—file transport 677
A.27.6 File-control—file transport status 679
A.27.7 File-control—file descriptor 681
A.27.8 File-control—file specification string 684
A.28 Object group 80: internal indications 686
A.28.1 Internal indications—packed format 686
A.29 Object group 81: device storage 688
A.29.1 Device storage—buffer fill status 688
A.30 Object group 82: Device Profiles 689
A.30.1 Device Profile—functions and indexes 689
A.31 Object group 83: data sets 692
A.31.1 Data set—private registration object 692
A.31.2 Data set—private registration object descriptor 694
A.32 Object group 85: data set prototypes 696
A.32.1 Data set prototype—with UUID 696
A.33 Object group 86: data set descriptors 698
A.33.1 Data set descriptor—data set contents 698
A.33.2 Data set descriptor—characteristics 700
A.33.3 Data set descriptor—point index attributes 701
A.34 Object group 87: data sets 703
A.34.1 Data set—present value 703
A.35 Object group 88: data set events 705
A.35.1 Data set event—snapshot 705
A.36 Object group 90: applications 707
A.36.1 Application—identifier 707
A.37 Object group 91: status of requested operations 708
A.37.1 Status of requested operation—active configuration 708
A.38 Object group 100: floating-point 710
A.38.1 Floating-point—none—general description common to all variations 710
A.39 Object group 101: binary-coded decimal integers 711
A.39.1 Binary-coded decimal integer—small 711
A.39.2 Binary-coded decimal integer—medium 712
A.39.3 Binary-coded decimal integer—large 713
A.40 Object group 102: unsigned integers 714
A.40.1 Unsigned integer—8-bit 714
A.41 Object group 110: octet strings 715
A.41.1 Octet string—none—general description common to all variations 715

Copyright © 2012 IEEE. All rights reserved.

Documents
Document Sharing Hub

Authorized licensed use limited to: Tsinghua University. Downloaded on February 25,2026 at 01:06:46 UTC from IEEE Xplore. Restrictions apply.

Full document details: IEEE 1815-2012

A.42 Object group 111: octet string events 716
A.42.1 Octet string event—none—general description common to all variations 716
A.43 Object group 112: virtual terminal output blocks 717
A.43.1 Virtual terminal output block—none—general description common to all variations 717
A.44 Object group 113: virtual terminal event data 718
A.44.1 Virtual terminal event data—none—general description common to all variations 718
A.45 Object group 120: authentication 719
A.45.1 Authentication—challenge 719
A.45.2 Authentication—reply 722
A.45.3 Authentication—Aggressive Mode request 724
A.45.4 Authentication—session key status request 726
A.45.5 Authentication—session key status 727
A.45.6 Authentication—session key change 730
A.45.7 Authentication—error 733
A.45.8 Authentication—user certificate 736
A.45.9 Authentication—message authentication code (MAC) 741
A.45.10 Authentication—user status change 743
A.45.11 Authentication—update key change request 748
A.45.12 Authentication—update key change reply 750
A.45.13 Authentication—update key change 752
A.45.14 Authentication—update key change signature 754
A.45.15 Authentication—update key change confirmation 756
A.46 Object group 121: security statistics 758
A.46.1 Security statistic—32-bit with flag 758
A.47 Object group 122: security statistic events 760
A.47.1 Security statistic event—32-bit with flag 760
A.47.2 Security statistic event—32-bit with flag and time 762

Annex B (informative) DNP3 quick reference 764

Annex C (informative) Associations 769
C.1 Introduction 769
C.2 Association definition 769
C.3 Association issues 769
C.4 UDP associations 770
C.5 TCP associations 770

Annex D (normative) UTF-8 related copyright 772

Annex E (informative) Sample CRC calculations 773

Annex F (informative) Managing Secure Authentication updates 776
F.1 Introduction 776
F.2 Secure Authentication version updates 777
F.3 Recommendations 777
F.3.1 For outstations 777
F.3.2 For master stations 777
F.3.3 For DNP3 system users 778
F.3.4 Commercial considerations 778

Annex G (informative) Bibliography 779

Copyright © 2012 IEEE. All rights reserved.

Documents
Document Sharing Hub

Authorized licensed use limited to: Tsinghua University. Downloaded on February 25,2026 at 01:06:46 UTC from IEEE Xplore. Restrictions apply.

Full document details: IEEE 1815-2012

Figures

Figure 0-1—DNP3 master–outstation model xviii
Figure 0-2—Fragmented Application Layer message xx
Figure 0-3—Polled sequence with Data Link Layer confirmation xxii
Figure 0-4—Unsolicited response sequence xxiii
Figure 4-1—Layering diagram 13
Figure 4-2—Point type arrays 14
Figure 4-3—Event buffering concepts 19
Figure 4-4—Fragment structure 20
Figure 4-5—Application request header 21
Figure 4-6—Application response header 21
Figure 4-7—Application control octet fields 21
Figure 4-8—Internal indications octets 28
Figure 4-9—Object header fields 30
Figure 4-10—Qualifier octet fields 32
Figure 4-11—Objects prefixed 32
Figure 4-12—Index list 33
Figure 4-13—Example exchange to activate configuration 80
Figure 4-14—Event buffer overflow example 87
Figure 4-15—Unsolicited timing diagram 89
Figure 4-16—Ideal mixed unsolicited and solicited communications 94
Figure 4-17—Unsolicited response or confirmation not received 96
Figure 4-18—Regenerated unsolicited response 97
Figure 4-19—Read request received while awaiting unsolicited confirm 98
Figure 4-20—Non-read request received 99
Figure 5-1—Virtual channels illustrated 110
Figure 5-2—Relationships 123
Figure 5-3—Sample data set with CTLS and CTLV elements 139
Figure 5-4—Example control message exchange 141
Figure 6-1—Outstation fragment state diagram 162
Figure 6-2—Master solicited response reception state diagram 167
Figure 6-3—Master unsolicited response reception state diagram 170
Figure 7-1—Assumed implementation architecture 174
Figure 7-2—Overview of interaction among authority, master, and outstation 179
Figure 7-3—Example of successful challenge of Critical ASDU 180
Figure 7-4—Example of failed challenge of Critical ASDU 180
Figure 7-5—Example of a successful Aggressive Mode Request 181
Figure 7-6—Example of a failed Aggressive Mode Request 181
Figure 7-8—Example of communications failure followed by Session Key Change 183
Figure 7-9—Example of successful User Status Change and Update Key Change 184
Figure 7-10—Major state transitions for master 185
Figure 7-11—Major state transitions for outstation 186
Figure 7-12—Example of DNP3 Select/Operate authentication 193
Figure 7-13—Example of DNP3 Select/Operate authentication in Aggressive Mode 194
Figure 7-14—Example of failed DNP3 Select/Operate authentication 194
Figure 7-15—Example DNP3 initialization sequence 195
Figure 7-16—Example DNP3 authentication of outstation polling data 196
Figure 7-17—Example of failed authentication of outstation data 196
Figure 7-18—Successful User Status Change and Update Key Change 197
Figure 7-19—User changes masters 198
Figure 7-20—Master state machine showing DNP3 function codes and object variations 199
Figure 7-21—Outstation state machine showing DNP3 function codes and object variations 200
Figure 7-22—Master state machine for Update Key Change 201
Figure 7-23—Outstation state machine for Update Key Change 202
Figure 7-24—Behavior model for multiple users 204
Figure 7-25—Possible collision of confirmation challenge and next master request 209

Copyright © 2012 IEEE. All rights reserved.

Documents
Document Sharing Hub

Authorized licensed use limited to: Tsinghua University. Downloaded on February 25,2026 at 01:06:46 UTC from IEEE Xplore. Restrictions apply.

Full document details: IEEE 1815-2012

Figure 7-26—Preventing Confirmation challenge collisions using Aggressive Mode....209
Figure 7-27—Example use of Challenge Sequence Numbers (part 1)....212
Figure 7-28—Example use of Challenge Sequence Numbers (part 2)....213
Figure 7-29—Example of User Number and Association ID assignments....226
Figure 7-30—Valid profiles using the Secure Authentication mechanism....251
Figure 7-31—Example of user number assignments in a data concentrator....253
Figure 8-1—Transport Function location is between Application Layer and Data Link Layer....267
Figure 8-2—Transport segment....267
Figure 8-3—Header fields....268
Figure 8-4—Reception state diagram....273
Figure 9-1—DNP3 protocol stack....274
Figure 9-2—Transaction diagram....276
Figure 9-3—DNP3 frame format....276
Figure 9-4—Control octet bit definitions....277
Figure 9-5—Destination address format....280
Figure 9-6—Source address format....280
Figure 9-7—CRC ordering....281
Figure 10-1—Timing of non-LAN time synchronization....300
Figure 10-2—Timing of LAN time synchronization....302
Figure 11-1—Identification of non-originating devices (data concentrators)....323
Figure 11-2—Analog input model....332
Figure 11-3—Analog output point type model....335
Figure 11-4—Activation model....337
Figure 11-5—Complementary latch model....338
Figure 11-6—Complementary, two-output model....339
Figure 11-7—Counter point type model....341
Figure 11-8—Double-bit binary input model....345
Figure 11-9—Octet string model....346
Figure 11-10—Single-bit binary input point type model....347
Figure 11-11—Virtual terminal conceptual model....348
Figure 11-12—Security statistics model....350
Figure 13-1—Protocol stack....377
Figure 13-2—Single master connection....385
Figure 13-3—Connection based on master IP address....386
Figure 13-4—Connection based on port number....387
Figure 13-5—All connections accepted for browsing static data....388
Figure 13-6—Multiple outstation connections....389
Figure 13-7—Master station statechart for dual end point....391
Figure 13-8—Outstation statechart for dual end point....392
Figure 14-1—Top level of DNP3 Device Profile Schema....432
Figure 14-2—Example of the Schema's first element....432
Figure 14-3—Example of Schema's referenceDevice....433

Copyright © 2012 IEEE. All rights reserved.
Documents
Document Sharing Hub
Authorized licensed use limited to: Tsinghua University. Downloaded on February 25,2026 at 01:06:46 UTC from IEEE Xplore. Restrictions apply.
Full document details: IEEE 1815-2012

Tables

Table 0-1—Comparison of IEC 60870-5 and DNP3 Data Link Layers xiv
Table 0-2—DNP3 layer summary xxi
Table 4-1—Reporting classes table 18
Table 4-2—Function code table 24
Table 4-3—IIN bits 29
Table 4-4—Object prefix codes 32
Table 4-5—Range specifier codes 33
Table 4-6—Valid qualifier codes 34
Table 4-7—Preferred qualifier codes 35
Table 4-8—Qualifier codes used by subset requirements 35
Table 4-9—Action to perform with next request after a select request 50
Table 4-10—Example status codes and IIN bits in control response 54
Table 4-11—Freezing schedule interpretation 57
Table 4-12—Object headers used for re-assigning event classes 63
Table 4-13—Broadcast addresses 82
Table 4-14—Conditions for setting IIN2.1 85
Table 4-15—Conditions for setting IIN2.4 88
Table 4-16—Mandatory function codes and objects for broadcast messages 100
Table 5-1—Static data included in Class 0 data response 105
Table 5-2—Event data included in events class responses 106
Table 5-3—Example of event buffering and reporting order 107
Table 5-4—Electrical fault data set 121
Table 5-5—Pump-valve data set example 121
Table 5-6—Data type codes specific to data sets 128
Table 5-7—Descriptor codes 131
Table 5-8—Data set related group numbers and report classes 136
Table 5-9—Group numbers used for point types 137
Table 5-10—Element types in control requests and responses 138
Table 5-11—CTLS element structure and contents 139
Table 5-12—Data set descriptor for electrical fault 142
Table 5-13—Data set descriptor for electrical fault with prototype 143
Table 5-14—Data set prototype for electrical fault 144
Table 5-15—Electrical fault data set 146
Table 5-16—Attribute data type codes 150
Table 6-1—Outstation fragment state table 157
Table 6-2—Master reception state table, solicited responses 165
Table 6-3—Master reception state table, unsolicited responses 169
Table 7-1—Summary of symmetric keys used 176
Table 7-2—Summary of asymmetric keys used (optional) 177
Table 7-3—DNP3 master messages with correlation to IEC/TS 62351-5[a] 187
Table 7-4—DNP3 outstation messages with correlation to IEC/TS 62351-5[a] 190
Table 7-5—States used in the state machine descriptions 203
Table 7-6—Indexes of security statistics objects 206
Table 7-7—DNP3 Critical Request function codes 210
Table 7-8—Challenger state machine 215
Table 7-9—Use of Error message objects in DNP3 223
Table 7-10—Example of User Number and Association ID assignments 227
Table 7-11—When to use the reserved User Numbers 227
Table 7-12—User roles 228
Table 7-13—Master state machine—Changing Session Keys 231
Table 7-14—Master state machine—Changing Update Keys 235
Table 7-15—Special statistic event thresholds 243
Table 7-16—Algorithms and objects used for each Update Key Change Method 245
Table 7-17—Size of Challenge Data 246
Table 7-18—Configuration of cryptographic information 247

Copyright © 2012 IEEE. All rights reserved.

Documents
Document Sharing Hub

Authorized licensed use limited to: Tsinghua University. Downloaded on February 25,2026 at 01:06:46 UTC from IEEE Xplore. Restrictions apply.

Full document details: IEEE 1815-2012

Table 7-19—Legend for configuration of cryptographic information....248
Table 7-20—Construction of AES-GMAC Initialization Vector....249
Table 7-21—Source of Initialization Vector components in each DNP3 object....249
Table 7-22—Recommended cipher suite combinations....255
Table 7-23—Cryptographic notation....262
Table 7-24—Compliance with ISO/IEC 11770....264
Table 8-1—Transport Function reception state table....272
Table 9-1—Primary-to-secondary (PRM = 1) function codes....279
Table 9-2—Secondary-to-primary (PRM = 0) function codes....279
Table 9-3—Special use addresses....282
Table 9-4—Primary Station variables....285
Table 9-5—Secondary Station variables....285
Table 9-6—Primary Station state table....288
Table 9-7—Secondary Station state table....292
Table 11-1—Primitive data types....307
Table 11-2—BCD character coding....311
Table 11-3—Preferred printable characters....313
Table 11-4—Object data type codes....321
Table 11-5—Flag descriptions....323
Table 11-6—Setting of OVER_RANGE flag examples....327
Table 11-7—Control-related status codes....329
Table 11-8—File-related status codes....330
Table 11-9—Analog input point type object groups....334
Table 11-10—Analog output point type object groups....336
Table 11-11—BCD point type object groups....336
Table 11-12—Binary output point type object groups....340
Table 11-13—Counter point type object groups....342
Table 11-14—Double-bit binary input states....345
Table 11-15—Double-bit binary input point type object groups....346
Table 11-16—Octet string point type object groups....347
Table 11-17—Single-bit binary input point type object groups....348
Table 11-18—Virtual terminal point type object groups....349
Table 11-19—Security statistics versus standard DNP3 counters....349
Table 11-20—Security statistics point type object groups....350
Table 12-1—g0 device attribute objects....352
Table 12-2—g1 binary input static objects....352
Table 12-3—g2 binary input event objects....353
Table 12-4—g3 double-bit binary input static objects....353
Table 12-5—g4 double-bit binary input event objects....353
Table 12-6—g10 binary output static objects....354
Table 12-7—g11 binary output event objects....354
Table 12-8—g12 binary output command objects....354
Table 12-9—g13 binary output command event objects....354
Table 12-10—g20 counter static objects....355
Table 12-11—g21 frozen counter static objects....355
Table 12-12—g22 counter event objects....356
Table 12-13—g23 frozen counter event objects....356
Table 12-14—g30 analog input static objects....356
Table 12-15—g31 frozen analog input static objects....357
Table 12-16—g32 analog input event objects....357
Table 12-17—g33 frozen analog input event objects....357
Table 12-18—g34 analog input deadband objects....358
Table 12-19—g40 analog output status objects....358
Table 12-20—g41 analog output command objects....358
Table 12-21—g42 analog output event objects....359
Table 12-22—g43 analog output command event objects....359
Table 12-23—g50–g52 time information objects....360

Copyright © 2012 IEEE. All rights reserved.

Documents
Document Sharing Hub

Authorized licensed use limited to: Tsinghua University. Downloaded on February 25,2026 at 01:06:46 UTC from IEEE Xplore. Restrictions apply.

Full document details: IEEE 1815-2012

Table 12-24—g60 class information objects 360
Table 12-25—g70 file objects 360
Table 12-26—g80–g83 information objects 361
Table 12-27—g85–g88 data set objects 361
Table 12-28—g90-g91 application & status of operation information objects 361
Table 12-29—g101–g102 numeric static objects 361
Table 12-30—g110–g113 string & virtual terminal static & event objects 362
Table 12-31—g120–g122 security objects 362
Table 12-32—Function codes not used with objects 362
Table 12-33—g0 device attribute objects 364
Table 12-34—g1 binary input static objects 364
Table 12-35—g2 binary input event objects 364
Table 12-36—g3 double-bit binary input static objects 364
Table 12-37—g4 double-bit binary input event objects 365
Table 12-38—g10 binary output static objects 365
Table 12-39—g11 binary output event objects 365
Table 12-40—g12 binary output command objects 365
Table 12-41—g13 binary output command event objects 366
Table 12-42—g20 counter static objects 366
Table 12-43—g21 frozen counter static objects 366
Table 12-44—g22 counter event objects 367
Table 12-45—g23 frozen counter event objects 367
Table 12-46—g30 analog input static objects 367
Table 12-47—g31 frozen analog input static objects 368
Table 12-48—g32 analog input event objects 368
Table 12-49—g33 frozen analog input event objects 369
Table 12-50—g34 analog input deadband objects 369
Table 12-51—g40 analog output status objects 369
Table 12-52—g41 analog output command objects 370
Table 12-53—g42 analog output event objects 370
Table 12-54—g43 analog output command event objects 371
Table 12-55—g50–g52 time information objects 371
Table 12-56—g60 class information 372
Table 12-57—g70 file objects 372
Table 12-58—g80–g83 information objects 372
Table 12-59—g85–g88 data set objects 373
Table 12-60—g90 application & status of operation information objects 373
Table 12-61—g101, g102 numeric static objects 373
Table 12-62—g110–g113 string and virtual terminal static and event objects 374
Table 12-63—g120–g122 security objects 374
Table 12-64—Function codes not used with objects 375
Table 13-1—UDP port requirements 381
Table 13-2—Handling broken TCP connections 383
Table 13-3—Handling closed TCP connections 384
Table 14-1—Qualifiers used in the subset definitions 396
Table 14-2—Level 1 implementation (DNP3-L1) 398
Table 14-3—Level 2 implementation (DNP3-L2) 401
Table 14-4—Level 3 implementation (DNP3-L3) 406
Table 14-5—Level 4 implementation (DNP3-L4) 413
Table A-1—Interoperable control commands 508
Table A-2—Actions performed by outstation for interoperable commands 508
Table A-3—Data included in the MAC Value calculation 723
Table A-4—Data included in the MAC Value calculation 729
Table A-5—Data included in the key wrap (in order) 731
Table A-6—Example of key order 731
Table A-7—Example of wrapped key data 731
Table A-8—DNP3 Secure Authentication parameters in IEC/TS 62351-8 certificates 740

Copyright © 2012 IEEE. All rights reserved.

Documents
Document Sharing Hub

Authorized licensed use limited to: Tsinghua University. Downloaded on February 25,2026 at 01:06:46 UTC from IEEE Xplore. Restrictions apply.

Full document details: IEEE 1815-2012

Table A-9—Data included in the HMAC Value calculation in Aggressive Mode....742
Table A-10—Creation of certification data....743
Table A-11—Encrypted Update Key data....753
Table A-12—Data included in the digital signature....755
Table A-13—Data included in the MAC calculation....757

Copyright © 2012 IEEE. All rights reserved.
Documents
Document Sharing Hub
Authorized licensed use limited to: Tsinghua University. Downloaded on February 25,2026 at 01:06:46 UTC from IEEE Xplore. Restrictions apply.
Full document details: IEEE 1815-2012

Examples

EX 0-1 xxv
EX 4-1 35
EX 4-2 36
EX 4-3 36
EX 4-4 36
EX 4-5 37
EX 4-6 37
EX 4-7 38
EX 4-8 38
EX 4-9 42
EX 4-10 43
EX 4-11 44
EX 4-12 45
EX 4-13 46
EX 4-14 47
EX 4-15 47
EX 4-16 48
EX 4-17 51
EX 4-18 52
EX 4-19 53
EX 4-20 56
EX 4-21 57
EX 4-22 58
EX 4-23 59
EX 4-24 61
EX 4-25 63
EX 4-26 65
EX 4-27 66
EX 4-28 69
EX 4-29 70
EX 4-30 71
EX 4-31 73
EX 4-32 74
EX 4-33 75
EX 4-34 76
EX 5-1 111
EX 5-2 114
EX 5-3 116
EX 5-4 118
EX 5-5 141
EX 5-6 143
EX 5-7 145
EX 5-8 146
EX 5-9 148
EX 5-10 150
EX 5-11 151
EX 5-12 152
EX 8-1 270
EX 9-1 281
EX 11-1 309
EX 11-2 311
EX 11-3 319
EX 11-4 320

Copyright © 2012 IEEE. All rights reserved.

Documents
Document Sharing Hub

Authorized licensed use limited to: Tsinghua University. Downloaded on February 25,2026 at 01:06:46 UTC from IEEE Xplore. Restrictions apply.

Full document details: IEEE 1815-2012

Documents
Document Sharing Hub
Authorized licensed use limited to: Tsinghua University. Downloaded on February 25,2026 at 01:06:46 UTC from IEEE Xplore. Restrictions apply.
Full document details: IEEE 1815-2012

IEEE Standard for Electric Power Systems Communications—Distributed Network Protocol (DNP3)

IMPORTANT NOTICE: IEEE Standards documents are ~~This standard is~~ not intended to ensure safety, ~~security,~~ health, or environmental protection, or ensure against interference with or from other devices or networks. Implementers of IEEE ~~the~~ Standards documents are responsible for determining and complying with all appropriate safety, security, environmental, ~~and~~ health, and interference protection practices ~~or regulatory requirements~~ and all applicable laws and regulations.

This IEEE document is made available for use subject to important notices and legal disclaimers. These notices and disclaimers appear in all publications containing this document and may be found under the heading "Important Notice" or "Important Notices and Disclaimers Concerning IEEE Documents." They can also be obtained on request from IEEE or viewed at http://standards.ieee.~~org~~ ors/IPR/disclaimers.htmL

1 Overview

1.1 Scope

This document specifies the DNP3 protocol structure, functions, and interoperable application ~~alternatives. In addition to defining the structure and operation of DNP3, the standard~~ options (subset levels). The specified subset level defines ~~three application levels that are interoperable.~~the functionality implemented in each device. The simplest ~~application~~level is intended for ~~low-cost distribution feeder~~basic devices~~, and the most complex is for full-featured master stations. The intermediate application level is for substation and other intermediate devices.~~. More advanced levels support increasing functionality. The protocol is suitable for operation on a variety of communication media consistent with the makeup of most electric power communication systems.

Documents
Document Sharing Hub
Authorized licensed use limited to: Tsinghua University. Downloaded on February 25,2026 at 01:06:46 UTC from IEEE Xplore. Restrictions apply.
Full document details: IEEE 1815-2012

~~The standard consists of several clauses each related to an application or function.~~

1.2 Purpose

The purpose of this standard is to document and make available the specifications for the DNP3 protocol. While a primary focus of this protocol is the Electric Utility Industry, other industries that deliver Energy and Water are also using DNP3. The intent of this DNP3 standard is to meet the goal established by the National Institute of Standards and Technology (NIST) for a Smart Grid protocol:

— Provides a protocol standard from a recognized standard institution

— Provides interoperability with hundreds of operational systems and thousands of devices

— Provides cyber security based on IEC/TS 62351-5

— Provides Device data profiles in a format that can be mapped to IEC 61850 Object Models

Vendors may use this standard to implement and test the protocol in their products and be assured of interoperability. Users may use the document to specify the features they wish to apply. System Integrators may use this standard to assist in system integration and testing.

1.3 Octet order

Unless specified elsewhere, the least significant octet in multi-octet data values is transmitted first.

Documents
Document Sharing Hub
Authorized licensed use limited to: Tsinghua University. Downloaded on February 25,2026 at 01:06:46 UTC from IEEE Xplore. Restrictions apply.
Full document details: IEEE 1815-2012

2 Normative references

The following referenced documents are indispensable for the application of this document (i.e., they must be understood and used, so each referenced document is cited in text and its relationship to this document is explained). For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments or corrigenda) applies.

DNP3 Specification Supplement 1—Device Profile Template and XML Schema, DNP Users Group.[1]

FIPS 180-2, Secure Hash Standard (includes SHA-1, SHA-224, SHA-256, SHA-384, and SHA-512).[2]

FIPS 186-2, Digital Signature Standard (DSS), USA NIST, February 2000 including Change Notice #1, October 2001.[3]

FIPS 198, The Keyed-Hash Message Authentication Code (HMAC), March 2002.

IEC 60870-5, Telecontrol equipment and Systems—Part 5: Transmission protocols.[4]

IEC 61850, A New Approach to Substation Automation, Communications, and Integration.[3]

[1] DNP3 Publications are available at http://www.dnp.org/DNP3Downloads.

[2] FIPS publications are available from the National Technical Information Service ~~U. S. Dept. of Commerce, 5285 Port Royal Rd., Springfield, VA 22161~~ (http://w\v\v.ntis.gov/).

[2] Only the random number generation algorithms in the appendix are used.

[4] IEC publications are available from the International Electro technical Commission (http://www.iec.ch/). IEC publications are also available in the United States from the American National Standards Institute (http://www.ansi.org/).

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

Documents
Document Sharing Hub
Authorized licensed use limited to: Tsinghua University. Downloaded on February 25,2026 at 01:06:46 UTC from IEEE Xplore. Restrictions apply.
Full document details: IEEE 1815-2012

IEC/TS 62351-2, Power systems management and associated information exchange—Data and communications security. Part 2: Communication network and system security—Glossary.

IEC/TS 62351-3, Power systems management and associated information exchange—Data and communications security. Part 3: Communication network and system security—Profiles including TCP/IP.

IEC/TS 62351-5, Power systems management and associated information exchange—Data and communications security. Part 5: Communication network and system security—Security for IEC 60870-5 and derivatives.

IEC/TS 62351-8, Power systems management and associated information exchange—Data and communications security. Part 8: Role-based access control. ~~Part 1: Communication network and system security—Introduction to security issues.~~

IEEE Std 754™, IEEE Standard for Floating-Point Arithmetic.[5][6]

IETF RFC 768, User Datagram Protocol[7]

IETF RFC 791, DARPA Internet Program Protocol Specification.

IETF RFC 793, Transmission Control Protocol DARPA Internet Program Protocol Specification.

[5] The IEEE standards or products referred to in this clause are trademarks owned by the Institute of Electrical and Electronics Engineers, Incorporated.

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

[7] IEIF documents (i.e., RFCs) ~~publications~~ are available for download at http:/lw\v\v.rfc-archive.org/. ~~IETF are available from the Internet Engineering Task Force, IETF Secretariat, c/o Association Management Solutions, LLC (AMS), 48377 Fremont Boulevard, Suite 117, Fremont, CA 94538 (http://www.ietf.org).~~

Documents
Document Sharing Hub
Authorized licensed use limited to: Tsinghua University. Downloaded on February 25,2026 at 01:06:46 UTC from IEEE Xplore. Restrictions apply.
Full document details: IEEE 1815-2012

IETF RFC 2104, HMAC: Keyed-Hashing for Message Authentication.

IETF RFC 3174, US Secure Hash Algorithm (SHA-1).

IETF RFC 3280, Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (~~CRL~~ GEL) Profile.

IETF RFC 3394, Advanced Encryption Standard (AES) Key Wrap Algorithm.

IETF RFC 3447 Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1.

IETF RFC 3629, UTF-8, a transformation format of ISO 10646. IETF RFC 5246, The Transport Layer Security (TLS) Protocol.

IETF RFC 5280, Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile.

IETF RFC 5755, An Internet Attribute Certificate Profile for Authorization.

ISO/TEC 9798-4, Information technology—Security techniques—Entity authentication—Part 4: Mechanisms using a cryptographic check function.[8]

ISO/TEC 10646, Information technology—Universal Multiple-Octet Coded Character Set (UCS).

[8] ISO/IEC publications are available from the ISO Central Secretariat (http://www.iso.org~~ch~~/). ~~Case Postale 56, 1 rue de Varembé, CH-1211, Genève 20, Switzerland/ Suisse~~ ISO 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~~ (http://www.ansi.org/). ~~IEC publications are available from the Sales Department of the International Electro-technical Commission, Case Postale 131, 3 rue de Varembé, CH-1211, Genève 20, Switzerland/Suisse (http://www.iec.ch/). IEC publications are also available in the United States from the Sales Department, American National Standards Institute, 11 West 42nd Street, 13th Floor, New York, NY 10036, USA.~~

Documents
Document Sharing Hub
Authorized licensed use limited to: Tsinghua University. Downloaded on February 25,2026 at 01:06:46 UTC from IEEE Xplore. Restrictions apply.
Full document details: IEEE 1815-2012

ISO/IEC 11770-2:2008 Ed. 2, Information Technology—Security techniques—Key management—Part 2: Mechanisms using symmetric techniques.

ISO/IEC 11770-3:2008 Ed. 2, Information Technology—Security techniques—Key management—Part 3: Mechanisms using asymmetric techniques.

ISO/TEC 18033-2:2006, Information technology—Security techniques—Encryption algorithms—Part 2: Asymmetric ciphers. ~~Entity authentication—Part 4: Mechanisms using a cryptographic check function~~

NIST SP 800-108, Recommendation for Key Derivation Using Pseudorandom Functions.[9]

NIST SP 800-38D, Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC.

3 Definitions, acronyms, and abbreviations

3.1 Definitions

For the purposes of this document, the following terms and definitions apply. The *IEEE Standards Dictionary*~~: *Glossary of Terms & Definitions*~~ *Online* should be ~~referenced~~ consulted for terms not defined in this clause.[8][10]

[9] NIST publications are available from the National Institute of Standards and Technology (http://w\vvi.nist.govi).

[10] The IEEE Standards Dictionary Online subscription is available at http"//www.jeee.org/Portal/innovate/products/standard/Standards_dictionary.html.

~~[8] *The IEEE Standards Dictionary: Glossary of Terms & Definitions* is available at http://shop.ieee.org/.~~

Documents
Document Sharing Hub
Authorized licensed use limited to: Tsinghua University. Downloaded on February 25,2026 at 01:06:46 UTC from IEEE Xplore. Restrictions apply.
Full document details: IEEE 1815-2012