NEMA TS*3.1 96 6470247 0509458 596

NEMA STANDARDS PUBLICATION NO. TS 3.1

NATIONAL TRANSPORTATION COMMUNICATIONS FOR ITS PROTOCOL (NTCIP) OVERVIEW

NATIONAL ELECTRICAL MANUFACTURERS ASSOCIATION

Copyright National Electrical Manufacturers Association
Provided by IHS under license with NEMA
No reproduction or networking permitted without license from IHS
Not for Resale

NEMA Standards Publication TS 3.1-1996

NATIONAL TRANSPORTATION COMMUNICATIONS FOR ITS PROTOCOL (NTCIP) OVERVIEW

Published by

National Electrical Manufacturers Association
1300 N. 17th Street
Rosslyn, Virginia 22209

© 1996 National Electrical Manufacturers Association

Copyright National Electrical Manufacturers Association
Provided by IHS under license with NEMA
No reproduction or networking permitted without license from IHS

Not for Resale

CONTENTS

Page

Foreword iii

Section I GENERAL
1.1 SCOPE 1
1.2 REFERENCES 1
1.2.1 Normative References 1
1.2.2 Other References 3
1.3 TERMS 3
1.3.1 Serial Interface Related Terms 5
1.4 ABBREVIATIONS AND ACRONYMS 9

Section 2 NTCIP OVERVIEW
2.1 GENERAL ASPECTS 11
2.2 ITS ENVIRONMENT 12
2.2.1 ITS Communications Topologies 12
2.2.2 ITS Communications 13
2.2.3 Traffic Control Communications 14
2.3 NTCIP APPROACH 14
2.4 NTCIP COMMUNICATIONS FRAMEWORK; THE REFERENCE MODEL FOR OPEN SYSTEMS INTERCONNECTION 15
2.5 PROTOCOL PROFILES 17
2.5.1 Physical Layer (Layer 1) 18
2.5.2 Data Link Layer (Layer 2) 19
2.5.3 Network Layer (Layer 3) 21
2.5.4 Transport Layer (Layer 4) 23
2.5.5 Session, and Presentation Layers 24
2.5.6 Application Layer (Layer 7) 31
2.5.7 Security 31
2.5.8 Conformance and Protocol Implementation Conformance Statement (PICS) 31
2.5.9 Conclusion 32

Copyright National Electrical Manufacturers Association
Provided by IHS under license with NEMA
No reproduction or networking permitted without license from IHS

Not for Resale

Copyright National Electrical Manufacturers Association
Provided by IHS under license with NEMA
No reproduction or networking permitted without license from IHS

Not for Resale

Foreword

This document meets the criteria of NEMA Authorized Engineering Information. User inputs are solicited by canvass on each NEMA standards proposal for Transportation Management and Associated Control Equipment. This procedure provided guidance before industry action. Every comment received is acknowledged and the action taken reported to the submitter. Comments on this publication should be submitted to:

Vice President, Engineering Department
National Electrical Manufacturers Association
1300 North 17th Street
Rosslyn, Virginia 22209

This standards publication was developed by the Transportation Management Systems and Associated Control Devices section of the National Electrical Manufacturers Association. Section approval of the standard does not necessarily imply that all section members voted for its approval or participated in its development. At the time it was approved, the Transportation Management Systems and Associated Control Devices section had the following members.

ADDCO Manufacturing Co.—St. Paul, MN
American Electric Sign—Spokane, WA
Automatic Signal/Eagle Signal Corporation—Austin, TX
BI Tran Systems, Inc.—Sacramento, CA
Cylink Corporation—Sunnyvale, CA
Eberle Design, Inc.—Phoenix, AZ
Econolite Control Products, Inc.—Anaheim, CA
Fiberoptic Display Systems, Inc.—Smithfield, RI
Intersection Development Corp.—Fullerton, CA
ITS Product Group—Ormond Beach, FL
McCain Traffic Supply, Inc.—Vista, CA
P B Farradyne Inc.—Rockville, MD
Peek Traffic - Transyt—Tallahassee, FL
Rockwell Automation—Mayfield Heights, OH
Skyline Products, Inc.—Colorado Springs, CO
3M Traffic Control Systems—St. Paul, MN
Traffic Sensor Corp.—Corona, CA
Vultron, Inc.—Rochester Hills, MI

Introduction

The NTCIP standard consists of a set of documents which define the details required to implement a working NTCIP-based transportation system. This document provides an overview of the concepts and protocols that are detailed in the individual documents.

Motivation

As transportation control equipment becomes more sophisticated, planners, users, and equipment manufacturers are recognizing the need to establish system inter-operability and integration standards. To deploy the national Intelligent Transportation Systems (ITS) program, a communications backbone based on standard communications protocols must be defined.

Historically, there has been no standardized communications protocol used by the various manufacturers of transportation equipment. Within the traffic control industry, local controller units operating on the same physical link, normally have to be from the same manufacturer as the system.

Copyright National Electrical Manufacturers Association
Provided by IHS under license with NEMA
No reproduction or networking permitted without license from IHS
Not for Resale

When systems from different manufacturers are integrated into a central control system, the communications protocol to each system is different and manufacturer specific.

The requirements of large transportation management systems compound the integration problem. These systems must communicate with a large variety of devices including traffic controllers, surveillance cameras, variable message signs, and other centralized systems.

Industry wide standards for system communications are needed for device connectivity and inter-operability and to accommodate future technologies. The requirements of ITS make it clear that the ability to transfer data throughout a transportation system in a standardized fashion is crucial. A standard meeting these requirements must accommodate the present communications infrastructure as well as the undefined needs of the future.

Purpose of this Document

The purpose of this document is to provide an introduction and overview of the National Transportation Communications for ITS Protocol (NTCIP).

The NTCIP is based upon a suite of internationally recognized communications protocols that are divided into several class profiles. The wide ranging subject of communications protocols can be overwhelming to those new to the field. This document narrows the field to the aspects of communications related to the transportation control environment. It introduces the basic concepts of layered communications protocol stacks and shows how these concepts can be utilized to obtain interoperability and manufacturer interchangeability of transportation control equipment.

This document also presents overviews of the specific protocols defined for use within this standard and describes how the protocols are arranged into environment specific profiles tailored to the requirements of several communications topologies. Background information on the various communications topologies commonly used within traffic control and ITS environments is included.

Individual profile documents provide the detailed definition of the data transport aspects of the various profiles. These contain the protocols and procedures needed to establish communications and move data through the network of devices constituting a transportation control system. Other TS 3 documents define common sets of manageable objects that can be used to control, monitor, and manage a transportation control system.

Copyright National Electrical Manufacturers Association
Provided by IHS under license with NEMA
No reproduction or networking permitted without license from IHS
Not for Resale

Section 1
GENERAL

1.1 SCOPE

The scope of this communications standard encompasses device control, data collection data routing and file transfer services utilizing various communication system topologies. To accomplish this, the NTCIP standards define the following:

a. The physical interconnection between ITS components.
b. The protocol and procedures for establishing communications between ITS components.
c. The procedures to define and register common sets of manageable objects related to controlling and managing ITS components.
d. The device control and status variables required by the various transportation related devices to attain device interoperability.

To accommodate the broad scope of this standardization effort, the NTCIP document has been divided into several sub documents. At present, the following documents are defined or proposed:

a. Communications Standards

   1. STMF—Simple Transportation Management Framework (NEMA TS 3.2)
   2. The proposed Class A Communications Profile (NEMA TS 3.x)
   3. Class B Communications Profile (NEMA TS 3.3)
   4. The proposed Class C Communication Profile (NEMA TS 3.x)

b. Device Object Definitions

   1. Global Object Definitions (NEMA TS 3.4)
   2. Actuated Signal Controller Objects (NEMA TS 3.5)
   3. Variable Message Signs Objects (NEMA TS 3.6)
   4. Closed Circuit Television Control Objects (NEMA TS 3.9)
   5. Ramp Meter Controller Objects (NEMA TS 3.10)
   6. Road/Weather Station Objects (NEMA TS 3.11)
   7. Highway Advisory Radio Objects (NEMA TS 3.12)
   8. Loop Detector Objects (NEMA TS 3.13)
   9. Priority Device Objects (NEMA TS 3.14)

1.2 REFERENCES

1.2.1 Normative References

The following standards contain provisions which, through reference in other documents, are part of the NTCIP. This is not a complete list of all references described by NTCIP, but include those references discussed in this document that are normative to other NTCIP documents. At the time of publication, the editions indicated were valid. All standards are subject to revision, and parties to agreements based on this Standard are encouraged to investigate the possibility of applying the most recent editions of the standards listed below. Contact information regarding the referenced standards is provided.

Copyright National Electrical Manufacturers Association
Provided by IHS under license with NEMA
No reproduction or networking permitted without license from IHS
Not for Resale

ANSI
11 West 42nd Street, 13th Floor
New York, New York 10036

ISO/IEC 3309:1994, *Information technology—Telecommunications and information exchange between systems—High-level Data Link Control (HDLC) procedures—Frame structure*

ISO/IEC 4335:1994, *Information technology—Telecommunications and information exchange between systems—High-level Data Link Control (HDLC) procedures—Elements of procedures*

ISO/IEC 7498-1:1994, *Information technology—Open Systems Interconnection—Basic reference model: The basic model*

ISO/IEC 7498-4:1994, *Information technology—Open Systems Interconnection—Basic reference model—Part 4: Management framework*

ISO/IEC 7809:1994, *Information technology—Telecommunications and information exchange between systems—High-level Data Link Control (HDLC) procedures—Classes of procedures*

ISO/IEC 8824-1:1995, *Information Technology—Abstract Syntax Notation One (ASN.1): Specification of Basic Notation*

ISO/IEC 8824-2:1995, *Information Technology—Abstract Syntax Notation One (ASN.1): Information Object Specification*

ISO/IEC 8824-3:1995, *Information Technology—Abstract Syntax Notation One (ASN.1): Constraint Specification*

ISO/IEC 8824-4:1995, *Information Technology—Abstract Syntax Notation One (ASN.1): Parametrization of ASN.1 Specifications*

ISO/IEC 8825-1:1995, *Information Technology—Open Systems Interconnection—Specification of Basic Encoding Rules for Abstract Syntax Notation One (BER)*

ISO/IEC 8886:1992, *Information Technology—Telecommunications and information exchange between systems—Data link service definition for Open Systems Interconnection*

ISO/IEC 9577:1993, *Information Technology—Telecommunications and information exchange between systems—Protocol identification in the network layer*

ISO/IEC 10028:1993, *Information Technology—Telecommunications and information exchange between systems—Definition of the relaying functions of a network layer intermediate system*

ISO/IEC 11575, *Information Technology—Telecommunications and information exchange between systems—Protocol mapping for the OSI Data Link service*

DDN Network Information Center
14200 Park Meadow Drive
Suite 200
Chantilly, VA 22021

RFC 1155, *Structure and Identification of Management Information for TCP/IP-based Internets.* K. McCloghrie; M. Rose; 05/10/1990

Copyright National Electrical Manufacturers Association
Provided by IHS under license with NEMA
No reproduction or networking permitted without license from IHS
Not for Resale

RFC 1157, *A Simple Network Management Protocol (SNMP).* M. Schoffstall; M. Feder; J. Davin; J. Case; 05/10/1990

RFC 1212, *Concise MIB Definitions,* K. McCloghrie; M. Rose; 03/26/1991

RFC 1213, *Management Information Base for Network Management of TCP/IP-based Internets: MIB-II.* K. McCloghrie; M. Rose; TCP/IP-base

RFC 1317, *Definitions of Managed Objects for RS-232-like Hardware Devices,* B. Stewart, 04/16/1992

Electronic Industries Association
Engineering Department
2500 Wilson Blvd.
Arlington, VA 22201-3834

EIA /TIA-232-E-1991, *Interface Between Data Terminal Equipment and Data Communications Equipment Employing Serial Binary Data Interchange*

Motorola / Universal Data Systems
5000 Bradford Drive
Huntsville, Alabama 35805

Bell 202T, *Data Sets 202S and 202T Interface Specification,* American Telephone and Telegraph, 1978

International Telecommunications Union
Place des Nations
CH-1211
Geneva 20
Switzerland

CCITT Recommendation X.213 (1992) ISO/IEC 8348:1992, *Information technology—Network service definition for Open Systems Interconnection*

CCITT Recommendation X.212 (1988), *Data Link service definition for Open Systems Interconnection for CCITT applications*

ITU-T Recommendation X.210 ISO/IEC 10731, *Information technology—Open Systems Interconnection—Conventions for the definition of OSI services*

1.2.2 Other References

The following list of documents may also be applicable to NTCIP or referenced by the documents in 1.2. These documents are not normative to NTCIP documents.

ANSI
11 West 42nd Street, 13th Floor
New York, New York 10036

ISO/IEC 2382-9: 1995, *Data Processing—Vocabulary—Part 09: Data Communication*

ISO/IEC 7478: 1987, *Information processing systems—Data communication—Multilink procedures*

ISO/IEC 8072: 1994, *Information processing systems—Open Systems Interconnection—Transport Service Definition*

Copyright National Electrical Manufacturers Association
Provided by IHS under license with NEMA
No reproduction or networking permitted without license from IHS
Not for Resale

ISO/IEC 8348: 1993, *Information Technology—Open Systems Interconnection—Network service definition*

ISO/IEC 8348/Add. 3: 1988, *Information processing systems—Data Communications—Network service definition - Addendum 3: Additional features of the network service*

ISO/IEC 8471: 1987, *Information processing systems—Data communication—High-level data link control balanced classes of procedures—Data link layer address resolution/negotiation in switched environments*

ISO/IEC 8880-2: 1992, *Information Technology—Data Communications—Protocol combinations to provide and support the OSI network service—Part 2: Provision and support of the connection-mode network service*

ISO/IEC 8885: 1991 (E), *Information technology—Telecommunications and information exchange between systems—High-level data link control (HDLC) procedures—General purpose XID frame information field content and format*

DDN Network Information Center
14200 Park Meadow Drive
Suite 200
Chantilly, VA 22021

RFC 1214, *OSI Internet Management: Management Information Base,* L. Labarre, 04/05/1991

RFC 1229, *Extensions to the Generic-Interface MIB*, K. McCloghrie, 08/03/1992 (Historic)

RFC 1238, *CLNS MIB—for use with Connectionless Network Protocol (ISO 8473) and End System to Intermediate System (ISO 9542),* G. Satz, 06/25/1991 (Experimental)

RFC 1304, *Definitions of Managed Objects for the SIP Interface Type*, T. Cox, K. Tesink, 02/28/1992

RFC 1316, *Definitions of Managed Objects for Character Stream Devices*, B. Stewart, 04/16/1992

RFC 1354, *IP Forwarding Table MIB*, F. Baker, 07/06/1992

RFC 1414, *Indent MIB*, M. St. Johns, M. Rose, 02/04/1993

RFC 1441, *Introduction to version 2 of the Internet-standard Network Management Framework*, J. Case, K. McCloghrie, M. Rose, S. Waldbusser, 05/03/1993

RFC 1442, *Structure of Management Information for version 2 of the Simple Network Management Protocol (SNMPv2),* J. Case, K. McCloghrie, M. Rose, S. Waldbusser, 05/03/1993

RFC 1443, *Textual Conventions for version 2 of the Simple Network Management Protocol (SNMPv2),* J. Case, K. McCloghrie, M. Rose, S. Waldbusser, 05/03/1993

RFC 1444, *Conformance Statements for version 2 of the Simple Network Management Protocol (SNMPv2),* J. Case, K. McCloghrie, M. Rose, S. Waldbusser, 05/03/1993

RFC 1445, *Administrative Model for version 2 of the Simple Network Management Protocol (SNMPv2),* J. Davin, K. McCloghrie, 05/03/1993

RFC 1446, *Security Protocols for version 2 of the Simple Network Management Protocol (SNMPv2),* J. Galvin, K. McCloghrie, 05/03/1993

RFC 1447, *Party MIB for version 2 of the Simple Network Management Protocol (SNMPv2),* K. McCloghrie, J. Galvin, 05/03/1993

Copyright National Electrical Manufacturers Association
Provided by IHS under license with NEMA
No reproduction or networking permitted without license from IHS
Not for Resale

RFC 1448, *Protocol Operations for version 2 of the Simple Network Management Protocol (SNMPv2),* J. Case, K. McCloghrie, M. Rose, S. Waldbusser, 05/03/1993

RFC 1449, *Transport Mappings for version 2 of the Simple Network Management Protocol (SNMPv2),* J. Case, K. McCloghrie, M. Rose, S. Waldbusser, 05/03/1993

RFC 1450, *Management Information Base for version 2 of the Simple Network Management Protocol (SNMPv2),* J. Case, K. McCloghrie, M. Rose, S. Waldbusser, 05/03/1993

RFC 1471, *The Definitions of Managed Objects for the Link Control Protocol of the Point-to-Point Protocol,* F. Kastenholz, 06/08/1993

RFC 1472, *The Definitions of Managed Objects for the Security Protocols of the Point-to-Point Protocol,* F. Kastenholz, 06/08/1993

RFC 1565, *Network Services Monitoring MIB,* N. Freed, S. Killie, 01/11/1994

RFC 1573, *Evolution of the Interfaces Group of MIB-II,* K. McCloghrie, F. Kastenholz, 01/20/1994

Electronic Industries Association
Engineering Department
2500 Wilson Blvd.
Arlington, VA 22201-3834

EIA /TIA-530, *High Speed, 25 Position Interface for Data Terminal Equipment and Data Circuit Terminating Equipment*

1.3 TERMS

Application Services: the services collectively offered by the upper four layers of the OSI model.

Applications Programmer Interface (API): a set of calling conventions defining how a service is invoked through a software package.

Authentication: the process whereby a message is associated with a particular originating entity.

Authorization: the process whereby an access policy determines whether an entity is allowed to perform an operation.

Basic Encoding Rules (BER): the OSI language for describing transfer syntax.

Broadcast Address: an address referring to all stations on a medium.

Checksum: an arithmetic sum used to verify data integrity.

Data: information before it is interpreted.

Data Link Layer: that portion of an OSI system responsible for transmission, framing, and error control over a single communications link.

Datagram: a self-contained unit of data transmitted independently of other datagrams.

End-to-End Services: the services collectively offered by the lower three layers of the OSI model.

Gateway: a router; also, (imprecise usage) an entity responsible for complex topology mappings.

Copyright National Electrical Manufacturers Association
Provided by IHS under license with NEMA
No reproduction or networking permitted without license from IHS
Not for Resale

Hardware Address: see **media address.**

Host: (Internet usage) an end-system.

Indirect Routing: the process of sending a network message to a router for forwarding.

Intelligent Transportation Systems (ITS): major national initiative to improve information, communication and control technologies in order to improve the efficiency of surface transportation.

Intelligent Vehicle Highway System (IVHS): Obsolete term. See **Intelligent Transportation Systems.**

Intermediate System: a network device performing functions from the lower three layers of the OSI model. Intermediate systems are commonly thought of as routing data for end-systems.

International Organization for Standardization (ISO): An international standards organization. ANSI is the primary interface to ISO within the US. Often thought to be International Standards Organization because of the usage ISO for short.

International Telephone and Telegraph Consultative Committee (CCITT): a body comprising the national Postal, Telephone, and Telegraph (PTT) administrations.

Internet: a large collection of connected networks, primarily in the United States, running the Internet suite of protocols. Sometimes referred to as the *DARPA Internet, NSF/DARPA, Internet,* or the *Federal Research Internet.*

Internet Layer: the layer in the Internet suite of protocols responsible for providing transparency over both the topology of the internet and the transmission media used in each physical network.

Internet Protocol (IP): the network protocol offering a connection-less mode network service in the Internet suite of protocols.

Internet suite of protocols: a collection of computer-communication protocols original developed under DARPA sponsorship.

IP address: a 32-bit quantity used to represent a point of attachment in an internet.

Local Area Network (LAN): any one of a number of technologies providing high speed, low-latency data transfer and being limited in geographic size.

Management Information Base (MIB): a collection of objects that can be accessed via a network management protocol. See **Structure of Management Information.**

Maximum Transmission Unit: the largest amount of user-data that can be sent in a single frame on a particular medium.

Media Address: the address of a physical interface.

National Institute of Standards and Technology (NIST): the branch of the U.S. Department of Commerce charged with keeping track of standardization. Previously known as the National Bureau of Standards.

Network: a collection of subnetworks connected by intermediate-systems and populated by end-systems.

Copyright National Electrical Manufacturers Association
Provided by IHS under license with NEMA
No reproduction or networking permitted without license from IHS
Not for Resale

Network Layer: that portion of an OSI system responsible for data transfer across the network, independent of both the media comprising the underlying subnetworks and the topology of those subnetworks.

Network Management: the technology used to manage in a network. Usually referring to the management of networking specific devices such as routers. In the context of this document, refers to all devices including end systems that are present on the network or inter-network.

Network Identifier: that portion of an IP address corresponding to a network in an internet.

Open Systems Interconnection (OSI): an international effort to facilitate communications among computers of different manufacture and technology.

Physical Layer: that portion of an OSI system responsible for the electro-mechanical interface to the communications media.

Port Number: identifies an application-entity to a transport service in the Internet suite of protocols. The concept of ports are often present in OSI literature, however, ports are not internetwork standard, but exists as local network conventions only.

Presentation Layer: that portion of an OSI system responsible for adding structure to the units of data that are exchanged.

Protocol Control Information: (conceptually) the initial part of a protocol data unit used by a protocol machine to communicate information to a peer.

Protocol Data Unit (PDU): a data object exchanged by protocol machines, usually containing both protocol control information and user-data.

Prototype: (management usage) the object type corresponding to an instance.

Retransmission: the process of repeatedly sending a unit of data while waiting for an acknowledgment.

Router: a level-3 (network layer) relay.

Service primitive: an artifact modeling how a service is requested or accepted by a user.

Session layer: that portion of an OSI system responsible for adding control mechanisms to the data exchange.

Socket: a pairing of an IP address and a port number.

Subnet: a physical network within a network.

System management: the OSI equivalent of network management.

Transmission Control Protocol (TCP): the transport protocol offering a connection-oriented transport service in the Internet suite of protocols.

Transport layer: that portion of an OSI system responsible for reliability and multiplexing of data transfer across the network (over and above that provided by the network layer) to the level required by the application.

Transport-stack: the combination of protocols, at the transport layer and below, used in a given context.

Copyright National Electrical Manufacturers Association
Provided by IHS under license with NEMA
No reproduction or networking permitted without license from IHS
Not for Resale

Transportation management: Short for the management of networks of transportation devices and the network itself.

Transportation network: A network of transportation devices. Usually in the context of transportation management.

Upper-layer protocol number: identifies a transport entity to the IP.

User Datagram Protocol (UDP): the transport protocol offering a connection-less mode transport service in the Internet suite of protocols.

User data: conceptually, the part of a protocol data unit used to transparently communicate information between the users of the protocol. Prefixed by the protocol control information.

Wide Area Network (WAN): any one of a number of technologies providing geographically distant transfer.

1.3.1 Serial Interface Related Terms

These terms define the nomenclature frequently used in regard to the RS-232 interfaces and modems.

ASCII: American Standard Code for Information Interchange. A 7-bit binary code representation of letters, numbers and special characters. It is universally supported in computer data transfer.

Asynchronous: Data transmission in which the actual data is preceded by a start bit and followed by a stop bit since the time between transmitted characters varies.

Baud Rate: The number of discrete signal events per second occurring on a communications channel. It is often referred to as bits per second (BPS) which is technically inaccurate but widely accepted.

Bit: Binary Digit. A single basic computer signal consisting of a value of 0 or 1, off or on.

Byte: A group of bits acted upon as a group, which may have a readable ASCII value as a letter or number or some other coded meaning to the computer. It is commonly used to refer to 8-bit groups.

Carrier: A continuous frequency capable of being either modulated or impressed with another information-carrying signal. Carriers are generated and maintained by modems via the transmission lines.

CRC: Cyclical Redundancy Check. An error-detection technique consisting of a cyclic algorithm performed on each "block" of data at the sending and receiving end of the transmission. As each block is received, the CRC value is checked against the CRC value sent along with the block.

DTE: Data Terminal Equipment. The device that is the originator or destination of the data sent by a modem.

DCE: Data Circuit Terminating Equipment. The device that translates RS 232 to the correct electrical and physical interface for transmission to or reception from distant communicating device. Typically the DCE is a modem.

DTR: Data Terminal Ready. A signal generated by most modems indicating a connection between the DTE (computer) and the modem. When DTR is "high" the computer is connected.

Data Transmission Protocols: These are standards for modulation and transmission of data at various speeds. The standards are Bell 103 & V.21 for 300 bps, Bell 202T, Bell 212A, and V.22 for 1200 bps, V.22

Copyright National Electrical Manufacturers Association
Provided by IHS under license with NEMA
No reproduction or networking permitted without license from IHS
Not for Resale

bis for 2400 bps, V.32 for 9600 bps and V.32 bis for 14,400 bps. Proprietary protocols are also used extensively for higher baud rates.

Echo: The display of transmitted data on a local display. See also **full duplex** and **half duplex** below.

Flow Control: A mechanism that compensates for differences in the flow of data to and output from a modem or computer. Either hardware or software can be used for this control to prevent data loss. Hardware flow control using the modem makes use of a buffer to store data to be sent and data received. Flow control is necessary if the communications port is locked at a higher rate than the connection rate.

Full Duplex: Signal flow in both directions at the same time. It is sometimes used to refer to the suppression of on-line LOCAL ECHO and allowing the remote system to provide a REMOTE ECHO.

Half Duplex: Signal flow in both directions, but only one way at a time. It is sometimes used to refer to activation of LOCAL ECHO which causes a copy of sent data to be displayed on the sending display.

Parity: An error detection method used in both communications and computer memory checking to determine character validity. Communications now makes use of more efficient cyclic redundancy checking algorithms.

Protocol: A system of rules and procedures governing communications between two devices. File transfer protocols in your communications program refer to a set of rules governing how error checking will be performed on blocks of data.

1.4 ABBREVIATIONS AND ACRONYMS

ANSI—American National Standards Institute
ASN.1—Abstract Syntax Notation One
ASYNC—Asynchronous
ATMS—Advanced Traffic Management System
BER—Basic Encoding Rules or Bit Error Rate
bps—Bits per second
CCITT—International Telegraph and Telephone Consultative Committee
CLNS—Connectionless-mode Network Service
CONS—Connection Oriented Network Service
CRC—Cyclic Redundancy Check
DARPA—Defense Advanced Research Projects Agency
DCE—Data Circuit Terminating Equipment
DLSAP—Data Link Service Access Point
DLSDU—Data Link Service Data Unit
DTE—Data Terminal Equipment
EIA—Electronic Industries Association
FCS—Frame Check Sequence
FDDI—Fiber Distributed Data Interface
FHWA—Federal Highway Administration
FSK—Frequency Shift Keying
FTP—File Transfer Protocol
HDLC—High-level Data Link Control
IANA—Internet Assigned Numbers Authority
IEC—International Electrotechnical Commission
IETF—Internet Engineering Task Force
IP—Internet Protocol
IPI—Initial Protocol Identifier
ISO—International Organization for Standardization
ITS—Intelligent Transportation Systems
ITU-T—International Telecommunications Union, Telecommunications Sector

Copyright National Electrical Manufacturers Association
Provided by IHS under license with NEMA
No reproduction or networking permitted without license from IHS
Not for Resale

IVHS—Intelligent Vehicle Highway System
LAN—Local Area Network
LLC—Logical Link Control
MIB—Management Information Base
MMU—Malfunction Management Unit
NEMA—National Electrical Manufacturers Association
NSDU—Network Service Data Unit
OSI—Open Systems Interconnection
PDU—Protocol Data Unit
PER—Packed Encoding Rules
PICS—Protocol Implementation Conformance Statement
RA—Registration Authority
RFC—Request for Comment
RM-0S—Reference Model OSI
SAP—Service Access Point
SDLC—Synchronous Data Link Control
SDU—Service Data Unit
SNMP—Simple Network Management Protocol
STMP—Simple Transportation Management Protocol
STMF—Simple Transportation Management Framework
STMI—Structure and Identification of Transportation Management Information
TIA—Telecommunications Industries Association
TCP—Transmission Control Protocol
TMC—Traffic Management Center
TMIB—Transportation MIB
UCC—Unbalanced Connectionless Class
UDP—User Datagram Protocol
UI—Unnumbered Information (Frame)
VMS—Variable Message Sign

Copyright National Electrical Manufacturers Association
Provided by IHS under license with NEMA
No reproduction or networking permitted without license from IHS
Not for Resale

Section 2
NTCIP OVERVIEW

2.1 GENERAL ASPECTS

The NTCIP standards development program began with the NEMA traffic control equipment manufacturers recognition of the need to extend the TS 2 Standard to cover traffic control hardware interchangeability and communications standards. As the development effort proceeded, the FHWA sponsored a Signal Manufacturers Symposium in May of 1993. The participants, who represented manufacturers and users, suggested that the NEMA Committee broaden the scope of their work to define a truly "open" system including not just NEMA and Type-170 controllers but other control related equipment as well. They also asked the NEMA Committee to consider how the protocol would tie into transportation information networks and different communications architectures. NEMA sought input from interested parties including members of the user community, consultants, and equipment suppliers. With this input, a decision was made to extend the NEMA protocol standard into a national, industry wide "open" protocol standard.

The NTCIP meets existing traffic control functional requirements, supports traffic management communications, and lends itself to other, as yet undefined, application requirements of ITS. For a protocol to be considered "open," the communications aspects of the protocol must be distinctly separate from the application. Since few of the existing traffic control protocols meet these criteria, communications industry standards have been used as a model. NTCIP embraces the features of several existing worldwide communications standards. These standards conform to the ISO Open Systems Interconnect Reference Model (ISO-OSI Model) which deals with how information is passed in open systems. These standards provide the mechanisms to transport information between traffic-control and/or ITS devices. For example, they allow information to be passed from an arterial master to any one of several traffic controllers, from different manufacturers, all residing on the same physical link or from a central computer through several intermediate devices to an ITS control/monitoring device.

The NTCIP does not preclude the possibility of upgrading existing hardware to the standard. A significant, productive, installed base of signal systems is currently deployed and an effective evolution path for these systems is addressed in the NTCIP. Specifically, a class of operation is defined that may be implemented in current state-of-the-art hardware. As explained further on, the NTCIP Class B Profile supports this downward compatibility. With its simplified protocol and functionality, it reduces communications overhead to a level compatible with the capabilities of current hardware. The functional complexity and therefore code size is on par with existing protocols. A device supporting the Class B Profile is able to coexist in a system that implements other compatible class profiles.

An integrated system of transportation devices must allow its components to be managed in a heterogeneous fashion. Device information must be interpreted in a manufacturer-independent manner. The information must be accessible via well defined interfaces and protocols. The NTCIP includes a formal definition of how information is classified, constructed, and supported based on the Internet-Standard Network Management Framework. These procedures, entitled the Simple Transportation Management Framework (STMF) are the interface between the device communications and the transportation applications.

Copyright National Electrical Manufacturers Association
Provided by IHS under license with NEMA
No reproduction or networking permitted without license from IHS

Not for Resale

2.2 ITS ENVIRONMENT

2.2.1 ITS Communications Topologies

The NTCIP addresses the needs of both current and future communications topologies or architectures. Currently there are two topologies that are widely used, centralized and distributed.

In a centralized system (Figure 2-1), a central computer communicates directly with each device under its control. However, all of the devices in the system may not be on the same communications channel or physical layer. The number of devices on a channel is variable. In some applications, a separate communications channel is routed to each device.

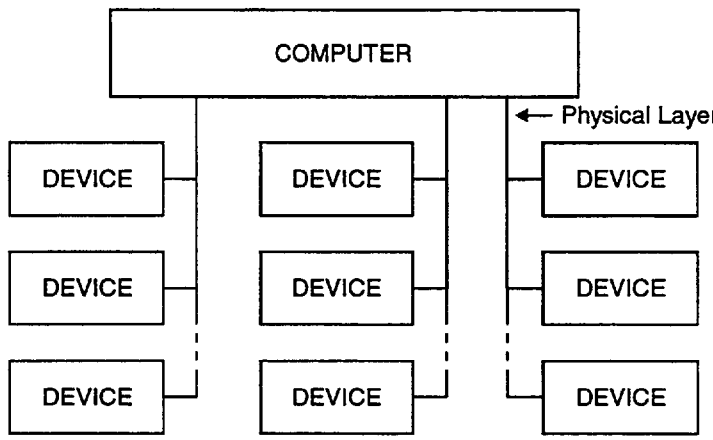


Figure 2-1
CENTRALIZED SYSTEM

The communications structure at the central computer must have some type of routing mechanism that sends messages to a given device over the appropriate physical channel. Centralized systems may access devices as often a once per second and therefore require a permanent connection on the physical layer between the central computer and controllers.

In distributed or multi-level system (Figure 2-2) another level of control may reside in what is called a link controller or arterial master. Distributed systems delegate real time control to the link controller so that permanent links between the central computer and remote devices are not necessary.

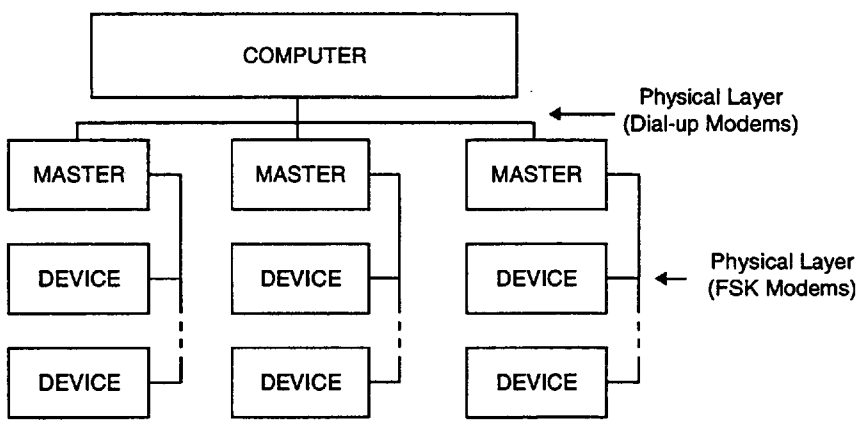


Figure 2-2
DISTRIBUTED SYSTEM

Copyright National Electrical Manufacturers Association
Provided by IHS under license with NEMA
No reproduction or networking permitted without license from IHS
Not for Resale

When communications with the central computer is required, the link controller or arterial master establishes a connection to it via a dial-up telephone circuit or leased line. To meet the requirements of this topology, the protocol must present a standard means of transferring information from the central computer, through a master, to a controller.

ITS systems may require more complex topologies to handle the communications needs of central management and control centers. Figure 2-3 presents a possible multi-jurisdictional management system topology.

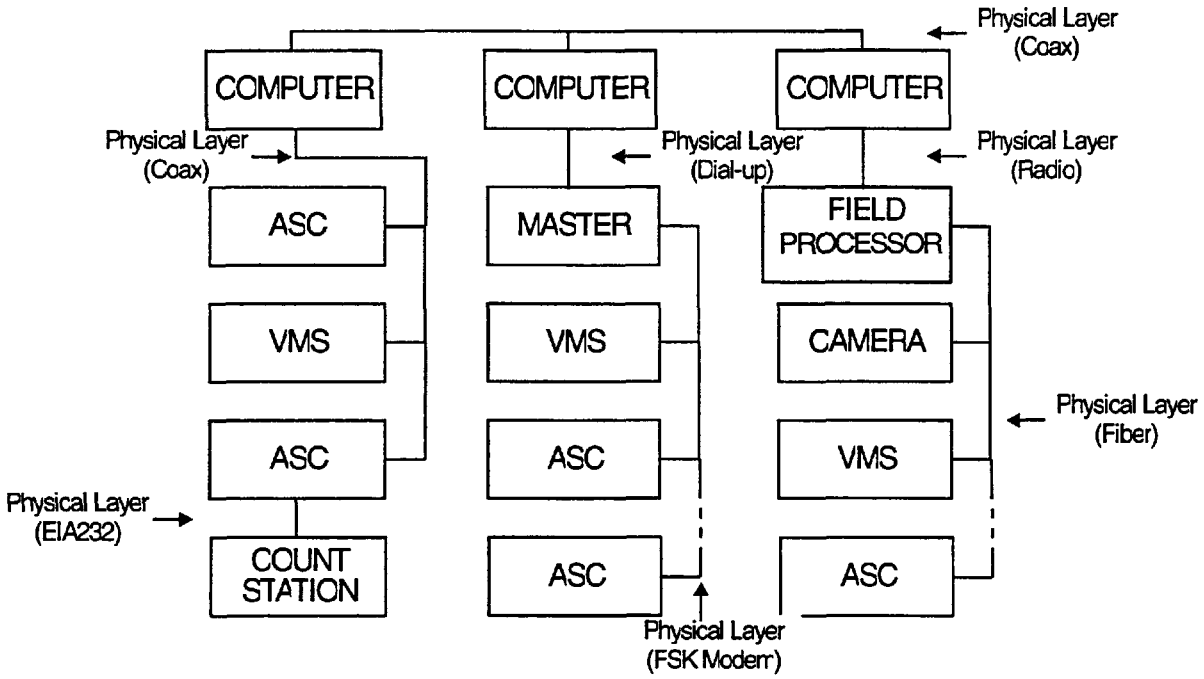


Figure 2-3
MULTI-JURISDICTIONAL SYSTEM

2.2.2 ITS Communications

One of the points raised early in discussions about ITS was the need to establish communications standards. "Key elements of the United States highway system must be equipped with the appropriate technology to facilitate system management as well as communications between highway and vehicle systems. Early deployment of U.S. standards for communications and other systems will be necessary to ensure compatibility among systems in various states and metropolitan areas."[1]

The backbone of ITS is the Advanced Traffic Management System (ATMS). A key element of ATMS is an extensive communication network that will carry data and control information. The NTCIP anticipates the communications needs of ITS in applications such as:

a. Motorist guidance via variable message signs.
b. Real-time adjustment of traffic control systems.
c. Real-time reporting of traffic incidents and control of incident response functions such as rerouting traffic, dispatching tow trucks and reporting alternate routes to drivers about to begin their trips.
d. Delivering information on the new/current location of commercial and transit vehicles.
e. Measuring and reporting trip times for each monitored roadway segment.
f. Exchanging information between regional systems.

[1] U.S. Department of Transportation, Intelligent Vehicle/Highway System Discussion Paper, May 1989.

Copyright National Electrical Manufacturers Association
Provided by IHS under license with NEMA
No reproduction or networking permitted without license from IHS
Not for Resale

These applications and systems are currently in the process of being defined through multiple research and demonstration projects. Although their precise definitions are not yet known, it is clear that extensive communication among widely separated locations and widely varied hardware is required. This communication network may ultimately be required to support the transmission of virtually all ITS communications. For reliability, control intelligence will be distributed, and redundant communication links will be used for critical communication paths. The network may include segments of switched communication networks used by the general public as well as communication links dedicated to ITS use.

2.2.3 Traffic Control Communications

Different control algorithms place varied requirements on the communication channels in a traffic control system. There are three general types of control: second-by-second, cycle-by-cycle, and off-line control. Peer-to-peer control algorithms are being developed.

Many centralized systems exercise control on a second-by-second basis. In this scheme, a central computer is used to control the timing of the signal lights and the sequence in which they occur. Every second, the computer tells each controller to either stay where it is or advance to another phase.

Some central systems and most distributed systems employ a control algorithm that uses a periodic approach. In this scheme, the central or master sends a timing pattern selection to each controller. A sync reference establishes the offset relationship between controllers. In this control method, commands are not transmitted unless a pattern change is necessary. Commands are transmitted on a periodic basis. This type of control makes more efficient use of the communication channel bandwidth. When not selecting a new pattern, intersection status reports, controller timing and other parameters can be either uploaded or downloaded.

Some probable future requirements are:

a. Network configurations other than PC-master-controller (e.g., multiple arterial masters connected simultaneously to a single host, etc.).
b. Transfer of data between ITS field processors.
c. Transfer of setup information to/from secondary devices in the controller cabinet (e.g., to/from detector amps).
d. Uploading of collected data from devices connected to the TS 2 Port 1 channel (e.g., a stand-alone vehicle classifier).
e. Uploading of application specific event data from the TS 2 Malfunction Management Unit (MMU).
f. Peer-to-peer message transfers where any device can communicate with any other device.

2.3 NTCIP APPROACH

The NTCIP is a modular, extensible protocol. Thus, it can support both legacy second-by-second, multi-drop, low speed modem signal systems and modern Internet Protocol based communications architectures. This modularity is achieved by adhering to the International Standards Organization (ISO) Open Systems Interconnect (OSI) 7-layer reference model. By following the ISO-OSI model in defining the NTCIP protocol "stack" (i.e., the layers), modularity is achieved. This permits NTCIP to be compatible with both the current installed signal system infrastructure and advanced applications and technology.

The NTCIP uses this modular approach to define several protocol stack and conformance level "profiles." Each profile is tailored to support the requirements of a particular type of communications link. For example, to support the Class B profile, only layers 1, 2 and 7 protocols are required. Full support for an advanced ITS system may require layers 1, 2, 3, 4 and full support of several layer 7 protocols. The protocols that reside within each layer are described next.

Copyright National Electrical Manufacturers Association
Provided by IHS under license with NEMA
No reproduction or networking permitted without license from IHS
Not for Resale

To address the aforementioned goals and topologies, the NTCIP uses an industry standard, generalized communications approach. This approach starts with a general model for communications and then adds specific protocols to provide the basis of information transfer. The International Standards Organization (ISO) Open Systems Interconnect (OSI) Reference Model defines a stack of seven layers and associated protocols and interfaces. The seven layers are:

a. Layer 7 Application (Highest)
b. Layer 6 Presentation
c. Layer 5 Session
d. Layer 4 Transport
e. Layer 3 Network
f. Layer 2 Data Link
g. Layer 1 Physical (Lowest)

System stack profiles may include protocols for each of the seven layers or, where appropriate, one or more layers can be combined. By following the model in defining the NTCIP protocol stack layers, modularity is achieved. The various protocols adopted by the NTCIP meet the need for reliable communications. The NTCIP supports the following requirements of ITS:

a. Connectionless services. (Connection-oriented service support is under development.)
b. A mechanism for acknowledged and unacknowledged data transfers.
c. An error detection algorithm that ensures the probability of accepting a bad frame is exceedingly small.
d. A structured approach that supports transmission media and data rate independence.
e. An addressing scheme that is extensible to cover existing and future requirements.
f. Support of a message structure that is extensible to account for variability, changeable data content, and varying length structures.

With a connection oriented service, Network Layer communications are setup by establishing a path of communication between two end devices that can pass through any number of intervening devices. This path is then maintained and used for all subsequent communications between the two ends. The connection is broken only when both parties terminate the path. The telephone network is an illustration of this approach.

In a connectionless service, packets of data stand on their own because sequences of packets can travel over different routes and arrivals times are not guaranteed. A good analogy is how an airline handles passengers and their luggage. The passenger may travel on a flight from New York to Los Angeles with a stop in Chicago, but the luggage may go on a different flight with a different stop. Sometimes the luggage may get there before the passenger, some times after, and at times may never get there at all.

2.4 NTCIP COMMUNICATIONS FRAMEWORK; THE REFERENCE MODEL FOR OPEN SYSTEMS INTERCONNECTION

The ISO-OSI model uses the following principles to define seven distinct layers:

a. A layer should be defined for every distinct level of functionality.
b. The function of each layer should be well defined and limited to its scope.
c. International standardized protocols should be used wherever possible.
d. The interface between the layers should minimize the interaction between them.

The seven layers of the ISO-OSI are the Physical, Data Link, Network, Transport, Session, Presentation, and Application Layers. These seven layers can be viewed as forming two groups of functionality to support open communications. The first group (Layers 1-4) is responsible for data transport. The second group (Layers 5-7) is responsible for data processing.

Copyright National Electrical Manufacturers Association
Provided by IHS under license with NEMA
No reproduction or networking permitted without license from IHS
Not for Resale

The transport group defines the following functionality for each layer. Layer one, the Physical Layer, deals with how the bits of information are transmitted over a communications channel. It deals with the mechanical and electrical interfaces, and the physical transmission medium. Layer two, the Data Link Layer, has the task of transforming the information that came in over the wire into data that appears to be free of transmission errors. It should incorporate mechanisms to ensure the integrity of the data and provide a method of ensuring that, if need be, no data is lost. The function of the Network Layer is to control how packets of data are routed from source to destination. It is responsible for ensuring that information sent through several sequential physical links arrives intact. The primary purpose of the Transport Layer is to organize data to be passed to and from the lower layers. This entails breaking messages into smaller units (packets) so that they are handled efficiently by the lower layers, and assembling packets from the lower layers into messages for the higher layers. This layer is the first to deal with end-to-end communications.

The next three layers, the Session, Presentation, and Application layers, deal with application and information specific uses of data provided by the lower layers. As described in the OSI Model, the Session Layer allows different equipment to establish dialogues. A dialogue allows one piece of equipment to transfer a file or log from another machine. The Presentation Layer is concerned with the syntax and semantics of the information transferred. The Application Layer is concerned with such things as file transfers, file and device access methods, and management of data objects.

One of the basic tenets of the ISO-OSI model is the principle of *layer independence*. This allows the protocol of one layer to be independent of the protocol of an adjacent layer as long as the boundary between them provides a consistent interface. This has lead to the concept of a *layer service definition* as the specification of that interface. The layer service definition defines a set of abstract capabilities made available by the layer below the boundary to the layer above the boundary. Using this concept, protocols below a boundary may be swapped without affecting the protocol of the upper layer. Each layer of the ISO-OSI has a service definition described in terms of the layer providing the service to the layer using the service. The services themselves are made available through a conceptual link between the layers known as a *service access point* (SAP). The services are provided through an exchange of *primitives* and associated *parameters* between the *service user* and *service provider*. The primary objective of the service provider is the transparent transfer of the data given to it in a data parameter of a primitive by the service user. The data is known as a *service data unit* (SDU).

The idea of layer boundaries with well-defined service definitions (including SAPs) is a technique used for descriptive purposes. It is not intended to require that implementations be developed in such a fashion (it also does not preclude it). Indeed, implementation of the service definition within a system is not visible to other systems. The service definition concept is not intended to prohibit "streamlined" implementations that may couple several layers of protocol (and any associated state machines) nor to force each layer protocol to be implemented separately with a "clean" layer boundary above and below it.

The concept of layers is reflected in the following list showing some of the major OSI, Internet and NEMA protocols considered for the various layers. Conceptually, at any one layer, one protocol could be substituted for another.

Copyright National Electrical Manufacturers Association
Provided by IHS under license with NEMA
No reproduction or networking permitted without license from IHS
Not for Resale

Application:	RFC 1157	Simple Network Management Protocol
	NEMA TS 3.2	Simple Transportation Mgmt Protocol
	RFC 959	File Transfer Protocol
Presentation:	ISO/IEC 8825	Basic Encoding Rules
	NEMA TS 3.2	Packed Encoding Rules
Session:		
Transport:	RFC 793	Transmission Control Protocol
	RFC 768	User Datagram Protocol
Network:	ISO/IEC 8208	X.25 Packet Layer Protocol
	ISO/IEC 8473	Internetwork Protocol
Data Link:	ISO/IEC 8802	LAN Protocols
	ISO/IEC 9314-2	FDDI Token Ring MAC
	ISO/IEC 3309	HDLC
Physical:	EIA /TIA-232	RS-232 Interface
	EIA/TIA-449	
	Bell 202	FSK Modem Interface
	ISO/IEC 4903	
	IEEE 802	LAN
	ISO/IEC 9314-1	FDDI

An example of layer independence within the NTCIP Class B Profile is at the Physical Layer, where both RS-232 and Bell-202 FSK modem protocols are currently defined. Because NTCIP is extensible, other protocols may become part of the standard in future revisions.

2.5 PROTOCOL PROFILES

As mentioned earlier, the modular approach of the NTCIP enables a means of tailoring a protocol profile according to the requirements of a particular communications link or system. A profile combines a particular protocol stack with a conformance level specification for each layer of the stack. There are three basic protocol stacks defined.

For several communication profiles to co-exist (interoperate) on a common communications media, it is necessary that the Physical Layer and Data Link Layers be identical. Different Network, Transport, Session, Presentation and Application layers may be used above the Data Link Layer. If multiple Network Layers are utilized then unique Initial Protocol Identifiers (IPI) must be used to allow the received packets to be properly processed by the correct communications stack.

The following Class profile definitions identify possible stack profiles. The Class A and Class C profile definitions are not completely defined, and are shown here for comparison purposes. The Class B profile has been defined in the NEMA TS 3.3 Standard.

	Class-A	Class-B	Class-C
Layer 7	SNMP / STMP	SNMP / STMP	SNMP / STMP / FTP Etc.
Layer 6	...	...	...
Layer 5	...	...	...
Layer 4	UDP	...	TCP / UDP
Layer 3	IP	NULL	IP
Layer 2	ASYNC HDLC	ASYNC HDLC	ASYNC HDLC
Layer 1	EIA/TIA 232 / Bell 202	EIA/TIA 232 / Bell 202	EIA/TIA 232 / Bell 202

Copyright National Electrical Manufacturers Association
Provided by IHS under license with NEMA
No reproduction or networking permitted without license from IHS
Not for Resale

Layer 1 is common for all classes that must interoperate. Currently, two physical layer protocols have been defined: EIA/TIA 232 and Bell 202 FSK modem.

Layer 2 is also common for all classes that must interoperate and is defined as Asynchronous HDLC. This protocol provides Data Link Layer addressing and a reliable means of checking data frame (or packet) integrity.

Layer 3 is not required for Class B. Classes A and C will utilize the same Network Layer to provide routing capabilities.

Layer 4 is not required for Class B. Class A specifies the User Datagram Protocol (UDP), a connectionless service that provides additional user-data integrity. Class C specifies both Transmission Control Protocol (TCP) and UDP are present. TCP provides segmentation and reassembly capabilities and is a connection-oriented service.

Layers 5 and 6 are implemented by SNMP/STMP (see layer 7). For Class C, TCP provides session capabilities.

Layer 7 for Class A and Class B is defined as the Simple Network Management Protocol (SNMP) and/or the Simple Transportation Management Protocol (STMP). Both of these protocols provide for the remote access to data objects resident within a device. SNMP is the industry standard protocol. STMP has been developed to provide a more efficient means of accessing the objects on systems with bandwidth limitations or critical performance requirements. The details required to implement STMF/STMP are contained in NEMA TS 3.2.

Class B provides for bandwidth efficient exchange of information between the primary station and each secondary station on the same physical link. Class B does not ensure delivery. Frames received with errors are discarded. If retransmissions are needed, it is the responsibility of the Application Layer to provide them. This class of service is primarily intended for short command and reply messages where delivery time is a strong consideration.

The Class C stack may use TCP to guarantee delivery or signal when a message can not be delivered correctly. TCP uses sequence and acknowledge information and timers to make sure the individual frames are received and that they are put in their proper order. If a frame is garbled or lost, retransmissions are attempted. If a frame cannot be delivered, the upper layer is notified. This class of service ensures data integrity and correctness. Its primarily use is for large data transfers.

Class C may seem to provide the ideal service, however, it imposes additional overhead. Before any information can be passed, a connection between the devices must be established. The connection procedure takes a certain amount of time. When the information transfer is completed, the connection must be formally closed. The advantage of Class B is that it eliminates the overhead required to set up and tear down a connection and greatly minimizes the byte count of the messages thus, optimizing throughput.

To specify profiles, the level of conformance to the particular protocols within all layers should be defined. Specific profiles are described in separate documents. (e.g., NEMA TS 3.3 Class B Profile).

2.5.1 Physical Layer (Layer 1)

The communication channel, whether it be EIA/TIA 232, a fiber-optic modem, or radio, in ISO-OSI parlance, is called the Physical Layer. The purpose of the Physical Layer is to define what constitutes the channel and establish how the raw bits are transferred over the channel. This layer defines what a logic 1 or 0 is and what the physical transmission media is. The definition includes the mechanical, electrical, and procedural interfaces. It also establishes how a bit stream is sent or received but not its address, meaning or structure.

Copyright National Electrical Manufacturers Association
Provided by IHS under license with NEMA
No reproduction or networking permitted without license from IHS
Not for Resale

EIA/TIA 232 is specified because it is the most common method of interfacing to external communications equipment. The Bell-202 FSK Modem is specified because it is the typical method by which current traffic control systems implement communications. Other Physical Layer standards, such as RS-422 and RS-485 have been suggested but are not included in the currently defined NTCIP profiles.

2.5.2 Data Link Layer (Layer 2)

2.5.2.1 General

Data Link Layer communications are defined as the groups of bits and bytes that are transmitted over a single communication channel, in this case, Asynchronous HDLC frames. Since the information that is passed is independent of how it is passed, the Data Link Layer is distinct from the Physical Layer and can be addressed as a separate function.

The Data Link Layer operates on data that needs to be passed between two physically *connected* stations. Because there may be several stations on the same physical channel, the HDLC frame includes an address field to indicate which station is to receive the data. To indicate how the data is to be treated when it is received, a control field is also added. The Data Link Layer does not define the meaning of the data; only the meaning of its address and control fields. The definition of the "data" is left up to the higher layers and the end application. This makes the Data Link Layer communications distinct from the Physical Layer below it, and any higher layer function.

Today's typical traffic control system uses what is called an unbalanced or master / slave configuration. A single station (primary) controls access to the Physical Layer. All other stations (secondaries) connected to the Physical Layer do not have open access. This unbalanced configuration is illustrated in Figure 2-4. The HDLC standards also define a balanced configuration where any station can initiate access. NTCIP will initially support the unbalanced configuration.

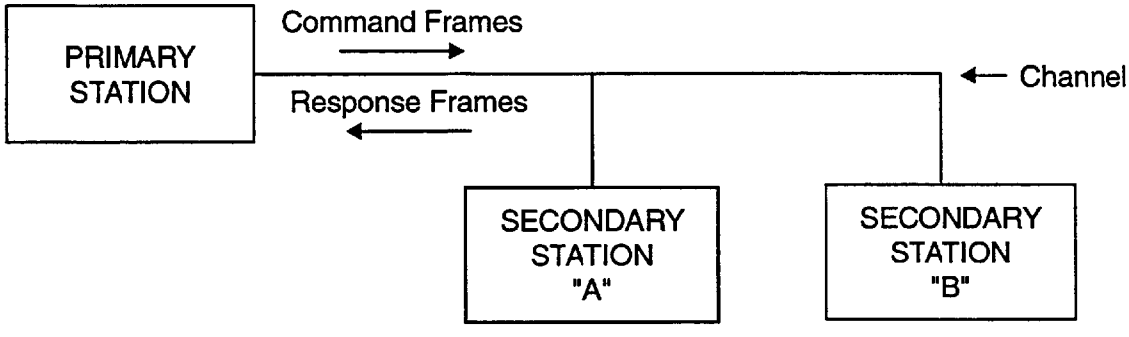


Figure 2-4
UNBALANCED MULTIDROP LINE

In systems with a centralized topology, the central computer is the primary station and the controllers/ITS devices connected directly to it are secondary stations. In a distributed closed loop traffic control topology, the primary station is the arterial master but only to the controllers (secondaries) connected to it. The arterial masters are also secondaries, but only with respect to the central computer. A similar relationship exists for ITS devices. When operating over a switched network the calling station acts as the primary when a physical connection has been established. The method of establishing the physical connection over a public switched network is the responsibility of the calling station.

There may be instances where a secondary wants to initiate an information transfer. To facilitate this, primary stations that have one or more physically connected secondaries incorporate a polling mechanism. Even if the primary station has nothing to send, it periodically solicits the secondaries to see if they have anything to send.

Copyright National Electrical Manufacturers Association
Provided by IHS under license with NEMA
No reproduction or networking permitted without license from IHS
Not for Resale

In NTCIP, secondary station replies will be limited to a single frame per response opportunity. This provides two advantages. First, the primary station controls the link timing; a secondary cannot hog the line and prevent the primary from polling another station. Secondly, it simplifies fault handling. Since the primary station always knows that there will be one and only one response frame to any command, it can take responsibility for detecting any missed frames. The secondary stations do not need to time-out or retry, since they can count on the primary to be aware of any errors.

2.5.2.2 Data Link Layer Protocol Overview

As discussed above, HDLC forms the basis for the Data Link Layer protocol of NTCIP. HDLC is comprised of four ISO/IEC standards, each providing numerous tools from which to draw when building a Data Link Layer protocol specification. The NTCIP Data Link Layer protocol is based on a subset of these tools. This subclause provides an overview of HDLC, especially as it relates to NTCIP. The detail specifications of the NTCIP Data Link Layer protocol are given in the various protocol profile documents.

HDLC provides for operation in either synchronous or asynchronous transmission mode at the Physical Layer. In a synchronous mode of transmission, the series of bytes making up a frames are sent back to back with a separate clock signal used to indicate the spacing between the bits. In asynchronous mode of transmission, a start bit and one or more stop bits are added to every byte. The data, itself, determines the spacing between the bits. At this time, NTCIP will only specify the use of asynchronous mode.

In HDLC, bits are transmitted in groups called *frames*. The basic frame structure of HDLC is defined in ISO/IEC 3309 and depicted in Figure 2-5.

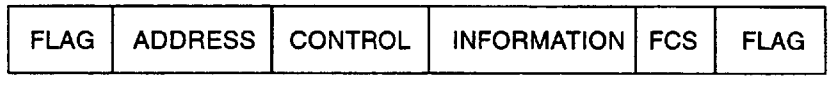


Figure 2-5
HDLC FRAME

The flag sequence is a unique bit pattern used to delimit the start and end of a frame. A transparency technique is applied to bytes between, but not including, the flags to ensure that any occurrence of the bit pattern in the data is not mistaken for a flag. In cases where throughput must be maximized, the closing flag of one frame can serve as the opening flag of the next.

As depicted in Figure 2-5, each secondary station is assigned an address that is unique among all secondary stations on the link. The primary station need not be given an explicit address since there is only one such station on a link in an unbalanced configuration. Secondary stations can only communicate with it. When the primary station and a secondary station exchange frames, the address field contains the secondary station's address. The address field may also contain a group address. This allows the primary station to send a frame to multiple secondary stations.

The control field identifies the type of frame and the actions to be taken on receipt of it. Definitions of HDLC frames types are given in ISO/IEC 4335. Although there are over twenty frame types in HDLC, NTCIP uses only two frame types known as the Unnumbered Information (UI) frame and the Unnumbered Poll (UP) frame. The information field of the UI frame is used to carry the Network Layer protocol and any higher layer information. Since there are no sequence numbers in a UI frame and no associated recovery mechanisms at the Data Link Layer, the contents of the UI frame may be lost. Recovery actions, if needed, are left to a higher layer.

The information field, also known as the Protocol Data Unit or PDU, is used to carry information received from the user of the Data Link Layer (e.g., a higher layer protocol). The Data Link Layer does not impose any constraints on the contents of this information.

Copyright National Electrical Manufacturers Association
Provided by IHS under license with NEMA
No reproduction or networking permitted without license from IHS
Not for Resale

The frame check sequence (FCS) field is used to guard against undetected bit errors in the frame. HDLC uses a CRC polynomial to generate the contents of this field based on the transmitted bits. On receipt of a frame, the same polynomial is used to check the incoming bits. If the calculated value of the FCS field does not match its contents, then the frame is discarded as having at least one bit in error. Traditional 8-bit checksums have an undetected error rate of $4x10^{-3}$. With the 16-bit CRC polynomial defined in ISO/IEC 3309, the probability of accepting a bad frame is $1.5x10^{-5}$. This polynomial detects all single and double bit errors, all errors with an odd number of bit errors, all burst errors of 16 bits or less, 99.9969% of 17-bit burst errors, and 99.9984% of all 18-bit or longer burst errors.

For proper operation of a Data Link Layer, there are a number of system parameters required. For the UCC class used by NTCIP, the only parameters are the maximum number of bytes allowed in the information field of a UI frame and four timers. The timers ensure that frames are send efficiently and that lost frames do not tie up the network.

2.5.3 Network Layer (Layer 3)

2.5.3.1 General

Network Layer communications are defined as the packets which are passed through one or more communication channels (or physical layers). Data Link Layer communications are point-to-point oriented (confined to one physical channel), Network Layer communications are end-to-end oriented.

In principle, a Network Layer message will consist of data that needs to be passed between two indirectly connected stations. Because there may be several intermediate stations, Network Layer packets are embedded in Data Link Layer frames which are passed to the appropriate secondary station. While an address in the Data Link Layer address field indicates the next secondary destination station, a Network Layer address field indicates the original source of the data and the final destination station.

Figure 2-6 may be used as an example to illustrate a Network Layer message transaction.

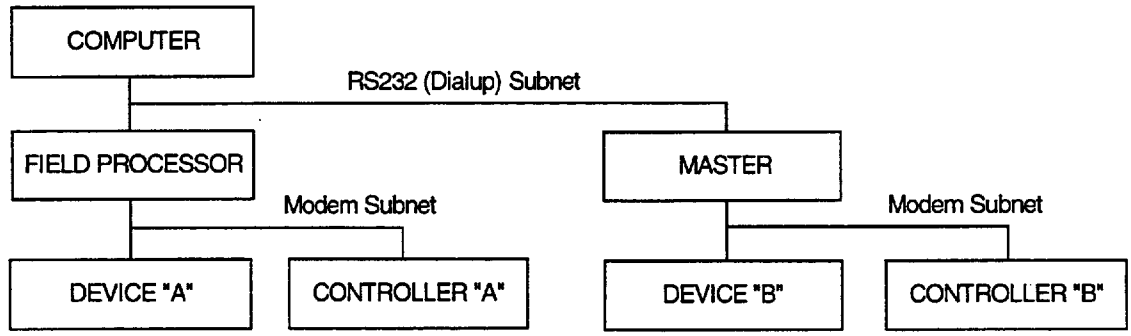


Figure 2-6
Network Example

The computer needs to send a message to Device 'A'. Since it does not have a direct link to Device 'A', it must first connect to the Field Processor over the RS-232 Dial-up Subnet. Once connection is made, the computer transmits the message in a frame which contains a Network Layer address. The Field Processor uses the Network Layer address to determine if the message is destined for one of its secondaries. Once this is done, the Field Processor determines the Data Link Layer address of the device, in this case Device 'A' and routes the message to Device 'A' using its Data Link Layer communications protocol. The two operations comprise a Network Layer transfer.

Copyright National Electrical Manufacturers Association
Provided by IHS under license with NEMA
No reproduction or networking permitted without license from IHS
Not for Resale

2.5.3.2 Network Layer Protocol Overview

In 2.5.3.1, there are several classes of operation at the Network Layer. The first byte of the information field is called the Initial Protocol Identifier or IPI. This byte is used to determine which Network and Transport layers a message must be processed by.

Class B, allows for bandwidth-efficient exchanges of data packets. This is a simple protocol with no functionality except to skip over the Network and Transport layers. Because it provides no routing capabilities, it is not considered a true network layer protocol. By eliminating the Network and Transport layer protocols (IP and UDP), the message length is shortened by 26 bytes.

The Internet Protocol (IP) is used by NTCIP to provide the routing services required by the Network Layer of the Class A and Class C protocol stacks. The IP header contains 20 bytes and includes source and destination addresses, etc. Due to its significant protocol overhead IP is not well suited for use with 1200 baud systems. The detailed specifications of all protocol modes are given in the various protocol profile documents.

2.5.3.3 Addressing

An address provides the means by which a station is identified. An address must be unique in the context in which it is used. Furthermore, an address is represented in an abstract fashion (such as a string of up to x digits where each digit is in the 0-9 range or a string of exactly y characters where each character is from the groups A-Z, a-z, and 0-9). This is independent of the encoding in a protocol used to carry the address (i.e., digits of the first type of address are encoded in binary coded decimal in one protocol whereas they may be encoded in binary in another protocol, but the semantic meaning of either type of encoding is the same).

In the NTCIP environment, there are two types of addresses; the Data Link Layer address and the Network Layer address.

A unique Data Link Layer identifier is assigned to each secondary station or node sharing a physical link and is used only for communications on that common link. This identifier is used in the address field of Data Link Layer frames. Stations on different links may have an address field with the same value, but since they do not communicate directly, the address value is unique within its context. In NTCIP, the Data Link Layer address space allows for many stations to be uniquely defined on any one physical communications link.

When a system consists of several interconnected physical links and data needs to be routed between devices on these links, additional address information is required to route the data. In the case of the Class-A and Class-C profiles, which support routing, Network Layer addresses must be assigned to each device. The Network Layers of these profiles use the IP protocol to direct datagrams from the source computer to the destination computer. Thus, an IP address is assigned to the appropriate devices on the internet. The IP address is 4 bytes long and is represented by 4 decimal numbers separated by dots. This address is contained in the IP header section of a frames information field when IP is used.

NTCIP does not define a formal definition of how addresses are assigned or allocated. What is specified is the address space and how it is interpreted. It is assumed that it is the responsibility of the system implementer or installer to:

a. Set the Data Link Layer addresses as part of establishing communications between the primary and secondary devices on any particular link or channel.
b. Assign network (IP) addresses for the devices on an internet.

Copyright National Electrical Manufacturers Association
Provided by IHS under license with NEMA
No reproduction or networking permitted without license from IHS
Not for Resale

How addresses are allocated and the scope over which they are unique is left up to the system implementer since different jurisdictions may want to set up systems differently. When a communications network is set up, one or more Registration Authorities (RA) are usually established to coordinate and perform the function of allocating and assigning unique identifiers to devices served by the network. The roles and responsibilities of an RA are best explained by way of example. The telephone network has several RAs who allocate and assign phone numbers. Each branch exchange assigns a circuit number to a customer. Each regional telephone company has an RA that allocates and assigns an exchange number to that customer. In order to coordinate unique telephone numbers across North America, the regional companies defer to the North American Numbering Plan Administration for assignments of area code numbers. That agency in turn concedes authority to ITU-T to establish country codes. Each is responsible for establishing an unique identifier for all devices that fall under their jurisdiction.

One of the main references on RAs in the field of open computer communications is CCITT Rec. X.660 I ISO/IEC 9834-1. This provides a general description of the procedures used in the operation of a RA. It develops concepts that are applicable to any environment that has a concern about unique and unambiguous identification of objects. In ITS applications, the RA has not been determined at this time.*

2.5.3.4 Routing

Routing is a Network Layer function by which a path is found from one system needing to transmit information to another system identified by a destination address. The destination address is the unique (in the NTCIP environment) Network Layer address described in 2.5.3.3. Using this address, the routing function of a station derives the next *datalink* to be traversed towards the destination and the datalink address corresponding to a station on that datalink. As such, all stations perform a routing function although it may be simpler in some than in others.

2.5.3.5 Relaying

Relaying is a function performed at the Network Layer by systems acting as an Intermediate System (IS). An Intermediate System simply forwards information received from one subnetwork (NTCIP link) to another. The relay function transfers the semantic content of the incoming packet into an outgoing packet independent of (protocol) syntax. The relay function is independent of the incoming and outgoing Network Layer protocols. For example, the protocol on the incoming side could be X.25 with IP on the outgoing side. For protocol translation to be completely successful, both protocols must support the same features. Features supported by one protocol, but not the other, can not be "relayed" across the IS. The relay function works in conjunction with the routing function.

2.5.4 Transport Layer (Layer 4)

Class B does not utilize a Transport Layer. It performs no segmentation and reassembly functions.

2.5.4.1 User Datagram Protocol (UDP)

The Class A and Class C protocol stacks use UDP, an Internet standard, as its connectionless-mode transport protocol. UDP segments are transmitted in IP datagrams. This protocol provides a means of identifying the "port" or application on a device that is to receive the data by including source and destination port fields. It contains a length field which includes the length of the UDP header and user data. It also provides a checksum of the UDP header and data. UDP is the standard interface to SNMP, the primary Application Layer protocol used by the NTCIP.

---

* The recommendations for addressing schemes are still under development. For the latest information regarding the continuing development of NTCIP, jump to the NTCIP home page on the World Wide Web at: http://www-fhwatml.com/ntcip

Copyright National Electrical Manufacturers Association
Provided by IHS under license with NEMA
No reproduction or networking permitted without license from IHS
Not for Resale

2.5.4.2 Transmission Control Protocol (TCP)

The Class C protocol stack uses TCP, another Internet standard, as its connection-oriented transport protocol. TCP provides the logic that ensures data exchanged between hosts are reliably delivered. It also routes incoming data to the proper application. TCP includes the port identification and checksum features of UDP and includes the required connection establishment, data transfer and connection release services. In order to make transmission of a block of data more manageable, TCP may break the block into smaller segments. Each segment is sequentially numbered. This allows the receiving device to reorder any segment received out of sequential order. TCP also provides for packet retransmission in the event of lost data packets.

2.5.5 Session, and Presentation Layers

The functions of the Session and Presentation Layers are performed by SNMP/STMP, UDP or FTP and TCP (Class C).

2.5.6 Application Layer (Layer 7)

2.5.6.1 General

By specifying various protocol profiles, the NTCIP provides a mechanism for supporting "plug and play" capability for common device types. At the Applications Layer, this is accomplished through the use of the Simple Network Management Protocol (SNMP) and its derivative, the Simple Transportation Management Protocol (STMP). Both SNMP and STMP use the word "objects" to refer to the accessible data or variables within a device. Objects are used for both data retrieval and device control. Devices are controlled by changing the value of an object. Each class of device has a set of defined objects that support basic device functionality. As an example, all the objects required to control a variable message sign are defined in the TS 3.6 document. Each object has a well defined function and a unique identifier. Thus, an object on the same class of device from several different manufactures has the same address and performs in an identical manner. For a device to comply with a particular NTCIP profile, it must support all the mandatory objects defined for the device profile. To provide for innovation, experimental and non-standard objects can be defined. This allows the standard to be upgraded over time as new, innovative objects become standardized after wide acceptance.

SNMP was chosen because it provides a well defined mechanism for generically managing devices on large networks and internets. Several benefits result from selecting an Internet standard such as the wide availability of development tools, the pre-existent management applications and the low cost of registration and validation functions offered through the Internet Assigned Number Authority (IANA). SNMP has proven to be a successful protocol for managing a wide variety of communications equipment from a diverse base of manufacturers.

STMP was designed by NEMA to provide a bandwidth-efficient means of supporting the legacy infrastructure. It can be used independently or in conjunction with SNMP. The STMP protocol is able to perform the general functions of SNMP in a less flexible but, significantly more efficient manner. The SNMP and STMP protocols compliment each other. SNMP is designed foremost for extensibility and flexibility while STMP is designed for efficiency on communications mediums with limited bandwidth. Using two complementary protocols results in a solution that satisfies more requirements than a single (compromised) protocol.

2.5.6.2 Simple Transportation Management Framework (STMF)

The overall structure of the NTCIP Application Layer is based upon the Simple Transportation Management Framework (STMF). STMF is the result of studying the Internet-Standard Network Management Framework and applying it to the management of transportation equipment and transportation networks. STMF is intended to satisfy the requirements for integrated device management within the transportation industry.

Copyright National Electrical Manufacturers Association
Provided by IHS under license with NEMA
No reproduction or networking permitted without license from IHS
Not for Resale

STMF has four components:

a. Structure and Identification of Management Information (SMI)
b. Management Information Base (MIB)
c. Simple Network Management Protocol version 1 (SNMP)
d. Simple Transportation Management Protocol (STMP)

The SNMP and STMP components of the Applications Layer are concerned with the syntax and semantics of the information being transferred. Their task is to encode data (objects) from its internal representation to a form suitable for transmission and decode received data into a form used internally.

2.5.6.3 Structure and Identification of Management Information (SMI)

The SMI describes the identification scheme and common structures that define information used by a system or network. The SMI structure is specified in Abstract Syntax Notation One (ASN.1). ASN.1 was standardized in 1984 by CCITT and is covered in Recommendation X.208. ASN.1 is a language designed for the purpose of describing structured information. It is used to describe Protocol Data Units (PDU) or message formats for various communications protocols. A companion standard, Recommendation X.209, is used to encode data for transmission by lower layer services.

To identify data objects, ISO/IEC and the CCITT have established a hierarchical structure of names (a tree). This structure is outlined in CCITT RECOMMENDATION X.660 I ISO/IEC 9834-1. Under this structure, data objects are unambiguously identified by constructing names composed of one component from each level of the tree. NEMA has been registered under the Internet network management portion of the *global name tree* as the information registration authority for NTCIP as shown in Figure 2-7. Further information is provided in Clause 2.5.6.7.

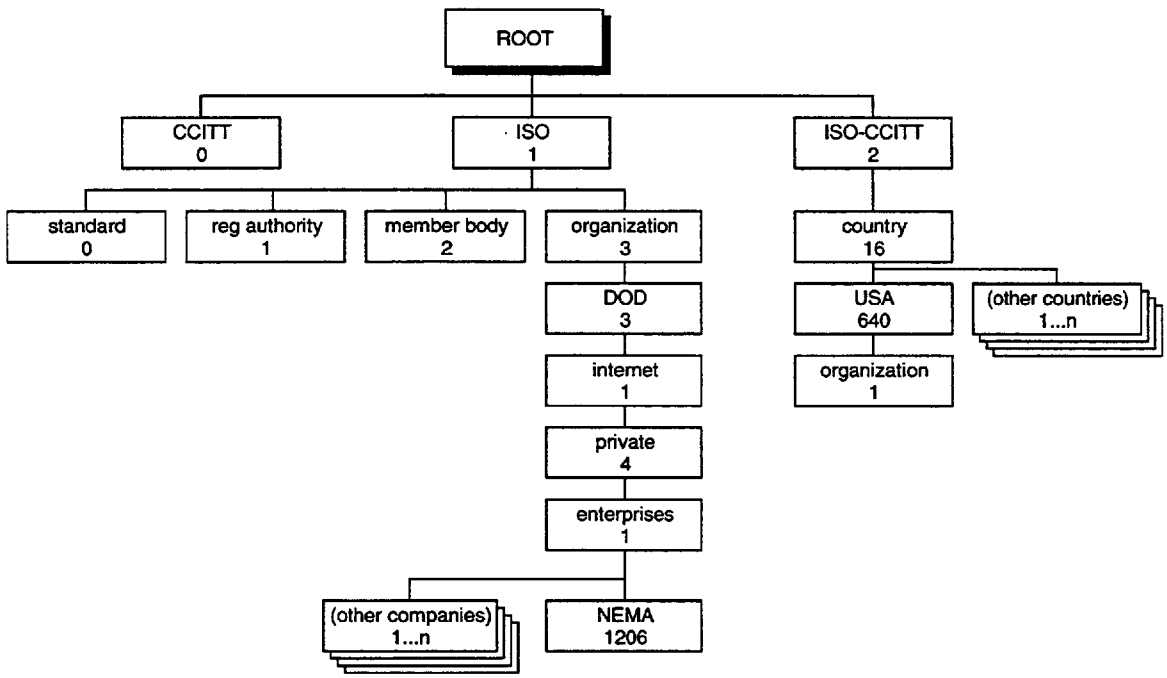


Figure 2-7
THE INTERNET AUTHORITY HIERARCHY

Copyright National Electrical Manufacturers Association
Provided by IHS under license with NEMA
No reproduction or networking permitted without license from IHS
Not for Resale

2.5.6.4 Management Information Base (MIB)

A Management Information Base (MIB) is an ASCII text document written using the ASN.1 notation. This machine readable document describes the information used in a system. Each unit of information is termed a *managed object.* A managed object is the smallest entity that can be exchanged between a device and a management application. Objects can be of the primitive type such as a single byte or word. Objects can also be constructed from primitive objects. For example, a "string" is a sequence of bytes.

A collection of related managed objects is defined in a document termed a MIB module. Single or multiple modules may be required to define the complete Management Information Base for a transportation system. MIB module files are typically made available for downloading.

The result of creating and identifying managed objects using ASN.1 is that a standard computer readable description of a devices internal data format exists. A MIB module for each NTCIP compliant product should be available from the manufacturer. When users purchase equipment, the MIB module is used to update their management applications. An SNMP management application, running on a central control system, typically loads the MIB modules from a floppy diskette. The management application then has a description of the data objects resident within the remote device and the information required to properly access the data. See Figure 2-8.

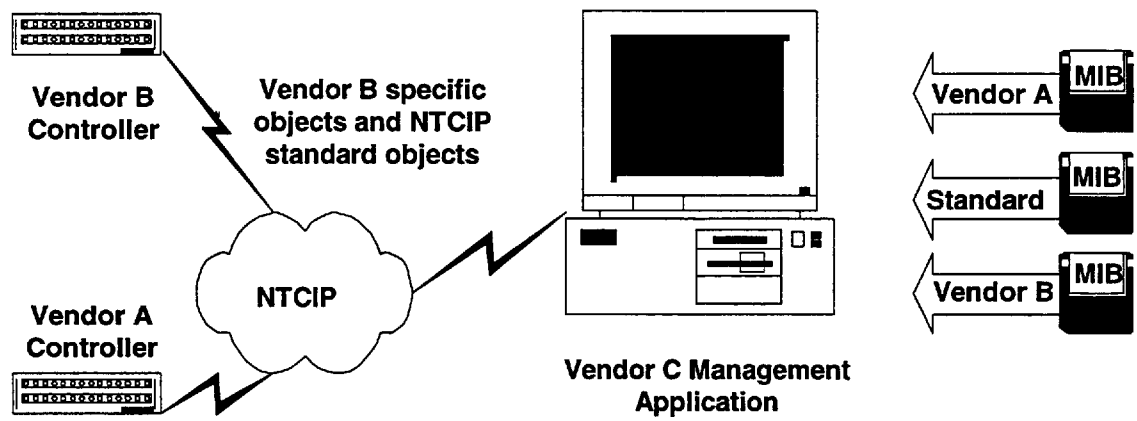


Figure 2-8
MIB INTEGRATION

2.5.6.5 Simple Network Management Protocol (SNMP)

The Simple Network Management Protocol (SNMP) is used by the Internet networking community for management of intelligent devices in a network. It is the dominant network management protocol used in computer networks today. For use within NTCIP, SNMP is used with no changes. SNMP uses Basic Encoding Rules (BER) to encode data for transmission by the lower layer services.

In concept, a network management system consists of three components:

a. One or more *managed nodes (devices)*, each with an (SNMP) *agent* which sends and receives SNMP messages.
b. At least one *network management station* (NMS), each with at least one network management application—each sending and receiving SNMP messages.
c. The network management protocol, SNMP, which is used by the *agent* and *manager* to exchange management information.

Copyright National Electrical Manufacturers Association
Provided by IHS under license with NEMA
No reproduction or networking permitted without license from IHS
Not for Resale

The SNMP protocol uses a remote debugging paradigm. Each managed node has management information (configuration, operating parameters, and monitored variables) within the device. These variables are referred to as managed objects. By changing the value of these objects, the managed node is controlled. This means that imperative commands, such as "restart device," are not needed. Any necessary command can be realized by changing the value of an object defined for this purpose. In addition to changing (configuring or controlling) objects within a device, other objects can be defined for the purpose of monitoring.

The SNMP protocol specifies four basic operations:

a. get—Read the contents of a managed object.
b. set—Change the contents of a managed object.
c. get-next—Read the contents of the object that has the next sequential address in a devices Object ID tree. (Allows interrogation of a device for supported features.)
d. trap—allows a device to indicate to a management application that an event has occurred.

A *get-request* is the basic command to ask for data and the *get-response* is the reply to that request. The *set-request* and *get-response* are used to send data and confirm its reception. The *get-next* operation causes the return of the value of the next object instance in the lexicographic order of the tree supported by the device.

In network management terminology, an interrupt or the occurrence of an event is called a *trap*. The easiest way to configure, monitor and control traps are by using managed objects for that purpose. For example, a "Cabinet Door Open" object could be identified. If trap generation for this object is enabled, a *trap* message containing the objects' identifier and data is prepared to be sent to the management application to indicate the event has occurred. With NTCIP, the trap response is not transmitted until the secondary device receives a poll command from its primary device.

To encode the data for use by the lower layers, Basic Encoding Rules (BER) are used as specified in ISO 8825. Although ASN.1 can describe complex data structures, the representation of data on a communication medium requires additional rules. These rules are encompassed within the BER. The definition of an object includes a description of how it is encoded by BER.

2.5.6.6 Simple Transportation Management Protocol (STMP)

The purpose of the Simple Transportation Management Protocol (STMP) is to offer a method to set or get objects in a device with a minimum amount of communications protocol overhead.

STMP accesses objects with maximum efficiency. Both STMP and SNMP perform the same basic operations (get, set, and trap) on simple objects. STMP lessens the amount of data required to perform such operations, however, by eliminating 20 bytes from each message header and eliminating 6 bytes from the length of each objects ID as compared to an equivalent SNMP message. SNMP does not have a convenient method for accessing aggregate objects. STMP defines an new method for doing this.

This new STMP mechanism is called *dynamic objects*. The dynamic object mechanism allows a user to access multiple objects using a single request. Using SNMP or STMP, the user can define a list of objects to access. The user can then set or get all objects in the list using only one byte of protocol overhead. A dynamic object consists of both objects in its definition table and the actual data to be accessed. The definition table is a list of pointers to the objects to be accessed. The data is the information retrieved via the objects pointed to. For example, if you have objects 1.2.1, 7.6.4 and 3.17.9 and wish to retrieve them with one message, combine them into a single dynamic object. This is done by using an SNMP or STMP set-request to set up the definition table for a particular dynamic object. Once the values (1.2.1, 7.6.4, and 3.17.9.) are set in the definition table, any set or get to that dynamic object

Copyright National Electrical Manufacturers Association
Provided by IHS under license with NEMA
No reproduction or networking permitted without license from IHS
Not for Resale

will access all three objects. This eliminates the overhead associated with sending the Object ID for each object on every get or set request.

SNMP and STMP are intended to be complimentary members of the NTCIP Application Layer protocol.

2.5.6.7 Information Registration Authority Hierarchy

Standard and proprietary objects must be unambiguously identifiable. Ideally, all the operational characteristics of a class of equipment should be exactly the same. The information that each device handles and stores would then be exactly the same. Individual manufacturers and agencies, however, tailor equipment to specific needs. To provide standardization but still handle the special needs, it is imperative that all information be registered to ensure that there are no conflicts. To meet the general information identification/management requirement, ISO/IEC/ and the CCITT have established a hierarchical structure of names (a tree). This structure is outlined in CCITT RECOMMENDATION X.660 I ISO/IEC 9834-1. Under this structure, objects are unambiguously identified by constructed names composed of one component from each level of the Registration Authority hierarchy under which the object is registered. To conform to this standard, the Committee has registered NEMA as the information registration authority. NEMA has been registered under the Internet network management portion of the *global name tree*. Pending application to ISO-CCITT for a new position in the tree, the official identification number for all NEMA NTCIP related transportation management information is prefaced with:

1.3.6.1.4.1.1206

It can also be represented by the textual naming convention as:

iso.org.dod.internet.private.enterprises.nema

Figure 2-7 illustrates the global name tree structure and the position of NEMA. The organization of information under the NEMA node is then arranged in four subtrees as shown in Figure 2-9. The current complete NEMA tree is shown inFigure 2-10. Several other standard nodes, such as directory and security are not addressed at this time.

Management	1.3.6.1.4.1.1206.1
Experimental	1.3.6.1.4.1.1206.2
Private	1.3.6.1.4.1.1206.3
Transportation	1.3.6.1.4.1.1206.4

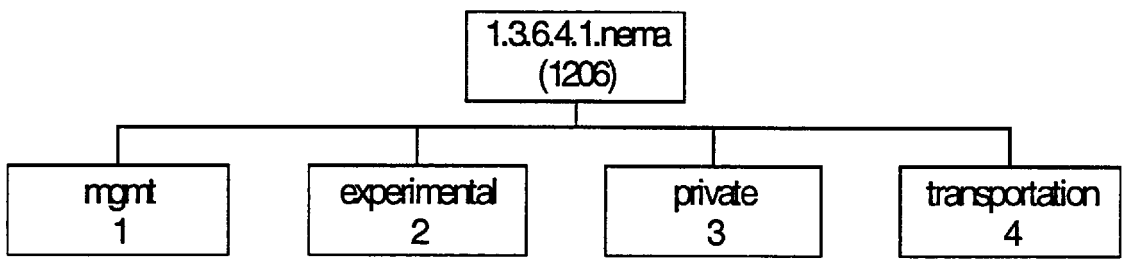


Figure 2-9
NEMA NODE

The *transportation* node will be subtreed to identify objects which are defined in NEMA approved documents. Administration of the transportation subtree is solely under the authority of NEMA. As proposals which define new versions of the NEMA Transportation Management Information Base are approved, they are assigned an identifier by NEMA for identifying the objects defined by that proposal. The *experimental* subtree is used to identify objects that are under investigation and trial. Objects under

Copyright National Electrical Manufacturers Association
Provided by IHS under license with NEMA
No reproduction or networking permitted without license from IHS
Not for Resale

the experimental subtree might include an initial proposal for a new untested device. The *private* subtree is used to identify objects defined unilaterally. Administration of the *private* subtree is by NEMA. A subtree under *private* called *enterprises* is typically used to identify proprietary but published information about an organization's device information database. This allows NEMA to ensure unique product identification and yet delegate the role of assigning numbers to those members requesting them, except of course, for the initial *enterprise* numbers.

Referring to Figure 2-10, the branches under the *transportation* node break its related information down into 2 subtrees; *protocols* and *devices*. The *protocols* subtree contains all information related to the communications aspect of NTCIP. This layer is further divided into 3 subtrees; *layers*, *profiles* and *dynObjMgmt*.

Each of the protocols and interfaces defined for use within NTCIP have objects associated with them that are required for proper system administration. Objects are already defined for these protocols and interfaces including SNMP, HDLC and EIA/TIA 232 in the global naming tree. When objects are already defined in other parts of the global naming tree, they should not be redefined under the NEMA root. The *layers* branch defines the subsets of these predefined objects which are pertinent to NTCIP systems. The *profiles* subtree defines further subsets of communications oriented objects required for the administration of devices complying with the various NTCIP class profiles. The *dynObjMgmt* (dynamic object management) subtree is used to define information related to the use of dynamic objects.

The *device* branch covers the standardized transportation object definitions. Because they are application specific and not related to the communications protocol they are covered under separate documents called *NTCIP Object Definitions*. A separate document will cover each device type shown in the figure.

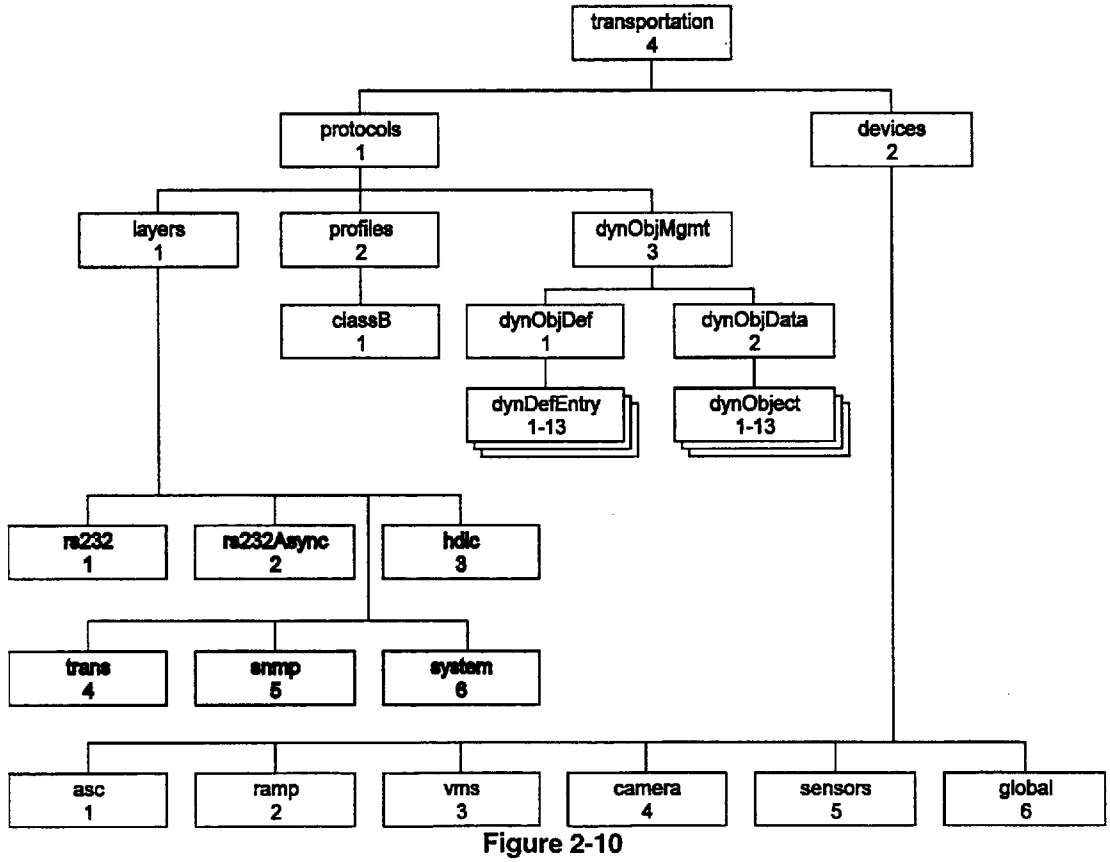


Figure 2-10
NEMA TREE

Copyright National Electrical Manufacturers Association
Provided by IHS under license with NEMA
No reproduction or networking permitted without license from IHS
Not for Resale

As can be seen, the *devices* subtree currently has six transportation related categories: actuated controllers, ramp meters, variable message signs, cameras, sensors and global. The *actuated signal controller* subtree covers the common objects found in actuated traffic controllers. The *ramp meter, camera* and *variable message sign, etc.* nodes cover the common objects found in those devices. The *global* subtree contains objects related to device ID, date and time, etc. The number of branches on a subtree is extendible. Thus, new devices can be added to a subtree as the objects for these devices become standardized.

Manufacturers and agencies who need to create custom objects and MIBs, should obtain a vendor number from IANA or NEMA. Once this is done, each enterprise can define their own sub-branches of the tree with knowledge that all object identifications prefixed with their vendor code are unique within the ISO-CCITT registration tree. If a NEMA number is obtained, the objects scope will be limited to the NEMA tree.

In order to compile a MIB module, the SMI definitions header must be included in the module. SMI does not define objects but instead defines *how* to create managed objects. In other words, SMI defines how to utilize ASN.1 to create and identify managed objects within a tree like structure.

2.5.6.8 Object Management

In ASN.1, an object type definition consists of seven fields:

a. Object name—A textual name and an identifier for the object type
b. Syntax—The abstract syntax of the object, i.e. an INTEGER, OCTET STRING, etc.
c. Definition—A textual description the object and its usage
d. Access—The object can be read-only, read-write, write-only, or not-accessible
e. Status—Support is either mandatory, optional, or obsolete
f. Reference—[Optional] reference information for object
g. Default Value—[Optional] value to be used when creating new entries

The object name is represented uniquely as an *OBJECT DESCRIPTOR* and an *OBJECT IDENTIFIER*. Each OBJECT DESCRIPTOR corresponds to an object type in the STMF standard MIB. It is a unique mnemonic composed of printable characters. The OBJECT IDENTIFIER is the sequence of integers used to locate the object within the global tree.

The syntax of an object type defines the abstract data structure corresponding to that object type. For example, the structure of a given object type might be an INTEGER, OCTET STRING, or a SEQUENCE of BYTES. BER uses the object's syntax field to encode the object for transmission or to decode the data after reception.

The definition field contains ASCII text that describes the object. This field should include information that fully describes the object's operational use.

The read-only, read-write, and write-only options for access are commonly used. The not-accessible attribute is used to note that this object is used for definition purposes and is not substantiated or an actual object.

2.5.6.8.1 NTCIP Managed Objects

In the NTCIP environment, there are certain objects that must be supported by all devices complying with the standard. These objects are covered by branches under the *protocols* and *global* nodes of the *nema.transportation* tree. The following are several of the types of objects under the global node to provide a sense of what is covered:

Copyright National Electrical Manufacturers Association
Provided by IHS under license with NEMA
No reproduction or networking permitted without license from IHS
Not for Resale

a. Time: Current time of day
b. Manufacturer: Manufacturer's Name
c. Protocol: Protocol version
d. Device: Device type
e. Version: Software version

These types of global object definitions can be found in NEMA TS 3.4.

2.5.6.8.2 Device Specific Objects

For a specific type of device, standard objects need to be defined in order to allow for interchangability between similar devices from different manufacturers. Several documents have been developed to specify the standard objects for classes of devices. The following documents are currently defined for device specific objects:

a. Actuated Signal Control Device Object Definitions (TS 3.5)
b. Variable Message Sign Device Object Definitions (TS 3.6)

2.5.7 Security

Security procedures are needed to guard against threats from people/systems trying to undermine NTCIP systems. Different procedures are needed depending on the threats perceived to be relevant to the environment. In particular, threats and their associated procedures are defined as follows:

a. A system masquerading as another system for the purpose of obtaining service requires *authentication* procedures (such as passwords) as a counter-measure.
b. An unauthorized system unnecessarily tying up the resources of another system requires *access control* procedures.
c. A system receiving services but then claiming it did not so as to not pay the charge requires *non-repudiation* procedures (such as digital signatures).
d. A system eavesdropping on the data flow between two other systems for the purpose of reading the information or for determining data traffic patterns requires *confidentiality* procedures (such as encryption or traffic padding).
e. A system changing, adding or deleting information flowing between two systems requires *integrity* procedures.

Currently, NTCIP does not explicitly define security procedures. However, authentication procedures utilizing SNMP community names and IP addresses are possible within the Class A and proposed Class C profiles. Other methods may involve the use of a password exchange at the Application Layer. Procedures to guard against other threats will be considered for inclusion in a future edition of NTCIP.

2.5.8 Conformance and Protocol Implementation Conformance Statement (PICS)

Implementation of a protocol from a common standard does not ensure that two systems can inter-operate with each other. The situation is exacerbated when the standard includes ranges of parameters or various options that may or may not be included in the implementation. To maximize the potential of inter-operability, a protocol standard should state the mandatory features that all conforming implementations shall include. A Protocol Implementation Conformance Statement (PICS) proforma is a questionnaire that implementers fill out describing the features of the system. Questions about mandatory features only allow for a "Yes" answer while questions about optional features allow a "Yes" or "No" answer. In this way, the PICS proforma can be used to determine if a system conforms to the standard (all mandatory features checked as "Yes") and what options have also been implemented.

Copyright National Electrical Manufacturers Association
Provided by IHS under license with NEMA
No reproduction or networking permitted without license from IHS
Not for Resale

A completed PICS proforma can be used for several purposes:

a. To allow an implementer to verify that all mandatory features have been implemented;
b. To allow a tester to determine which features to test (i.e., tests should not be run on optional features that have not been implemented, but a system is considered not to conform to the standard if it does not implement one or more mandatory features); and
c. To allow the procurer of the system to know what features have been included in the product.

A Protocol Implementation Conformance Statement (PICS) Proforma will be included with each class profile.

The main body of the protocol is copyrighted to ensure the integrity of the standard. The intention of providing the PICS proforma as an attachment is to clearly point out that it can be copied and used by agencies to ensure conformance to the standard.

2.5.9 Conclusion

The intent of this document is to provide an overview of the NTCIP and the various protocol profiles defined by this standard. Further details required to implement the Class A through Class C profiles are contained in the following documents:

a. Class A: NTCIP-Class A Profile (TS 3.x)
b. Class B: NTCIP-Class B Profile (TS 3.3)
c. Class C: NTCIP-Class C Profile (TS 3.x)

The details required to implement STMF/STMP are contained in NEMA TS 3.2.

These documents contain information not covered in this overview document. Each document contains the details of each protocol that can be used within a profile.

Device specific objects defined to date are contained in NEMA TS 3.4, NEMA TS 3.5, and NEMA TS 3.6.

Copyright National Electrical Manufacturers Association
Provided by IHS under license with NEMA
No reproduction or networking permitted without license from IHS
Not for Resale

NEMA STANDARDIZATION BACKGROUND

The purpose of NEMA standards, their classification, and status are set forth in certain clauses of the NEMA *Standardization Policies and Procedures* manual and are referenced below:

Purpose of Standards

National Electrical Manufacturers Association Standards are adopted in the public interest and are designed to eliminate misunderstandings between the manufacturer and the purchaser and to assist the purchaser in selecting and obtaining the proper product for their particular needs. Existence of a National Electrical Manufacturers Association Standard does not in any respect preclude any member or nonmember from manufacturing or selling products not conforming to the standard.

Definition of a Standard

A standard of the National Electrical Manufacturers Association defines a product, process, or procedure with reference to one or more of the following; nomenclature, composition, construction, dimensions, tolerances, safety, operating characteristics, performance, rating, testing, and the service for which they are designed.

(Standardization Policies and Procedures, p. 1)

Dimensions

Where dimensions are given for interchangeability purposes, alternate dimensions satisfying the other provisions of the Standards Publication may be capable of otherwise equivalent performance.

(Standardization Policies and Procedures, p. 6)

Categories of Standards

National Electrical Manufacturers Association Standards are of three classes, which have received the affirmative vote of at least two-thirds of the Subdivision votes cast in the affirmative or negative:

NEMA Standard, which relates to a product, process, or procedure commercially standardized and subject to repetitive manufacture.

Suggested Standard for Future Design, which may not have been regularly applied to a commercial product, but which suggests a sound engineering approach to future development.

Adoptive Standard, which is adopted in whole or in part from the standards of another organization, either domestic, regional, or international.

(Standardization Policies and Procedures, p. 5)

Authorized Engineering Information

Authorized Engineering Information consists of explanatory data or other engineering information of an informative character not falling within the classification of NEMA Standard or Suggested Standard for Future Design, which standard has received the affirmative vote of at least two-thirds of the Subdivision votes cast in the affirmative or negative.

(Standardization Policies and Procedures, p. 5)

Identification of Status

Standards in NEMA Standards Publications are identified as "NEMA Standard," "Suggested Standard for Future Design," or "Adoptive Standard." These indicate the status of the standard. A statement incorporating the auxiliary verb "shall" indicates that compliance with a requirement is mandatory for compliance with the standard. These classes of standards are identified in the foreword or throughout the text.

The material identified as "Authorized Engineering Information" is designated similarly. Statements incorporating other auxiliary verbs such as "should," "may," etc. refer to the authorized engineering information and not to procedures required for compliance with the standard.

Copyright National Electrical Manufacturers Association
Provided by IHS under license with NEMA
No reproduction or networking permitted without license from IHS
Not for Resale

NEMA TS*3.1 96 6470247 0509497 236



NATIONAL ELECTRICAL MANUFACTURERS ASSOCIATION • 1300 N. 17TH STREET • ROSSLYN, VA 22209

Copyright National Electrical Manufacturers Association
Provided by IHS under license with NEMA
No reproduction or networking permitted without license from IHS
Not for Resale