**This paper was presented at the ITS America 2009 Annual Meeting and the 2009 ITE District 6 Annual Meeting**

# NTCIP Center-To-Field Step by Step

**Ralph W. Boaz**

**Abstract.** The National Transportation Communications for ITS Protocol (NTCIP) standards have been in existence for over 10 years. Early deployments of NTCIP had many issues as deployers had difficulties getting their systems operational. NTCIP is now widely deployed and accepted across the country as the communications protocol of choice for the transportation industry. This paper is written to agencies and consultants providing an up-to-date, accurate and concise primer on NTCIP center-to-field communications. It describes NTCIP in an easy to understand fashion through a series of questions: "Why NTCIP?", "How does NTCIP work?", "How is NTCIP specified?", "How is NTCIP tested?" and "What are the lessons learned?" The specification of NTCIP is described in a unique step by step fashion including a flow chart to help users identify the NTCIP profiles standards they will need. The paper also introduces the new *NTCIP Guide Version 4* that was just recently accepted as a Recommended Information Report by the NTCIP Joint Committee.

**Keywords.** NTCIP, center-to-field, communication, interoperable, specification

## WHY NTCIP?

The transportation industry has a history of deploying systems with unique data definitions and proprietary communications protocols. Field devices and systems from one manufacturer or developer were not *interoperable* with those of other manufacturers or developers (second sources). *Interoperability* is defined as the ability of two or more devices to exchange information and use the information that has been exchanged. As deployed, proprietary systems require upgrades or expansion, agencies are forced to go back to the original equipment suppliers, face deploying separate systems and communications for each new field device, or pay for extensive integration projects developing common interfaces or translators for their particular needs. The National Transportation Communications for ITS Protocol (NTCIP) has been developed to mitigate these issues. The standards define common data definitions and open protocols ("open" meaning available to everyone) which, when specified properly, create a system environment that can be expanded and adapted with multiple types of field equipment from multiple manufacturers (see Figure 1). It should be emphasized that NTCIP deployments are not routine. NTCIP is not like a consumer product that will work between two devices just because they have the same type of connector. The transportation industry is full of both standardized and custom equipment operating on 1200 baud serial lines to Gigabit Ethernet. It is common to use modern communications network media in an older technology fashion and vice versa. From the agency's point of view, they simply want their central systems and varied field devices to work together. NTCIP facilitates this but it is up to the agency to specify their system in a fashion where it can occur.

There are two types of communications defined by the NTCIP standards: Center-to-Field (C2F) and Center-to-Center (C2C). A center may be a workstation, a laptop, personal data assistant (PDA) or anything other device used to manage the operation of field devices. Field devices include traffic controllers, cameras, detection equipment, dynamic messages signs, ramp meters, environmental sensors, street lighting and others. C2C communication uses a peer-to-peer communication model. It was designed to share information between centers whose main functions may be diverse such as traffic systems and traveler information systems or emergency management systems and toll collection. Users are directed to the *NTCIP Guide* for more information on C2C communications. C2F communication uses a client-server communication model where the center is the client and the field devices are servers. It is designed so that a center may configure, control, monitor, and retrieve historical reports from numerous transportation field devices regardless of who manufactured the device.

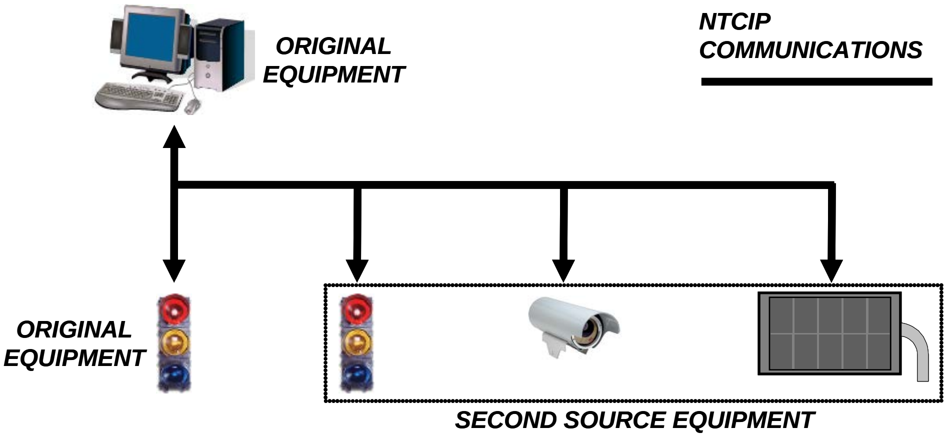


**Figure 1. NTCIP *facilitates* interoperability across transportation field equipment.**

## HOW DOES NTCIP WORK?

NTCIP supports a broad spectrum of applications, devices, and communication media in order to meet the needs of the transportation industry. Before NTCIP can be specified for a project or agency, it is essential to understand how it works to the extent that it allows the proper reference to the group of NTCIP standards. The NTCIP C2F standards are generally divided into three groups: base standards, device standards and profile standards as follows:

- The base standards (numbered 11XX) define general procedures and rules for using NTCIP and specifying data.

- The device standards (numbered 12XX), also known as data dictionaries, define the data and messages, or *what*, to be transmitted to the specific end ITS system or field device. The data and messages of the standard are specified in a Management Information Base (MIB) which is a formal specification of the "language" (data and messages) that devices adhering to the standard use to communicate with central systems.

- The profile standards (numbered 23XX, 22XX and 21XX) define *how* the data and messages are to be transmitted. The profile standards are said to address *compatibility*, that is, the ability of two or more systems or components to exchange information.

Each of the NTCIP standards used for Center-to-Field communications is listed in Table 1. Understanding all three types of these standards is necessary to properly specify a C2F system. If the standard has a commonly used abbreviation, it is included.

**Table 1. Standards used for NTCIP Center-to-Field Communications.**

| Doc # | Document Name (Abbreviated) |
|---|---|
| 1102 | NTCIP Octet Encoding Rules (OER) |
| 1103 | NTCIP Transportation Management Protocols (TMP) |
| 1201 | NTCIP Global Object Definitions (GO) |
| 1202 | NTCIP Object Definitions for Actuated Traffic Signal Controller Units (ASC) |
| 1203 | NTCIP Object Definitions for Dynamic Message Signs (DMS) |
| 1204 | NTCIP Environmental Sensor Station Interface Standard (ESS) |
| 1205 | NTCIP Object Definitions for Closed Circuit Television Camera Control (CCTV) |
| 1206 | NTCIP Object Definitions for Data Collection and Monitoring Devices (DCM) |
| 1207 | NTCIP Object Definitions for Ramp Meter Control Units (RMC) |
| 1208 | NTCIP Object Definitions for Closed Circuit Television Switching (CCTV) |
| 1209 | NTCIP Data Element Definitions for Transportation Sensor Systems (TSS) |
| 1210 | NTCIP Field Management Stations – Part 1: Object Definitions for Signal System Masters (FMS) |
| 1211 | NTCIP Object Definitions for Signal Control and Prioritization (SCP) |
| 1213 | NTCIP Object Definitions for Electrical and Lighting Management Systems (ELMS) |
| 2101 | NTCIP Point to Multi-Point Protocol Using RS-232 Subnetwork Profile |
| 2102 | NTCIP Point to Multi-Point Protocol Using FSK Modem Subnetwork Profile |
| 2103 | NTCIP Point-to-Point Protocol over RS-232 Subnetwork Profile |
| 2104 | NTCIP Ethernet Subnetwork Profile |
| 2201 | NTCIP Transportation Transport Profile |
| 2202 | NTCIP Internet (TCP/IP and UDP/IP) Transport Profile |
| 2301 | NTCIP Simple Transportation Management Framework (STMF) Application Profile |
| 2302 | NTCIP Trivial File Transfer Protocol Application Profile |
| 2303 | NTCIP File Transfer Protocol Application Profile |

NTCIP uses a layered communication architecture adapted from the layering architecture established by the International Organization of Standards (ISO) Open Systems Interconnect (OSI) model. This architecture has been demonstrated to be an effective design for communication software for virtually any media and topology of devices. The OSI model defines seven layers with each layer addressing distinct requirements from the other layers and used together to enable communication to take place between devices. Each layer is independent of the other layers. See www.iso.org (or any of the numerous networking texts or websites available) for a detailed explanation of each OSI layer. NTCIP uses a simplified layering scheme defining five "levels" which can be mapped to the OSI layers as shown in Figure 2. In practice, each level of an NTCIP stack is made up of a group of protocols to address the different communication needs at that level. The NTCIP Working Groups have developed standards for each of the NTCIP levels. The *NTCIP Guide* describes the NTCIP levels as follows:

- NTCIP Information Level – Information level standards define the meaning of data and messages and generally deal with ITS information (rather than information about the communications network). This is similar to defining a dictionary and phrase list within a language. These standards are above the traditional OSI seven-layer model. Information level standards represent the functionality of the system to be implemented.

- NTCIP Application Level – Application level standards define the rules and procedures for exchanging information data. The rules may include definitions of proper grammar and syntax of a single statement, as well as the sequence of allowed statements. This is similar to combining words and phrases to form a sentence, or a complete thought, and defining the rules for greeting each other and exchanging information. These standards are roughly equivalent to the Session, Presentation and Application Layers of the OSI model.

- NTCIP Transport Level – Transport level standards define the rules and procedures for exchanging the Application data between point "A" and point "X" on a network, including any necessary routing, message disassembly/reassembly and network management functions. This is similar to the rules and procedures used by the telephone company to connect two remotely located telephones. Transportation level standards are roughly equivalent to the Transport and Network Layers of the OSI model.

- NTCIP Subnetwork Level – Subnetwork level standards define the rules and procedures for exchanging data between two "adjacent" devices over some communications media. This is equivalent to the rules used by the telephone company to exchange data over a cellular link versus the rules used to exchange data over a twisted pair copper wire. These standards are roughly equivalent to the Data Link and Physical Layers of the OSI model.

- NTCIP Plant Level – The Plant level is shown in the NTCIP Framework only as a means of providing a point of reference to those learning about NTCIP. The Plant level includes the physical communications infrastructure over which NTCIP communications standards are to be used and will have a direct impact on the selection of an appropriate Subnetwork level for use over the selected communications infrastructure. The NTCIP standards do not prescribe any one media type over another.

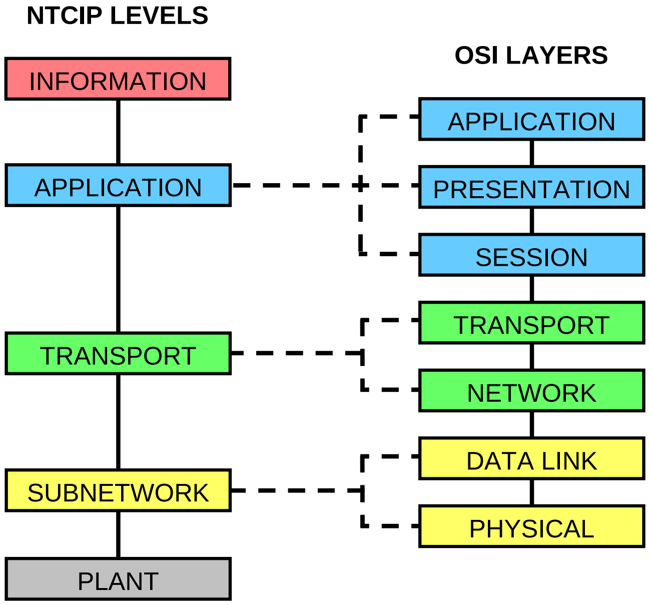


**Figure 2. Mapping of NTCIP Levels and the ISO OSI Layers**

The specific protocol or protocols chosen for a particular level of a stack will depend upon the application being performed, the type and frequency of the communications desired, and the communications infrastructure being used in the deployment. Figure 3 is an annotated diagram showing the various protocols which are used with NTCIP Center-to-Field communication stacks. The numbers next to the protocol represent the document number of the NTCIP communication standard that describes it. The protocols are shown at their applicable levels with lines that identify the most common connections to protocols in the adjacent levels. Not all possible stacks are indicated but those depicted are most common. Users should be aware that network media in C2F communications are not always used in the same fashion as that of common IT networks. For instance, although fiber and coax are commonly used for network communications, it is not uncommon to find a C2F implementation using these media in a serial manner. The protocols are summarized below:

- Simple Network Management Protocol (SNMP) is a communication protocol widely used in computer networks for managing network devices. For transportation communications, it the essential protocol used by all NTCIP compliant field devices. SNMP uses a client-server communications model where the central computer acts as the client and the field devices act as servers. The client uses four types of messages: "Set," "Get," "Get Next," and "Trap" to configure, control and monitor data elements in the field devices. SNMP uses ASN.1 notation to specify and encode data elements in a MIB for each compliant field device. A copy of the field device's MIB is on the central system so that the central system may access the field device appropriately.

- Simple Transportation Management Protocol (STMP) is an extension of SNMP in which the central system and the field device dynamically establish composite messages (typically when they are first connected) made up of a set of the field device data elements. The composite messages are still sent using SNMP but with greatly reduced overhead over sending the data elements individually. STMP is ideal for low-bandwidth communication media such as 9600 serial communication.

- File Transfer Protocol (FTP) is a widely used protocol to exchange files between computing devices. It uses the Transmission Control Protocol (TCP).

- Trivial File Transfer Protocol (TFTP) is a protocol used to exchange file between computing devices. It is less capable than FTP. TFTP uses the User Datagram Protocol (UDP).

- TCP/IP is made up of two protocols, Transmission Control Protocol (TCP) and Internet Protocol (IP). TCP/IP is most widely used protocol for internet communications. It is used for routed networks that require a reliable protocol. A reliable protocol, in this context, means that the protocol attempts to detect and recover from transmission errors. It should be noted that the additional reliability also results in reduced efficiency due to the overhead within the packet and more processing required. SNMP performs error handling at the application level making UDP/IP sufficient for most NTCIP applications that use routed networks.

- UDP/IP is made up of two protocols, User Datagram Protocol (UDP) and Internet Protocol (IP). UDP/IP is used for routed networks that do not require a reliable protocol (aka non-reliable). A non-reliable protocol, in this context, means that the protocol does not make any attempt to detect or recover from transmission errors. Any detection and error recovery must be done at a higher layer. Because of this, UDP/IP communications are more efficient than TCP/IP due to reduced overhead and processing requirements. UDP/IP is recommended for NTCIP in routed networks unless the application explicitly requires it.

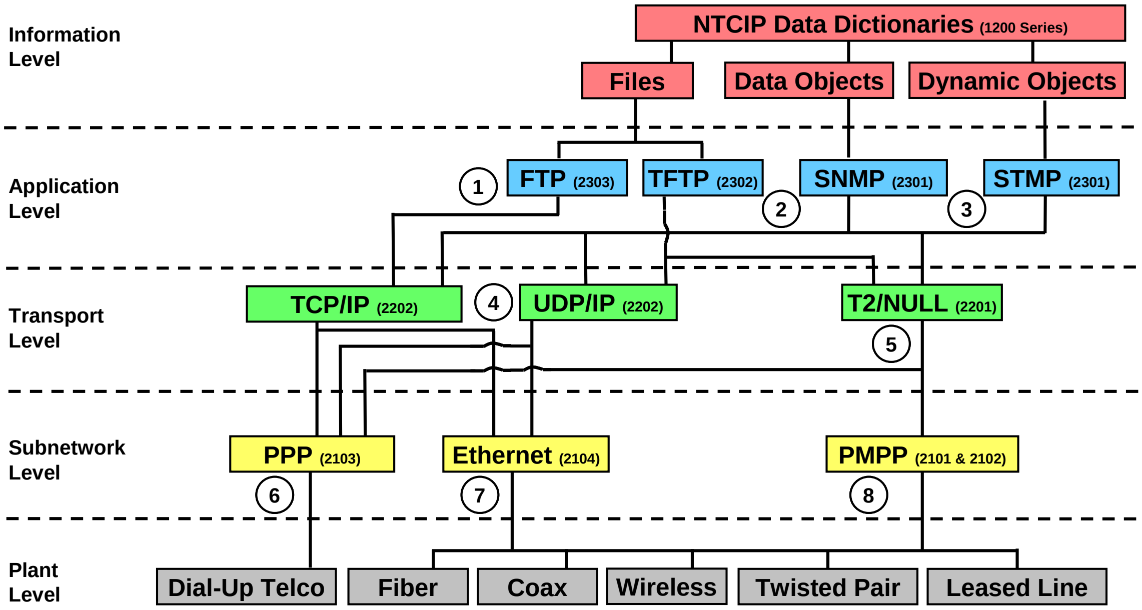
- T2/NULL is a non-routed serial communication protocol. T2/Null provides multiplexing on a single serial channel and works with half or full duplex.

- Ethernet is a protocol that provides for a connectionless and connection-oriented data link service and the physical interface between an end system and other compatible end systems. It has specific reference when these services are used through the Internet Protocol (IP) connectionless network service. "Ethernet" is somewhat of a misnomer. More precisely, NTCIP network-type communications are based on IEEE 802 family of network communications standards which are similar to Ethernet but also include Logical Link Control (LLC) and Media Access Control (MAC) layers.

- Point-to-Point Protocol (PPP) is a protocol that operates in a point-to-point configuration where exactly two devices (called peers) are connected by a communications link. PPP is intended to provide an interoperability standard for transportation related devices for dialed-up circuits using V Series Modems.

- Point-to-Multipoint Protocol (PMPP) is a protocol that operates in a primary/secondary configuration where one device is the designated primary and other devices on the communication channel act as secondaries. PMPP is intended to provide an interoperability standard for transportation related devices using FSK (frequency shift keying) modems.

Figure 4 identifies one example of a C2F communication stack. It depicts a stack that could be used for a C2F infrastructure of copper wire. The highlighted standards would be used to specify the standards that describe the appropriate software stack for the central system and field equipment. Note that for communications to take place, the appropriate protocols required for the particular deployment must be supported by the equipment initiating and receiving the message. How to insure this is covered in the next section.



Notes:
1) FTP is used over TCP/IP protocol.
2) TFTP is used over UDP/IP or T2/NULL protocols.
3) SNMP & STMP are used over TCP/IP, UDP/IP or T2/NULL.
4) TCP/IP & UDP/IP are used over Ethernet or PPP protocols.
5) T2/NULL is used over PMPP and PPP protocols.
6) PPP is used with Dial-Up Telephone lines.
7) Ethernet is used over almost any medium.
8) PMPP is mainly used with Twisted Pair copper wire, Leased Line and some Wireless media. It is occasionally used with Fiber or Coax.

**Figure 3. Common NTCIP Center-to-Field communications stacks.**

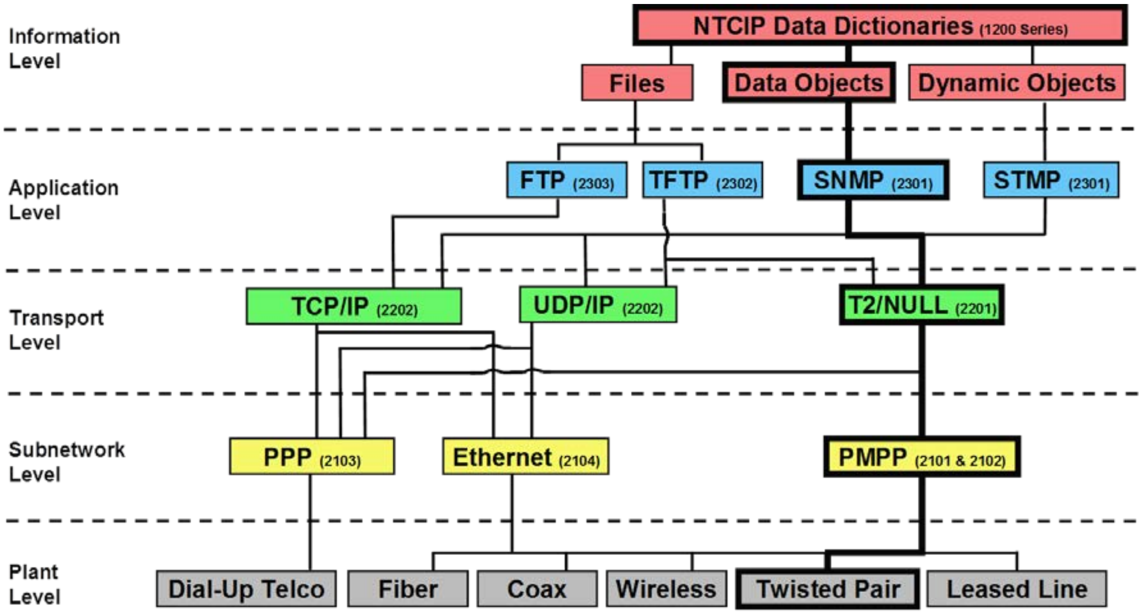


**Figure 4. Example of a NTCIP Center-to-Field communication stack (highlighted portion represents the stack).**

## HOW IS NTCIP SPECIFIED?

In reality, specifying a system can be an arduous task. Depending on the size and extent of the endeavor, a specification (agency specification, request for proposal or the like) may include:

a) physical requirements such as construction, durability, adaptability and environmental requirements;
b) performance requirements;
c) security requirements;
d) requirements for information management;
e) operational requirements such as human factors, maintainability and reliability;
f) policy and regulation requirements;
g) internal and external system interface requirements both human and other systems;
h) capability requirements; and
i) other requirements.

It is important for a specification development to use a systems engineering process to insure that the specification formally identifies the user needs of the system and that there are testable requirements associated to each user need that can be used to verify compliance by equipment suppliers, software vendors and system integrators. Users are directed to the *Systems Engineering Guidebook for ITS Version 2.0*, *IEEE Standard 1233-1998 IEEE Guide for Developing System Requirements Specifications*, *International Council on Systems Engineering (INCOSE) Systems Engineering Handbook Version 3.1*, and the *NTCIP Guide Version 4* for more information on the systems engineering process and suggested document outlines.

Specifying NTCIP cannot be done using a simple compliance requirement such as, "It shall be NTCIP compliant." It takes a collection of references including the device standards to be supported and the profile standards for the communications infrastructure. It also requires the specification of the scenarios, message definitions and dialogs of data that are used to perform the functional operations of the system. It should be noted that the device standards not only specify the data elements and messages but also specify the application level protocols that the device may use. Table 2 indicates the device standard and their associated application protocols. The steps which follow can be used to build the NTCIP requirements for a system specification.

**Table 2. Device standards and their associated Application Level protocols.**

| Doc # | Document Name (Abbreviated) | SNMP | STMP | FTP | TFTP |
|---|---|---|---|---|---|
| 1201 | NTCIP Global Object (GO) Definitions | X | | | |
| 1202 | NTCIP Object Definitions for Actuated Traffic Signal Controller Units | X | X | | |
| 1203 | NTCIP Object Definitions for Dynamic Message Signs (DMS) | X | | | |
| 1204 | NTCIP Environmental Sensor Station Interface Standard | X | | X | |
| 1205 | NTCIP Object Definitions for Closed Circuit Television (CCTV) Camera Control | X | | | |
| 1206 | NTCIP Object Definitions for Data Collection and Monitoring (DCM) Devices | X | | X | X |
| 1207 | NTCIP Object Definitions for Ramp Meter Control (RMC) Units | X | | | |
| 1208 | NTCIP Object Definitions for Closed Circuit Television (CCTV) Switching | X | | | |
| 1209 | NTCIP Data Element Definitions for Transportation Sensor Systems | X | | X | |
| 1210 | NTCIP Field Management Stations – Part 1: Object Definitions for Signal System Masters | X | | | |
| 1211 | NTCIP Object Definitions for Signal Control and Prioritization | X | | | |
| 1213 | NTCIP Object Definitions for Electrical and Lighting Management Systems (ELMS) | X | | | |

1) Based on the transportation field equipment identified for the system, select the applicable device standards in Table 2 to be used.

2) Based on the system requirements, determine what information is to be exchanged and the rate in which it will be exchanged.

   The device standards may contain conformance groups, a Protocol Requirements List (PRL) or a Profile Implementation Conformance Statement (PICS) to help users select the data that they wish to be exchange between their field devices and their central system. The use of "profile" here means "set" or "collection." It should not to be confused with the profile standards. For a description of these tools see the device standards listed.

In formulating requirements for the system, it is important to be specific concerning the data elements and rate of that data as this can influence what NTCIP protocols are used and be the basis of system acceptance testing. It should be noted that users may require vendors to demonstrate that proposed devices meet the entire MIB specified in a standard. This is still no substitute for the detailed specification of the data to be exchanged based on the system requirements.

3) Determine the NTCIP profiles that are required.

It can be assumed that the communication infrastructure is already been established or, at least, proposed. It is typically in place before a system specification is written and, consequently, usually represents a constraint on the system. It is also typical for there to be multiple communications media used in a single system deployment. For example, a traffic control system may use fiber optics to communicate to some field equipment and use dial-up telephone lines to communicate with others.

The flowchart in Figure 5 can now be used to determine the NTCIP profile standards to be used in the specification. It assumed that the appropriate devices standards are known, the communications infrastructure is known, and the common NTCIP C2F communication stacks in Figure 3 are to be used. The flowchart requires that the specification developer make certain decisions in order to determine the most appropriate NTCIP profiles to use for a particular communications media and field device. The numbered decision points in the flowchart are described as below:

[1] *Device Uses Ethernet?* – Is the primary communications port on the device an RJ-45 connector? If the answer is YES, it should be verified that the device is not using an internal terminal server, which could accept an Ethernet data packet, but internally strips the Ethernet header/footer to deliver a serial data packet to the field device application.

[2] *Device Uses Serial?* – If the answer to the first question (Ethernet) is NO, the device uses either a serial interface, a dial-up interface, or a non-NTCIP defined interface. If the device is supposed to conform to NTCIP, the answer is YES. If the device is something different, the answer to this question is NO.

[3] *Using Dial-Up?* – If the answer to the second question (Serial) is YES, the device uses either a serial interface or a dial-up interface. If the device uses an RS-232 interface, it is likely that the answer is NO. If the device has an internal dial-up modem or connects to an external dial-up modem the answer to this question is YES.

[4] *FSK Modem?* – If the interface to the device is serial, the user has to decide whether an FSK modem (also known as Bell 202) is to be used. Note that even though an external FSK modem, which typically contains a regular RS-232 port into the device,

is to be used, a user could decide to answer this question with NO. If external FSK modems are used on both ends, the result would be the same. It is a matter where NTCIP compliance is measured, on the outside or the inside of the external FSK modem.

[5] *File Transfer Required?* – There is currently no NTCIP-compliant device type that solely operates using a file transfer mechanism. Table 2 identifies the NTCIP field devices that use file transfers. It is suggested that agencies deploying a system ask the central system developer and field device vendors to determine if their particular system will require file transfers. If file transfers are required, the answer is YES, otherwise, the answer is NO.

[6] *Ack (Acknowledgement) Required?* – A decision has to be made whether UDP/IP or TCP/IP is to be supported. The answer to this question is YES, if the file transfer protocol is FTP. The answer is NO, if TFTP is to be supported. FTP is more commonly used but it requires more communication bandwidth and more processing capabilities. If neither FTP nor TFTP are required, either TCP or UDP may be used. However, it is recommended that UDP be used due to the improved efficiency.

[7] *STMP Required?* – STMP is a protocol that is only supported by Actuated Signal Control (ASC) devices at this time. The need to use STMP in these deployments is based on bandwidth requirements of the system and the media being used.

The flowchart should be exercised for each type of field device and media on the system. The use of terminal servers or other devices to extend or convert to alternate media are not covered. In most cases, the use of terminal servers is an innocuous wrapping and unwrapping of the NTCIP messages in protocols outside the scope of NTCIP.

4) Perform a bandwidth analysis.

Bandwidth is the maximum amount of information (usually measured in bits per second (bps)) that can be sent over a communication channel. Each channel of the system's communications infrastructure will have a maximum bandwidth that it can support (also called "capacity"). To verify that the NTCIP system being specified is feasible, the maximum bandwidth required by the system (also called "load") must be computed for each communication channel. The bandwidth required by the system can be computed based on the size of the data elements being used, the frequency of exchange, the protocols used, and the message dialogs that are taking place on the channel. The reader is referred to the *NTCIP Guide Version 4*, Appendix E. If the load exceeds tolerable portions of the available capacity some adjustment to the communications requirements may be necessary. It should be noted that it is generally accepted practice for systems on routed networks not to exceed half the capacity (Ex. On a 10Mbps Ethernet only 5 Mbps should be used).

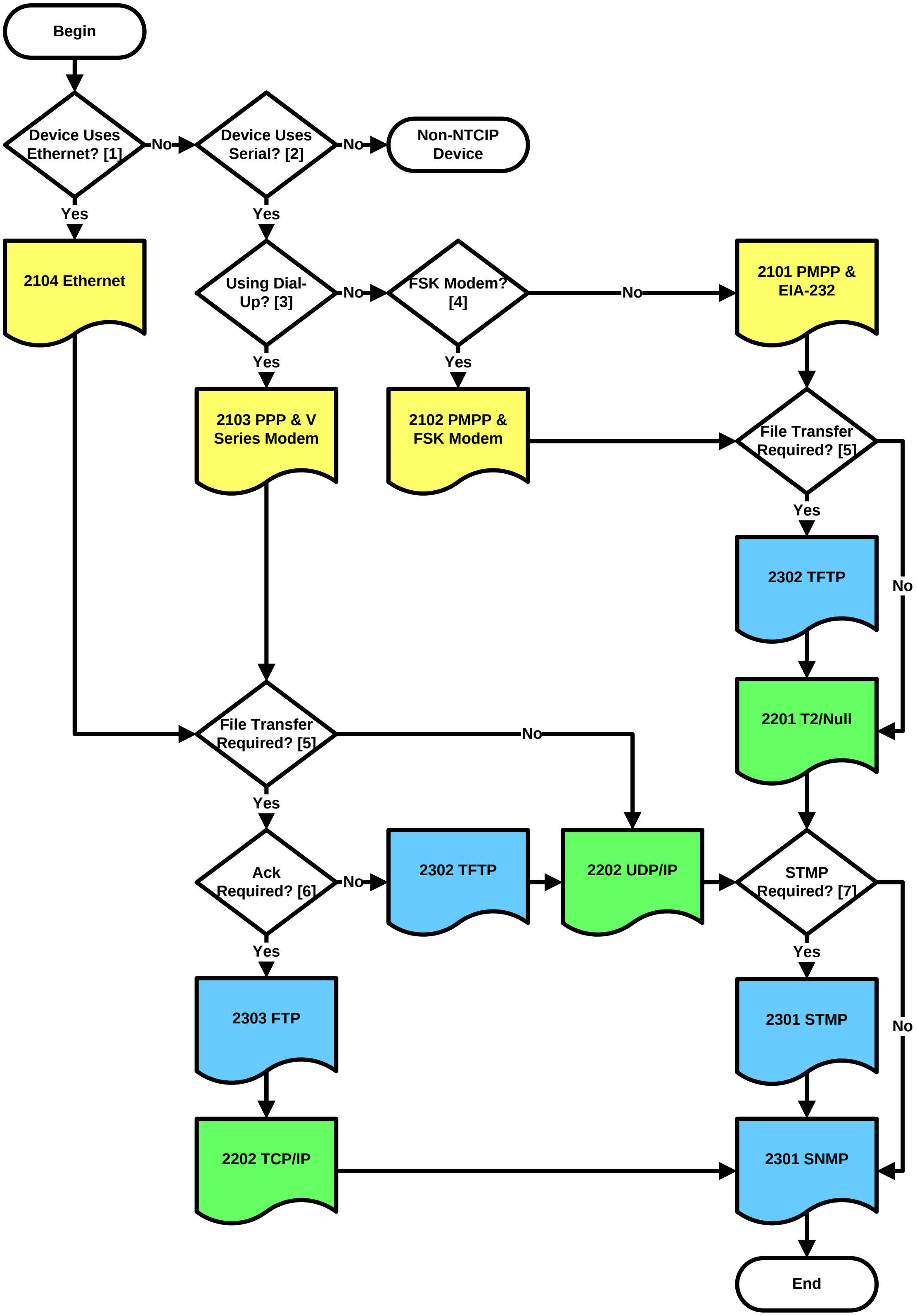


**Figure 5. NTCIP profile selection flowchart.**

## HOW IS NTCIP TESTED?

The guidance here is a general approach to testing. The *NTCIP Guide Version 4*, Section 7, has a brief discussion on testing using the *IEEE Standard 829 IEEE Standard for Software Test Documentation*. It is suggested that testing be in three stages: unit testing, integration testing, and operational testing.

The focus of unit testing is to compare the NTCIP implementation on the device to that defined by the user in the specification. This may be the entire MIB of the applicable device standard or a MIB specifically defined by the user. A vendor may provide a device that may have a MIB that is broader than required but care should be taken that the MIB of the device, in fact, is a superset of the MIB in the specification. See also the section on "Lessons Learned" below. There are several reliable off-the-shelf tools that can be used to perform unit tests. They typically involve a personal computer directly connected to the device. It should be noted that unit testing does not test the functionality of the device but only the adherence to NTCIP and the specific MIB being used. Unit testing is usually performed during a vendor qualification process so that it is not necessary to test every unit in this fashion once it has been established that the device and software version has been qualified.

Integration testing has to do with connecting the central system to the field device to make sure that the central system and the device work together according to the functional requirements. This type of testing is still performed in some sort of test environment or facility. Initially, the purpose here is to isolate the testing to the exchange of information between the central system and the device without clouding the test with infrastructure issues. A robust exercise of the devices should be performed via the central system to the extent possible. It is also an opportunity to exercise multiple qualified devices and those from different vendors simultaneously. Performance differences should be noted. Integration testing also tests the central system's NTCIP implementation. It is typical for software bugs to be exposed during this activity. Good integration testing can save considerable time and money by identifying issues before the devices are installed in the field.

System testing requires the testing of the central system and devices using the actual system communication infrastructure under real-world conditions. This includes the communications equipment such as modems, switches, routers, the various media that is to be used, etc. It is recommended that a system test be performed for a period of time on a very limited scale before proceeding with a complete deployment. It often takes time for aberrant behavior to occur.

## WHAT ARE THE LESSONS LEARNED?

While there are many lessons learned from the deployments of NTCIP, this section will highlight two: 1) interoperability and interchangeability and 2) MIB ownership or rights.

1) Interoperability and interchangeability are two concepts that can be confused in NTCIP discussions. As stated earlier, *interoperability* is defined as the ability of two or more devices to exchange information and use the information that has been exchanged. *Interchangeability* is defined as the capability to exchange devices of the same type on the

same communications channel and have those devices interact with other devices of the same type using standard functions.

As stated in the previous section, a device may have a MIB that is broader than asked for in a specification. It may use what is called "proprietary" data elements that are only supported by one manufacturer. If proprietary data elements are used in a C2F deployment it can a) make interoperability with other equipment on the same communication channel difficult and b) make interchangeability with like devices (from different vendors) on the same channel impossible. In past C2F deployments, proprietary data elements have been used simply because the users were unaware of the issues relating to proprietary data elements or because they had a custom operation they wished to trigger in a field device. Users need to consider that they may be losing interoperability or interchangeability should proprietary data elements be used. In regards to a custom operation, users should consider methods of performing the same or similar operation using standard NTCIP data elements instead of the proprietary ones.

2) The MIB is the key to communicating to an NTCIP-capable device. If an agency does not have the rights to a device's MIB after its initial installation, they may not be able to communicate to the device should a new NTCIP central system be installed later. Therefore, agencies should require that vendors supply the complete MIB of the device they purchase electronically in ASCII format. The agencies should also require that they have rights to distribute and use the MIB in the future.

## REFERENCES

*IEEE Guide for Developing System Requirements Specifications*, IEEE Std 1233-1998. Available from the Institute of Electrical and Electronics Engineers.

*IEEE Standard for Software Test Documentation*, IEEE Std 829-1998. Available from the Institute of Electrical and Electronics Engineers.

*INCOSE Systems Engineering Handbook Version 3.1*, INCOSE-TP-2003-002-03.1, August 2007. Available from the International Council on Systems Engineering.

*Systems Engineering Guidebook for ITS Version 2.0*, FHWA, 2 January 2007. Available from the Federal Highway Administration, California Division.

*National Transportation Communications For ITS Protocol NTCIP Guide Version 04.04*, NTCIP Joint Committee, 30 October 2008. Available from www.ntcip.org.

## ACKNOWLEDGEMENTS

Special appreciation is expressed for the NTCIP Base Standards and Protocols (BSP) Working Group (WG) for developing the protocol selection flow chart and updating the NTCIP protocol information that was source material for this paper and for the NTCIP Guide Version 4. Appreciation is also expressed to Bruce Schopp, Manager, Transportation Systems, of the

National Electrical Manufacturers Association (NEMA), for his review and comment on this paper.

## AUTHOR INFORMATION

Ralph W. Boaz
President
Pillar Consulting, Inc.
4511 Jicarillo Avenue
San Diego, CA 92117
858-352-6281
rboaz@pillarinc.com