A Recommended Information Report of the Joint Committee on the NTCIP

NTCIP 9001

National Transportation Communications for ITS Protocol

The NTCIP **Guide**

... updated version 3

Published by

American Association of State Highway and Transportation Officials (AASHTO)
444 North Capitol Street, N.W., Suite 249
Washington, D.C. 20001

Institute of Transportation Engineers (ITE)
1099 14th Street, N.W., Suite 300 West
Washington, D.C. 20005-3438

National Electrical Manufacturers Association (NEMA)
1300 North 17th Street, Suite 1847
Rosslyn, Virginia 22209-3801

v03.02b, October 2002

Inquires, comments, and proposed revisions should be submitted to:

NTCIP Coordinator
National Electrical Manufacturers Association
1300 North 17th Street, Suite 1847
Rosslyn, Virginia 22209-3801
fax: (703) 841-3331

e-mail: ntcip@nema.org

History

From 1996 to 1999, this document was referenced as the "NTCIP Guide." However, to provide an organized numbering scheme for the NTCIP documents, this document is now referenced as NTCIP 9001. The revisions and acceptance are noted in the development history below:

NTCIP Guide revision 1, February 1997. Written and edited by the Joint Committee on the NTCIP.

NTCIP 9001 v02.05, September 1999. New version prepared by project team. July 1999 – Accepted as a draft information report by the Joint Committee on the NTCIP. Spring 2000 – Prepublication draft v02.06 available.

NTCIP 9001 v03.02, October 2002. New version prepared by project team. October 2002 -- Accepted as a recommended information report by the Joint Committee on the NTCIP.

Acknowledgements

The NTCIP development effort is guided by the Joint Committee on the NTCIP, which has six representatives each from the American Association of State Highway and Transportation Officials (AASHTO), the Institute of Transportation Engineers (ITE) and the National Electrical Manufacturers Association (NEMA). This *NTCIP Guide* is one of the many NTCIP publications developed with assistance from the FHWA.

Members of the Joint Committee on the NTCIP include:

- Craig Anderson
- Jerry Bloodgood
- Steve Dellenback
- Richard Denney, Jr.
- Robert DeRoche
- Gary Duncan
- Michael Forbis
- Lap Hoang
- Mark Hudgins
- Jeff McRae
- Raman Patel
- Ed Roberts
- Ed Seymour
- Ray Starr
- Issac Takyi
- Warren Tighe
- Ken Vaughn

The first edition of *The NTCIP Guide* was prepared in February 1997. Version 02 of *The NTCIP Guide, NTCIP 9001,* was prepared in July 1999 and minor revisions were made to the publication through January 2001. *The NTCIP Guide* Project Team has updated *The NTCIP Guide, NTCIP 9001* to version 03 under the direction of the Joint Committee on the NTCIP and input from a peer review team selected for this project.

The following individuals were members of *The NTCIP Guide* version 03 Project Team:

- G. Curtis Herrick, Project Manager and Editor-In-Chief
- Robert De Roche, Principal Author
- Kenneth Vaughn, Principal Author
- Warren Tighe, Principal Author
- Joerg (Nu) Rosenbohm, Principal Author
- Paul Olson, Principal Author
- Scott Turner, Technical Editor
- Ed Seymour, Project Advisor
- Raman Patel, Project Advisor

Other individuals providing peer review and input to the publication include:

- John Corbin
- Don Creighton
- Arthur Dock
- David Holstein
- Galen McGill
- Robert Rausch
- Joe Stapleton
- Thomas Urbanik II

In addition to the many volunteer efforts, recognition is also given to those organizations that supported the efforts of *The NTCIP Guide* update by providing guidance, comments, and funding for the effort:

- Battelle Memorial Institute
- Bi Tran Systems
- California Department of Transportation
- City of Atlanta, Georgia
- City of Mesa, Arizona
- Eagle Traffic Control Systems, Inc.
- Econolite Control Products, Inc.
- Florida Department of Transportation
- Federal Highway Administration
- Gardner Transportation Systems Business Unit of Siemens Energy & Automation, Inc.
- G. C. Herrick & Associates, Inc.
- Georgia Department of Transportation
- Image Sensing Systems, Inc.
- Minnesota Department of Transportation
- New York City Transit Authority
- New York Department of Transportation
- Iteris, Inc.
- Ohio Department of Transportation
- Ontario Ministry of Transportation
- Oregon Department of Transportation
- P. B. Farradyne, Inc.
- Peek Traffic Systems, Inc.
- Robert DeRoche Consulting
- Southwest Research Institute
- Texas Department of Transportation
- Texas Transportation Institute
- Trevilon Corp.
- TransCore, Inc.
- University of Tennessee
- Virginia Department of Transportation
- Washington State Department of Transportation
- Wisconsin Department of Transportation

Contents

List of Exhibits

List of Sidebars

THIS PAGE LEFT INTENTIONALLY BLANK

Chapter 1

Foreword

The National Transportation Communications for ITS Protocol (NTCIP) family of standards defines protocols and profiles that are open, consensus-based data communications standards. When used for the remote control of roadside and other transportation management devices, the NTCIP-based devices and software can help achieve interoperability and interchangeability.

Why are NTCIP standards needed? How are NTCIP standards used? What is interoperability and interchangeability?

The NTCIP Guide will explain these terms, and give you the *why* and the *how* to use NTCIP standards in your products and systems.

The transportation industry has a history of unique data definitions and proprietary communications protocols. Devices and systems from one manufacturer or developer tended not to interoperate with those of other manufacturers or developers. All too often, agencies were faced with having to deploy separate systems and communications for each manufacturer and each device type. Now, the NTCIP makes possible the interoperability of transportation systems and interchangeability of devices using standardized feature sets.

1.1 When to Use The NTCIP Guide

It is well understood that the NTCIP standards publications are often difficult to read due to the need for technical precision, accuracy and completeness in standards publications. Additionally, it needs to be understood that most of the NTCIP publications are standards and not functional specifications. NTCIP standards define data communications protocols and profiles that enable implementations to interact and achieve the desired functionality.

The NTCIP Guide is an educational tool, created to assist decision makers, planners, specification writers, and implementers in understanding the various NTCIP standard publications and how to use them. *The NTCIP Guide* also explains the motivations behind the use of NTCIP. *The NTCIP Guide* is an informative NTCIP publication, but it is not an NTCIP standard and must therefore not be considered binding.

The NTCIP family of standards is comprised of numerous standalone publications, some have been fully approved, some are in the approval process, and some of which are still being drafted. Further, as the application of NTCIP continues to grow in the transportation community, the need will arise for additional NTCIP standards. As a result, *The NTCIP Guide* will be out of sync with the actual standards publications. The reader should understand that, in writing specifications or implementing systems, only the actual NTCIP standards govern and take precedence, not *The NTCIP Guide*. For updated information on NTCIP standards publications, please see the NTCIP website at www.ntcip.org/.

1.1.1 Purpose of *The NTCIP Guide*

The transportation community has long needed transportation systems that could be built using devices and components that were interchangeable and interoperable. It is for this reason that the NTCIP family of protocols is being widely embraced and specified in many new system deployments.

The term interoperability reflects the ability of multiple devices, often of different types, to seamlessly work together as a single system for the same purpose. An example of interoperability is, signal controllers and dynamic message signs sharing a single communications channel in the case of center-to-field communications.

Interchangeability is defined as the capability to exchange devices of the same type on the same communications channel and have those devices interact with others devices of the same type using standards-based functions. An example of interchangeability is a signal controller from different manufacturers interacting with each other to provide traffic signal coordination along an arterial throughway.

The subject of communications protocols and standards is a challenging one, even for engineers experienced in these topics. In the case of NTCIP, the level of difficulty is heightened by the fact that NTCIP is an entire family of standards designed to meet the communications needs of various fixed-asset roadside devices and traffic management centers. *The NTCIP Guide* is an educational tool that has been created to assist decision makers, planners, specification writers, and implementers understand the various NTCIP standards and how to use them.

1.2 Organization of *The NTCIP Guide*

The NTCIP Guide is divided into 10 chapters, with five of these chapters aimed at serving the needs of specific audience groups. The remaining chapters organize supporting information.

The *Executive Summary* is intended for decision makers. This chapter provides a brief overview of the NTCIP as well as a discussion of the motivations behind the use of these approaches, cast largely in the context of the National ITS Architecture. It also discusses the issues associated with NTCIP use, as well as required resources, testing and configuration management issues.

The *Understanding NTCIP* chapter is intended principally for systems planners, though it is also a general purpose technical overview of the issues associated with the use of NTCIP. It's a good starting point for anyone wishing to become better informed on the various technical aspects of the approach.

The *Procuring NTCIP* chapter is intended principally for specification writers. As the NTCIP standards consists of many publications, and many have numerous optional requirements, it is important that specification writers have a good grasp of the decision process by which these various options will be selected for any given planned deployment. Satisfying the user agency in an NTCIP deployment requires a careful analysis of the agency's requirements up front, and then a careful mapping of the various NTCIP options to those requirements by way of a well-written procurement specification. Further, this chapter describes the need for, and a means by which, the technical requirements of the communications infrastructure can be determined.

The *Designing NTCIP* chapter is intended principally for those faced with the task of designing the communications element of transportation systems that utilize NTCIP protocols. This section includes a detailed discussion on bandwidth analysis and system timing.

The *Implementing NTCIP* chapter is intended for systems implementers. This includes software and hardware developers for field equipment, traffic management center software and hardware developers and systems integrators. Because authors of *The NTCIP Guide* included of software and hardware developers and integrators, this section provides the necessary "read between the lines" type of insight often required to achieve successful deployments. In particular, some of the lessons learned and common pitfalls encountered during actual deployments will be discussed, with suggested solutions.

The remaining chapters provide a list of terms, abbreviations, acronyms and definitions. A partial list of NTCIP standards is also provided. Examples of NTCIP standards framework selections are shown for some applications of center-to-field and center-to-center communications.

1.3 Where to Purchase Published Standards

NTCIP standards are available from the following sources:

National Electrical Manufacturers Association
Published standards are available for purchase through the NEMA Website from Global Engineering Documents at www.nema.org/ or ordered directly from Global Engineering Documents by calling (800) 854-7179 or (303) 397-7956.

Institute of Transportation Engineers
Published standards are available for purchase directly from ITE at www.ite.org/ or by calling (202) 289-0222 ext. 130.

Draft standards, revisions, and amendment status may be found in the NTCIP Library on the NTCIP Website at www.ntcip.org/.

1.4 Where to Find Additional Information

More information about NTCIP standards can be found on the NTCIP Website at www.ntcip.org/. Those without access to the World Wide Web may contact:

NTCIP Coordinator
National Electrical Manufacturers Association
1300 N.17th Street, Suite 1847
Rosslyn, Virginia 22209-3801
fax: (703) 841-3331
e-mail: ntcip@nema.org/

NTCIP standards are developed with input from users and other interested parties. Such input was also sought and evaluated for the development of The NTCIP Guide. Anyone interested in making written inquiries, comments, and proposed or recommended revisions should submit them to the NTCIP Coordinator at the above address. Please include the following information in your correspondence:

Document Name:
Version Number:
Section Number:
Paragraph:
Comment:
Your Name:
Your Address:
Your Organization

Chapter 2

Executive Summary

2.1 Introduction

A communications protocol is a set of rules for how messages and data elements are coded and transmitted between electronic devices. The equipment at each end of a data transmission must use the same protocol to successfully communicate. The protocol is very much like human languages that have an alphabet, vocabulary and grammar rules used by everyone speaking that language.

Historically, each manufacturer of microcomputer control devices and software used in management systems either developed or adopted a different, proprietary protocol for data communications. This required extensive integration projects to mix equipment and software from different manufacturers in the same system and to communicate between systems operated by adjacent agencies. The NTCIP provides common standards for protocols that can be used by all manufacturers and system developers to help overcome these differences.

NTCIP is a family of communications standards for transmitting data and messages between microcomputer control devices used in Intelligent Transportation Systems (ITS). An example of such a system is a computer at city hall monitoring and controlling the operation of microprocessor-based roadside controllers at traffic signals within a city. The computer may send instructions to the traffic signal controllers to change signal timings as traffic conditions change and the intersection controllers send status and traffic flow information to the computer.

In another example, two transit management system computers may need to exchange real-time information about the location of transit vehicles bound for a shared timed-transfer center. This allows each system to know instantly when one vehicle is running significantly behind schedule and is unable to make the scheduled transfer time. Passengers could be notified automatically, and the local traffic management center could be automatically requested to provide priority at traffic signals for the delayed transit vehicle.

The family of NTCIP standards is intended for use in all types of management systems dealing with the transportation environment, including those for freeways, traffic signals, transit, emergency management, traveler information and data archiving. NTCIP is intended for wire-line or some wireless communications between computers in different

systems or different management centers, and between a computer and devices at the roadside. As of 2002, the NTCIP standards are not intended for use in devices owned by individual travelers or for wireless broadcast communications; other standards either currently exist or are in development for those purposes.

2.2 NTCIP Handles C2F and C2C

NTCIP provides communications standards for two different types of ITS communications. The first type is between a management system or center and multiple control or monitoring devices managed by that system or center. Examples of this type of communications include:

- A traffic signal management system communicating with traffic signal controllers at intersections;
- A transit management system communicating with monitoring devices and passenger information signs on transit vehicles and at transit stations and stops;
- A freeway management system communicating with detectors and ramp meters on freeways; and
- A traffic management system controlling CCTV cameras, dynamic message signs, advisory radio transmitters, environmental sensors and traffic count stations on roadways.

Since most applications of this type involve a computer at a management center communicating with various devices at the roadside or on agency vehicles, this type is referred to as center-to-field (C2F) communications. The NTCIP protocols intended for this communications application are often used in an environment where a central management station routinely polls each field device, as in the most common case of multiple field devices sharing a communications channel.

The second type of communication involves messages sent between two or more central management systems. Examples of this type of communication include:

- Two or more traffic signal management systems exchanging information (including second-by-second status changes) to achieve coordinated operation of traffic signals managed by the different systems and to enable personnel at one center to monitor the status of signals operated from another center;
- A transit system reporting schedule adherence exceptions to kiosks, to a transit customer information system and to a regional traveler information system, while also asking a traffic signal management system to instruct its signals to give priority to a behind-schedule transit vehicle;

- An emergency management system reporting an incident to a freeway management system, to a traffic signal management system, to two transit management systems and to a traveler information system;
- A freeway management system informing an emergency management system of a warning message just posted on a dynamic message sign on the freeway in response to its notification of an incident; and
- A weather monitoring system informing a freeway management system of ice forming on the roadway so that the freeway management system is able to post appropriate warning messages on dynamic message signs.

This type of communication is referred to as center-to-center (C2C) communications, although two or more of the various systems may in fact be located within the same "center" or building – they are logically separate. C2C involves peer-to-peer communications between any number of system computers in a many-to-many network. This type of communication is similar to the Internet, in that any center can request information from, or provide information to, any number of other centers. It is possible, though not yet common, to use such protocols for communication to and between field devices, as well as between computers.

Although both C2F and C2C communications can involve a human operator making requests or issuing instructions, one of the features of the NTCIP protocols is their support for continuous, automated functionality using pre-defined data transmissions with no human in the loop.

2.3 What is NTCIP?

NTCIP is a family of communications protocols and data definition standards that have been designed to accommodate the diverse needs of various subsystems and user services of the National ITS Architecture. NTCIP standards are intended to handle these needs in the two areas of C2F and C2C.

NTCIP differs from the past practice of transportation management protocols in that it is not a single communications protocol designed for one purpose. Rather, the NTCIP consists of a whole family of protocols covering the spectrum from simple Point-to-Point command/response protocols to quite sophisticated object oriented techniques. This is because of several reasons: the diversity of the applications into which NTCIP will be deployed, the resulting diversity of application specific characteristics such as type and quantity of data to be transferred, the criticality of data transfer times, acceptable cost of communications infrastructure, and the criticality of data security and integrity issues.

"NTCIP is a family of communications protocols and data definition standards …"

Starting in 2001, the NTCIP Joint Committee began adding several improvements to some of the standards:

- A concept of operations under which the defined data definitions are to be used.
- Precise definitions of the sequences in which certain data definitions are to be exchanged (dialogs) are being added. Examples of these dialogs include:
  - ❖ Standardized data elements pertaining to the definition of a phase within a signal controller must be set simultaneously to avoid using incomplete or wrong definitions, and
  - ❖ A text message to be displayed on a dynamic message sign must first be stored in the DMS controllers message table, and then verified before the message can be displayed on the sign.

2.4 Why Do We Need NTCIP?

Historically, there have been numerous problems associated with the deployments of management systems. Before describing some of these issues we will first define two terms. The terms interoperability and interchangeability generally reflect the ability to use multiple brands of a device on the same communications channel, along with the ability to swap them out. For example, the ability to put any brand of NTCIP-conformant traffic signal controller in the same system at the same time reflects interchangeability for that device type. The term interoperability reflects the ability of multiple devices, often of different types, to seamlessly work together as a single system for some common purpose. For example, using the same communications channel to interconnect a management system with traffic signal controllers, dynamic message signs, video surveillance controls and other devices reflects a real-world example of interoperability. Interoperability and interchangeability are two key goals of the NTCIP open-standards effort.

"…we will first define two terms. The terms interoperability and interchangeability…"

Historically, one problem commonly encountered results from the use of proprietary communications protocols. These protocols are often specific to the given project, as well as to the specific manufacturers involved in the project. As a result, expansion of the system after initial deployment can generally only be done using equipment of the same type and usually the same brand as in the initial deployment, unless there are investments in major systems integration efforts. There is little to no opportunity for realistic competitive bidding as additional field devices are added to the system, due to the lack of interchangeability. Nor, is there any opportunity to add additional types of field devices to the system, due to the lack of interoperability.

The proper use of NTCIP open-standards in an ITS deployment will allow the future expansion of the system to benefit from true competitive bidding, as well as allow other types of field devices to be added.

The Transportation Equity Act for the 21st Century, known as "TEA-21", requires that federally funded ITS projects "conform" with the National ITS Architecture. As defined in TEA-21, the term "intelligent transportation system" means "electronics, communications, or information processing used singly or in combination to improve the efficiency or safety of a surface transportation system". The National ITS Architecture defines both the functions performed in implementing ITS, and the information flows between transportation subsystems. On January 8, 2001 the USDOT published two important and related documents in the Federal Register:

- The Federal Highway Administrations **Final Rule** on the National ITS Architecture.
- The Federal Transit Administrations **Policy** on the National ITS Architecture.[1]

Key requirements of these regulations are that regional ITS architectures must be prepared, all ITS projects must follow a systems engineering process, and that ITS standards be used. The final two items in the preceding list are within the purview of this *NTCIP Guide*.

Systems engineering is an approach to designing projects that employs an iterative process in developing the concept of operations, needs and requirements, design, build, testing, evaluation, and deployment of the implementation. A systems engineering approach requires that project team considers all phases of a system's life cycle from the moment of the system's conception until its installation. This means taking into consideration the states of planning, design procurement, deployment, operations, maintenance, pre-planned enhancement or expansion, and retirement of the system or subsystems. This approach also requires the team to:

- Identify alternatives at each step of designing and building the system
- Evaluate requirements and design impacts for each alternative based on costs, political and technical considerations, and customers needs.
- Consider what risks exist throughout the process and plan for their management.

For ITS projects, the Rule/Policy states that a systems analysis shall include, at a minimum:

- Identification of those portions of the regional ITS architecture being implemented (or if a regional ITS architecture does not exist, the applicable portions of the National ITS Architecture).
- Identification of participating agencies roles and responsibilities.
- Requirements definitions.
- Analysis of alternative system architecture and design configurations and technology options to meet the requirements.

1. These documents are similar in nature and both became effective on April 8, 2001. Their differences reflect the processes by which FHWA and FTA administer projects.

- Procurement options.
- Identification of applicable ITS standards and testing procedures.
- Procedures and resources necessary for operations and management of the system.

The Rule/Policy requires that federally funded ITS projects use, where appropriate, U.S. DOT adopted ITS standards. The National ITS Architecture defines a common framework for ITS integration, and the ITS standards define how the system components operate within this framework. By specifying how systems and components interconnect, the standards allow for interoperability. To expedite deployment of nationally interoperable ITS systems and services, the U.S. DOT supports specific ITS standards initiatives, especially in those areas that have significant public benefit.

The U.S. DOT ITS Standards Program is working toward the widespread use of standards to encourage the interoperability of ITS systems. Through cooperative agreements with five standards development organizations (SDOs), the Standards Program is accelerating development of non-proprietary, industry and consensus-based open ITS standards, and is encouraging public-sector participation in the development process. The five SDOs are: AASHTO, ITE, NEMA, IEEE and SAE.

Various SDO's are now developing over 80 ITS standards. As an SDO-approved standard matures and the market for a standard expands, the U.S. DOT may decide to adopt an ITS standard through a formal rulemaking process. Only after a rulemaking is completed will an ITS standard be required for use in federally funded ITS projects.

Exclusive of adoption by U.S. DOT, ITS practitioners are encouraged to use SDO-approved ITS standards when deploying ITS projects in their region. The use of ITS standards is necessary to provide integrated, fully open systems.

U.S. DOT will continue to encourage stakeholders to test and evaluate developing standards, and where available, to use ITS standards products in their deployment. In support of early deployment, the ITS Standards Program offers a set of information and resources to those ITS project managers who decide to use ITS standards now. A website, located at www.its-standards.net, exists to provide background information, testing results, and guides to deploying specific standards. In addition, links to contacts, training, and technical assistance resources can also be found on this site.

The terms interchangeability and interoperability are used throughout the TEA-21 legislation, but interoperability is used more extensively. While the simple view of NTCIP often focuses on interchangeability, interoperability is actually far more important, for two reasons. First, since the communications infrastructure is usually the most costly element in a new system, using this infrastructure for multiple purposes lowers the overall initial

cost of the system. Second, and more important in terms of the TEA-21 legislation, interoperability in the C2C realm suggests the sharing and mutual understanding of data. This increases the operators' ability to efficiently manage these transportation systems, and to encourage the sharing of operational data across jurisdictional boundaries.

2.5 Benefits of NTCIP

NTCIP offers increased flexibility and choices for agencies operating transportation management systems. It removes barriers to interagency coordination and allows equipment of different types and manufacturers to be mixed on the same communications line. For these reasons, operating agencies will benefit from specifying NTCIP in future purchases and upgrades, even if NTCIP is not used initially.

2.5.1 Avoid Early Obsolescence

Even though it may not be practical to retrofit NTCIP support in some legacy equipment and systems, most manufacturers will offer NTCIP support in current and future products. It is possible to operate a mixture of NTCIP and non-NTCIP devices in the same system, although not on the same communications line. An operating agency can ensure that its equipment remains useful and compatible long into the future by requiring NTCIP support in all future purchases and upgrades of transportation management systems. This would include purchases of computer software, field masters, controllers for any type of traffic or transit control, or monitoring device.

2.5.2 Provide Choice of Manufacturer

Once an agency has a central computer system that includes support for NTCIP, it can purchase other systems, field devices, or software from any manufacturer offering NTCIP-conformant products that will communicate with that system. It may be the case that only products from the same manufacturer will be able to fully use the richness of features within the software or controller that are manufacturer specific, but basic functionality will be available regardless of the manufacturer, provided the procurement documents adequately specify the mandatory and optional features that support the agency's functional requirements. However, open NTCIP standards will make it easier for an agency to gradually change its software, controllers and other field devices from one manufacturer to another completely, or in part to simply add multiple manufacturer's devices to their system in the future.

2.5.3 Use One Communications Network for All Purposes

The communications network is usually one of the most expensive components of a transportation management system. NTCIP allows a management system to communicate with a mixture of device types on the same communications channel. NTCIP ensures maximum flexibility in future use of that major investment.

2.6 Lessons Learned

The principal issue associated with the use of NTCIP is that it represents an emerging technology in transportation. As is the case with most new or emerging technologies, the early implementers were on the leading edge of specifying NTCIP. These early adopters often lacked appropriate educational material on the best way to specify, procure, deploy, integrate and test these systems. The *NTCIP Guide* has been created largely in recognition of these issues, and to assist future implementers in avoiding the problems associated with the initial deployment of new NTCIP-based technology.

The NTCIP has been designed based upon existing and widely supported Internet and commercially available communications protocol standards to the greatest extent possible, thus minimizing the risk associated with the use of new and untested protocols.

Agencies considering the deployment of NTCIP should carefully consider their concept of operations and functional requirements of the system being implemented. For example, some agencies may only be concerned with the strictest interchangeability of field devices, and not with using the various proprietary features and functions specific to certain manufacturer's devices, while others may desire a reduced level of interchangeability in order to benefit from these various proprietary features. They should then express this preference as they map their requirements to the standards, both in terms of data elements and in terms of communications media. A desire to mix various devices in the communication infrastructure must also be considered. All of these issues will have significant impact on the procurement specification and agencies should consider their overall objective early in the system design and procurement phases.

Furthermore, it may not be practical to retrofit the NTCIP C2F protocol into some older legacy traffic control equipment due to a lack of processing power and memory capacity. Agencies should consider and investigate these issues, along with communications bandwidth considerations, when considering a migration strategy for system upgrade.

2.7 Resources

Agencies are often concerned with what resources they ***should*** bring to an NTCIP implementation. This section of the *NTCIP Guide* offers some discussion on some of the resources available for additional information on NTCIP.

2.7.1 Training

An understanding of the technical issues surrounding NTCIP will benefit agencies considering deployment. Various training opportunities are available. Training seminars on NTCIP are available from AASHTO, ITE and NEMA. Of particular interest may be the four ITE courses on ITS Standards, including NTCIP, that are offered throughout the country based upon agency requests. Further, some consulting firms and manufacturers also have the ability to offer in-depth training services on this topic.

Information about the course content and scheduling of the ITE Outreach, Education and Training (OET) Program can be found at on www.ite.org/standards/CourseSchedule.htm.

Additionally, C2C ITS procurements are essentially software acquisitions. The National Highway Institute (NHI) offers an excellent course on ITS Software Acquisition entitled *The Road to Successful ITS Software Acquisition*. Please consult the NHI course catalog for additional information on course content and scheduling a course on ITS software acquisition (on www.nhi.fhwa.dot.gov/catalog.asp).

General information on the subject of NTCIP is also available at on www.ntcip.org/. Because the NTCIP family of standards draws heavily on Internet-based or commercially available protocols, books and other descriptive information are readily available from public libraries, bookstores and the World Wide Web to assist in the planning of deployment-specific training programs.

2.7.2 Technical Abilities

While users of transportation management systems need not understand the engineering intricacies of the NTCIP protocols, they should have a basic understanding of several things: the relevant primary and supporting NTCIP standards publications, the *NTCIP Guide*, and the referenced Internet or commercially available protocols that are applicable to their project. Those who need to have a more in-depth understanding of NTCIP include: specification writers, system designers, integrators, suppliers and those responsible for testing.

2.7.3 Projects

It is highly recommended that projects implementing NTCIP include in their deliverables certain items relating to NTCIP training and documentation. General NTCIP awareness training for system operators and administrators throughout the project would assist with an understanding of the benefits associated with the use of NTCIP standards, as well as the opportunities, limitations and procedures for future expansion and/or improvement of the system. It is further recommended that a project-specific NTCIP manual should be included in the list of deliverables that thoroughly documents the details associated with the various NTCIP "as-built" options and features in the system. In systems using the Simple Network Management Protocol (SNMP), an electronic copy of the Management

Information Base (MIB) should also be requested so that NTCIP and project specific data elements will be available for future system expansion. It is important to note that authorizations will need to be secured for the use of manufacturer-specific data elements in future projects. These recommendations are especially important to meet future interoperability and interchangeability needs if the delivered system has been accepted with variations from the procurement specifications and/or variations of the features based on the NTCIP standards. A design baseline document will greatly facilitate any future work on the system, including improvements or expansions. The lack of such a document in older proprietary systems has been a great deterrent to cost-effective future improvements.

2.7.4 Conformance Testing and Certification

Each NTCIP standard contains a "Conformance Clause" which clearly states the requirements for conformance to the standard by implementations that embody that standard. The ease or difficulty to determine conformance depends on the complexity of the standard and the resulting implementation.

The outcomes or a "conformity assessment" are limited to: pass, pass with exceptions, and fail. This determination is based on an examination of the implementation through testing with a well-defined test suite. A test suite embodies the test cases, procedures, and expected results for exhaustive examination of the implementation against the requirements for conformance to the standard. If an implementation meets all requirements exactly—then "Pass." If it meets most requirements with a few exceptions—then "Pass with Exceptions", these exceptions would be listed in a test report. It should be noted that these exceptions may span the spectrum of little-to-no introduced risk or consequences, or they could be show-stoppers requiring complete rework of the implementation. Lastly, if the implementation does not meet a majority of the requirements—then it should "Fail" to achieve conformance.

When an ITS implementation achieves conformance to the standards it embodies, it then becomes a candidate for "Certification." Certification might be awarded by an accredited industry forum as an official recognition that the product meets the stated requirements for conformity to the standards. Examples of this process are found in everyday life—look at the bottom of your computer's keyboard—the statement that begins "This device complies with …" is an equivalent "Certification" similar to what would be attached to the conformant ITS implementation. Also notice that a certification must refer to the test suite or rules used to determine conformance—in the keyboard case, this is Part 15 FCC Rules and/or ICES-003 Class B (computing devices). Lastly, the logos on the certificate represent the joint approval of the several members of the industry certification forum.

Conformance differs from Compliance—the former is based upon and judged with respect to specific and unambiguous exact usage of the standard. The latter, compliance, is often used ambiguously to mean conformance, but it is less exact in its requirement to adhere to the standard. The term compliance is most often used in contractual language to assess the legal determination of meeting or not meeting the specifications of the contract. A real-

world example of this relationship between conformance and compliance would be the case where conformant and certified ITS implementations are assembled into a system for deployment in your city. You then include all the local specifics for your particular functionality and telecommunications infrastructure requirements. This requires "tweaking" some aspects of the use of standards in the implementations to "make them work" for you. Thus, the devices were conformant, now the tailored system is only compliant—to your specification, in your city, in this deployment—and, you are happy being "Compliant."

Chapter 2: Review

Questions:

1. The type of communications that involves a computer at a management center communicating with various devices at the roadside is referred to as _____ communications.
   a. Center-to-Field (C2F)
   b. Center-to-Center (C2C)
   c. Field-to-Center (F2C)
   d. All of the above

2. The type of communications that involves messages sent between two or more management systems is referred to as _____ communications.
   a. Building-to-Building (B2B)
   b. System-to-System (S2S)
   c. Center-to-Center (C2C)
   d. None of the above

3. What is not part of the NTCIP?
   a. Center-to-Center specifications
   b. Family of communications protocols
   c. Incident Management data
   d. Dynamic Message Sign (DMS) data dictionary

4. What is the primary goal of NTCIP?
   a. Interoperability
   b. Interference
   c. Interchangeability
   d. Intermodalism

5. Name the website where general information on the subject of NTCIP can be found.
   a. www.nasa.org
   b. www.ieee.org
   c. www.tmdd.org
   d. www.ntcip.org

Answers:

1. (a) Center-to-Field or (C2F)
2. (c) Center-to-Center or (C2C)
3. (c) Incident Management data
4. (d) Interoperability
5. (b) www.ntcip.org

THIS PAGE LEFT INTENTIONALLY BLANK

Chapter 3

Understanding NTCIP

3.1 Introduction

This chapter is intended for those with interest in exploring NTCIP beyond the "Chapter 2 Executive Summary", and particularly for those involved in planning ITS systems. It is assumed that the reader has already read the "Executive Summary" that provides much of the basic information that is not repeated in this section.

3.2 Benefits of NTCIP

NTCIP standards offer increased flexibility and choices for agencies operating transportation management systems. It removes barriers to interagency coordination and allows equipment of different types and different manufacturers to be mixed on the same communications line. For these reasons, operating agencies will benefit from specifying that NTCIP be included in all future purchases and upgrades, even if NTCIP is not initially used.

3.2.1 Avoiding Early Obsolescence

While retrofitting legacy equipment and systems with NTCIP support is not practical in most situations, most manufactures will offer NTCIP support in their current and future products. It is possible to migrate a system gradually, since it is possible to operate a mixture of NTCIP and non-NTCIP devices in the same system, though not on the same communications line. Equipment may also continue to use a current protocol even though the device may also support NTCIP as a second protocol. Integrating legacy equipment and systems with NTCIP-conformant upgrade purchases in this manner ensures that an operating agency's systems and equipment remain useful and compatible long into the future.

Buying a field device or central control system that has no software available to support NTCIP is like buying a computer that has no software available to access the Internet. Even if purchasers do not use the Internet now, they surely will during the lifetime of the computer.

3.2.2 Providing a Choice of Manufacturer

Since a computer system that supports NTCIP can communicate with any product from other manufacturers that are NTCIP-conformant, the number of manufacturers and systems, field devices, or software that can be considered for purchase increase greatly.

While manufacturer specific features will only be available to other software and controller products from the same manufacturer, the basic functionality described in the standard will be available regardless of the manufacturer. This requires that the procurement documents adequately specify the mandatory and optional conformance requirements that support the agency's functional requirements. However, NTCIP will make it easier for an agency to gradually change its software, controllers and other field devices from one manufacturer to another as part of a switch to a new manufacturer for the entire system.

Naturally, an agency has to consider not only the interoperability/interchangeability aspects inherent to the NTCIP family of standards, but also issues such as stocking replacement parts, which will most likely be different from provider to provider, and the knowledge-base of ITS technicians who would have to become familiar with other manufacturer's products.

3.2.3 Enabling Interagency Coordination

NTCIP allows agencies to exchange information and (with authorization) basic commands that enable any agency to monitor conditions in other agencies' systems, and to implement coordinated responses to incidents and other changes in field conditions when needed. Such data exchange and coordinated response can be implemented either manually or automatically. One agency can monitor, and issue basic commands, if authorized, to field devices operated by another agency, even though those devices may be from a different manufacturer than those used by the monitoring agency. Potential applications of interagency coordination include:

- Coordinating timed transfers at a shared transit center,
- Coordinating traffic signals across jurisdictional boundaries,
- Providing traffic signal priority for selected, e.g., behind schedule, transit vehicles,
- Providing real-time information to a shared traveler information center,
- Monitoring traffic volumes on another agency's roadway,
- Coordinating the operation of a freeway ramp meter with an adjacent traffic signal, or,
- Posting a warning message on another agency's dynamic message sign.

3.2.4 Using One Communications Network for All Purposes

NTCIP allows a management system to communicate with a mixture of device types on the same communications channel. For example, with the addition of appropriate application software in the system computer, a dynamic message sign could be installed near a signalized intersection, and the computer could communicate with the sign controller using the communications line or channel already in place for the traffic signal controller, if certain aspects of the communications protocols, that is, the Data Link and Physical layer protocols are the same. Similarly, a wide area network interface installed for communications with a system operated by another agency can be used for communications with any number of other systems, of any type, if NTCIP and the C2C Data Dictionaries and Message Sets of other efforts such as the Traffic Management Data Dictionary (TMDD) are used. The communications network is usually one of the most expensive components of a transportation management system. NTCIP ensures flexibility in the future use of that major investment.

3.3 Types of Systems and Devices Supported by NTCIP

NTCIP defines a family of general-purpose communications protocols and transportation-specific data dictionaries/message sets that support most types of computer systems and field devices used in transportation management. Applications for NTCIP are generally divided into two categories: C2F and C2C. The former, normally involves devices at the roadside, communicating with management software on a central computer. C2C applications usually involve computer-to-computer communications where the computers can be in the same room, in management centers operated by adjacent agencies, or across the country. The role of NTCIP in the National ITS Architecture is illustrated in Exhibit 3.1.

For both C2F and C2C applications, NTCIP supports systems and devices used in traffic, transit, emergency management, traveler information and planning/data archiving systems. Exhibit 3.2 illustrates how various transportation management systems and devices can be integrated using NTCIP.

Note: *Some computers involved in C2C communications may be located in the field, for example, kiosks, field masters, advanced controllers. NTCIP's C2F and C2C communications protocols have options to support dial-up communications links.*

The following are examples of systems and devices that can take advantage of NTCIP:

- ***Center-to-Field (C2F)***
  - ❖ Dynamic message signs
  - ❖ Traffic signals
  - ❖ Field masters (closed loop systems)

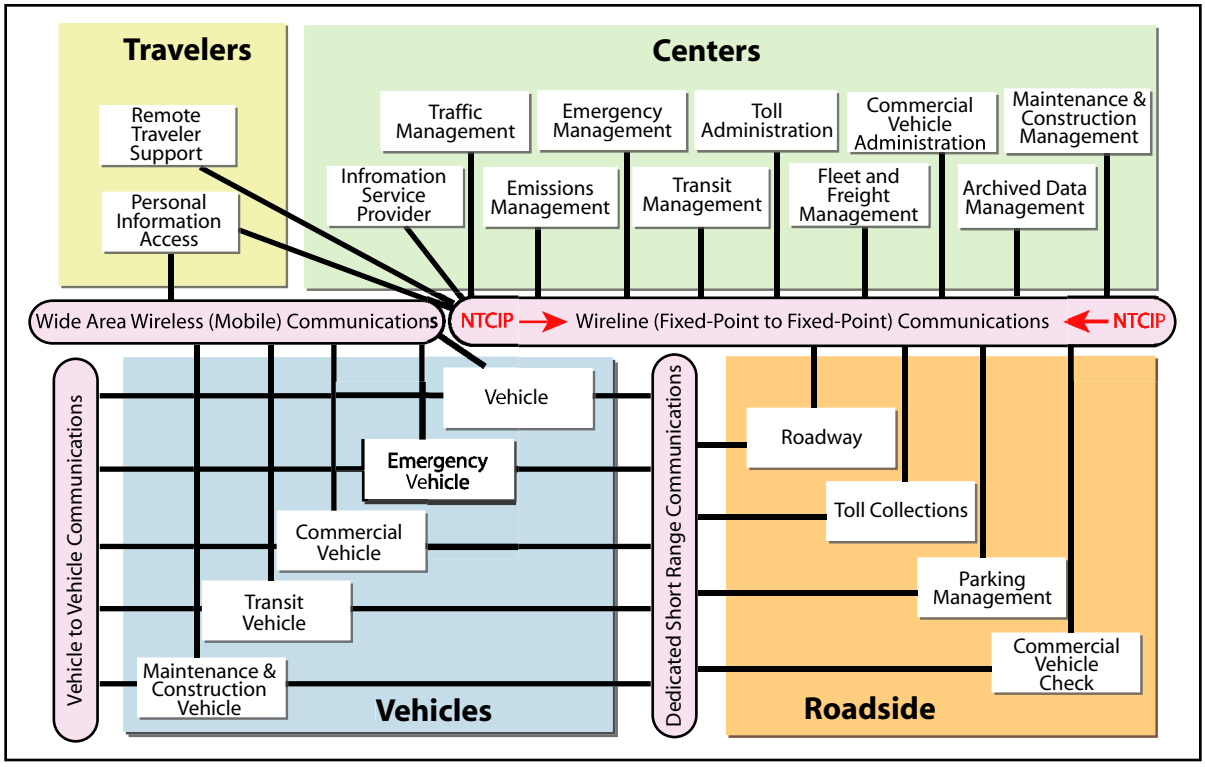


Exhibit 3.1: NTCIP and the National ITS Architecture

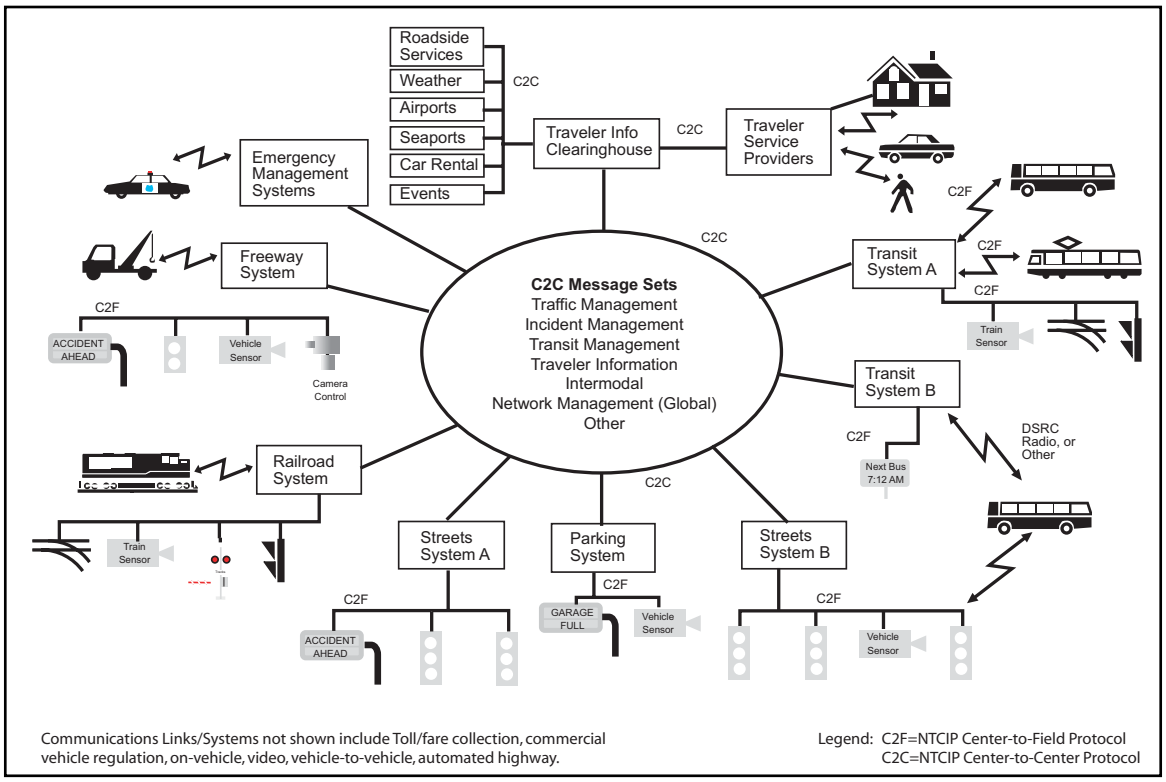


Exhibit 3.2: Example of ITS Integration Using NTCIP

- ❖ Data collection and monitoring devices such as traffic counter, traffic classifiers and weigh-in-motion stations
- ❖ On-board sensors and controllers
- ❖ Environmental sensors
- ❖ Ramp meters
- ❖ Vehicle detectors
- ❖ Closed circuit television cameras (camera control only)
- ❖ Video switches
- ❖ Highway lighting control

- ***Center-to-Center (C2C)***
  - ❖ Traffic management (freeway/surface street, urban/rural)
  - ❖ Transit management (bus/rail/other)
  - ❖ Incident management
  - ❖ Emergency management
  - ❖ Parking management
  - ❖ Traveler information (all modes)
  - ❖ Commercial vehicle operations regulation
  - ❖ Any mix of the above

Many applications of NTCIP are related to near real-time communications and involve continuous, automated transmissions of data or commands. NTCIP also supports human-to-remote-machine/system transmissions. Historical data can also be sent using NTCIP, but other communication standards, especially electronic mail and file transfer protocols developed for the Internet, may also be suitable for this purpose. Human-to-human communications are generally better served by fax/telephone and Internet protocols, for example, e-mail, chat, but basic support is also provided in the NTCIP C2C protocols.

3.4 Applications Not Addressed by NTCIP

Some of the data transfers involved in ITS operational uses have special needs that are the subject of other standards development efforts. The NTCIP effort is coordinating with the activities of these other groups to the extent practical. These other standards efforts include:

- A roadside device reading and/or writing to an electronic tag on a vehicle. This involves very fast and compact wireless data transfers over short distances of a few meters during the few milliseconds that a passing vehicle's tag is within that

reception range. However, NTCIP is suited to C2F communications between the roadside tag reader and a central computer;

- Full motion video images transmitted from a camera or recorded media. This involves specialized protocols able to accommodate the large volume of continuous streaming information making up a video signal, and several such industry standards already exist, for example, NTSC. However, NTCIP is suited to C2F transmission of video camera control commands and switch control data using a separate communications channel;
- Transmission of traveler information data to privately owned vehicles. This involves special broadcast and limited bandwidth protocols such as those that work in conjunction with the FM radio standards or cellular radio. However, NTCIP is suited to sending the information from various data sources to the traveler information service provider, using C2C communications;
- Communications for financial transactions. This involves special security measures not currently supported in NTCIP;
- In-vehicle communications for operations monitoring, advanced vehicle control and safety. This involves specialized protocols for very high speed and fail-safe transmissions between devices housed on the same vehicle; and
- In-cabinet communications between a controller and other electronic devices in a roadside cabinet. This involves specialized protocols for very fast high-volume data transmissions over short distances. The ITS industry is currently addressing these requirements in the Advanced Transportation Controller (ATC) efforts, which will result in three standards, the ATC Cabinet standard, the ATC Controller standard and the ATC Application Programming Interface (API) standard.

Other communications standards are available, or under development, to serve each of these specialized needs.

3.5 The NTCIP Communications Levels

NTCIP uses a layered or modular approach to communications standards, similar to the layering approach adopted by the Internet and the International Organization of Standards (ISO). In general, data communications between two computers or other electronic devices can be considered to involve the following primary layers, called "levels" in NTCIP, to distinguish them from those defined by ISO and the Internet. The NTCIP standards publication numbers are grouped in number ranges to indicate the standard type and the *level* where the standard goes.

- ***Information Level*** – This level contains standards for the data elements, objects and messages to be transmitted, for example, TCIP, NTCIP 1200 series Standards Publications, MS/ETMCC.
- ***Application Level*** – This level contains standards for the data packet structure and session management., for example, SNMP, STMP, DATEX-ASN, CORBA, FTP.
- ***Transport Level*** – This level contains standards for data packet subdivision, packet reassembly and routing when needed, for example, TCP, UDP, IP.
- ***Subnetwork Level*** – This level contains standards for the physical interface, for example, modem, network interface card, CSU/DSU, and the data packet transmission method, for example, HDLC, PPP, Ethernet, ATM.
- ***Plant Level*** – This level consists of the physical transmission media used for communications, for example, copper wire, coaxial cable, fiber optic cable, wireless. It should be noted that the plant level is an infrastructure choice and not a standards selection choice. However, the plant level selection will have an impact on the subnetwork level selection to which it must interface.

The information level standards used in ITS are unique to the transportation industry. The National ITS Architecture and much of the on-going standards development effort for ITS involve identification of required data elements and the definition of their use for all the different domains and functions within ITS, for example, traffic, transit, traveler information, emergency management.

At the application, transport and subnetwork levels, ITS can frequently use existing standards used by the broader computer and telecommunications industries. Below the Information level, the NTCIP standards deal with choosing which existing standards are to be used in ITS. The Internet standards have been adopted where possible. The NTCIP standards specify which options to use where alternatives are available in some standards. NTCIP has not had to develop significantly new standards in these areas. The two major exceptions are the protocols that support:

1. Slow speed, high frequency communications links as found in 1200 bps, once-per-second traffic signal systems, and
2. A simplified Publish-Subscribe C2C protocol.

NTCIP has extended existing standards or developed entirely new protocols as needed in cases where ITS has special protocol requirements. The two areas where special communications requirements of ITS are most evident, include:

- Continuous, automated, real-time exchange of large volumes of small data packets in a many-to-many multi-agency network (addressed by DATEX and the Near Real-Time Data Service addition to CORBA).

- Continuous high volumes of real-time data sent to and from embedded processors in roadside or on-vehicle equipment sharing the same, low-speed, data channel and requiring low latency (addressed by the Simple Transportation Management Protocol and the Point-to-MultiPoint Protocol).

Through a layered combination of existing communications standards and a few new standards developed specifically for ITS, NTCIP provides a family of communications protocols that serve many of the common needs in ITS transportation management.

3.6 The NTCIP Framework

When options are available with layered or modular protocols, the options can be diagramed in a "framework." Exhibit 3.3 illustrates the framework for NTCIP. The diagram shows the different protocols that can be chosen at each level (the boxes) and which ones are compatible (the lines connecting boxes). However, not all compatible configurations make sense, and there are mutually exclusive choices. For example, running SNMP over TCP/IP is not typically done in the Information Technology industry. Refer to "Chapter 7 Glossary" for an explanation of the acronyms used in this diagram.

"[The NTCIP Framework] shows the different protocols that can be chosen at each level…"

A particular message transmission can use at least one protocol from each level of the NTCIP framework. The series of protocols used in the message transmission is called a a "protocol stack." Some of the NTCIP standards publications only define one protocol within the publication. Other NTCIP standards define two of the protocol boxes at a level in the framework.

It is possible for a pair of electronic devices to exchange some messages using one stack and other messages using a different stack, though usually, such stacks will differ only at one or two levels or sublevels. In Exhibit 3.3, the lines connecting standards at different levels show optional standards at each level. If there is a continuous line (without reversal of direction) from one standard to another, then they are compatible and can be used together as part of a protocol stack.

There is also another way to classify the NTCIP standards: primary, supporting, and base standards and protocols.

A **primary standard** applies directly and specifically to the device or component subsystem being implemented. For example, the Standard 1203 applies specifically to DMS, 1204 to ESS; thus, Standard 1203, 1204 and several others are primary NTCIP standards.

A **supporting standard** applies in general to more than one specific device or component subsystem implementation. For example, the NTCIP Standard 1201 Global Objects standard applies to all devices and component subsystem implementations that use or require features such as: identification and location of equipment, global time, and event detection or scheduling. Similarly, the TCIP 1401 Common Public Transportation Objects

accomplishes this same general application for all other public transportation functional areas. Thus, standards like Standard 1201 and TCIP Standard 1401 are supporting standards. Both primary and supporting standards typically apply at the C2F or C2C information layer (Exhibit 3.3).

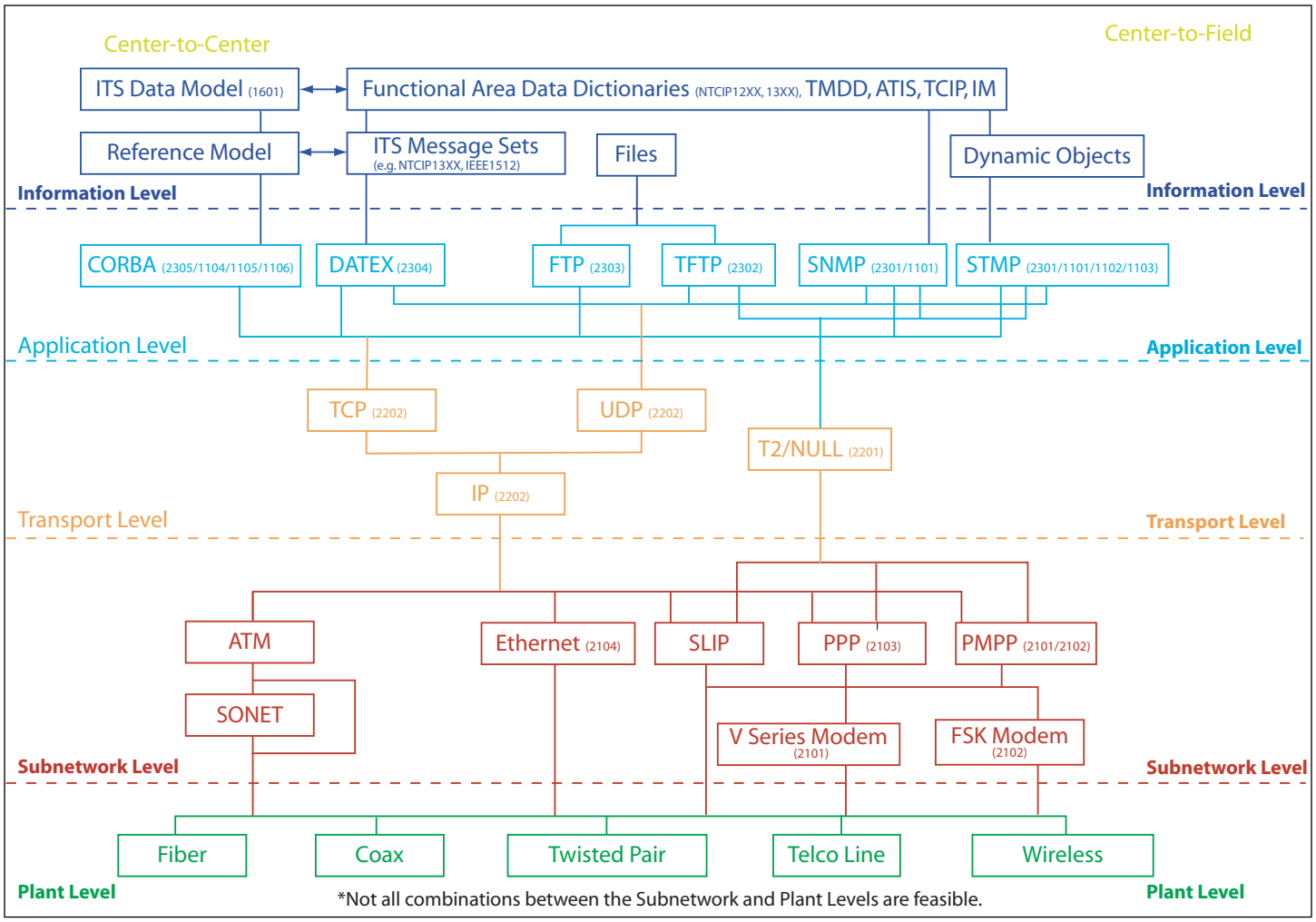


Exhibit 3.3: NTCIP Standards Framework

A **base standard and protocol** applies to the application, transport and sub-network levels. These standards define NTCIP unique capabilities for protocol and data transport choices to complete the design of an operational deployment. These standards differ from both primary and supporting standards in that the data being exchanged is irrelevant— they provide the specifications for critical and essential services. These standards are unaware and largely unaffected by their use in a signal control, DMS, and ESS applications.

The levels shown in the framework are somewhat different from communication stack layers defined by the ISO's Open Systems Interconnect seven-layer reference model and other standards developing organizations. The NTCIP stack extends beyond the communications stack to include informational data and interfaces to the physical

communications infrastructure. The levels and terminology used in NTCIP were chosen for simplicity and ease of understanding by lay readers, and relevance to typical applications in the transportation industry. The OSI layers and terminology are often referenced in later technical sections of this publication and in many of the standards defined by NTCIP.

When a user wants to deploy an NTCIP-based system, they have to choose the protocols they want. The highlighted portion of Exhibit 3.4 illustrates an example if a C2F protocol stack choice that can be defined using NTCIP standards. A stack is a subset of the overall NTCIP framework—a selected route through the levels, given the choices available. Some stacks include two standards at some levels, which usually mean the protocol can use either of the optional standards. NTCIP protocols generally offer further options within most of the standards. Examples of sub-options within a standard are: which subset of messages are supported, or which bit rate is used at the physical interface.

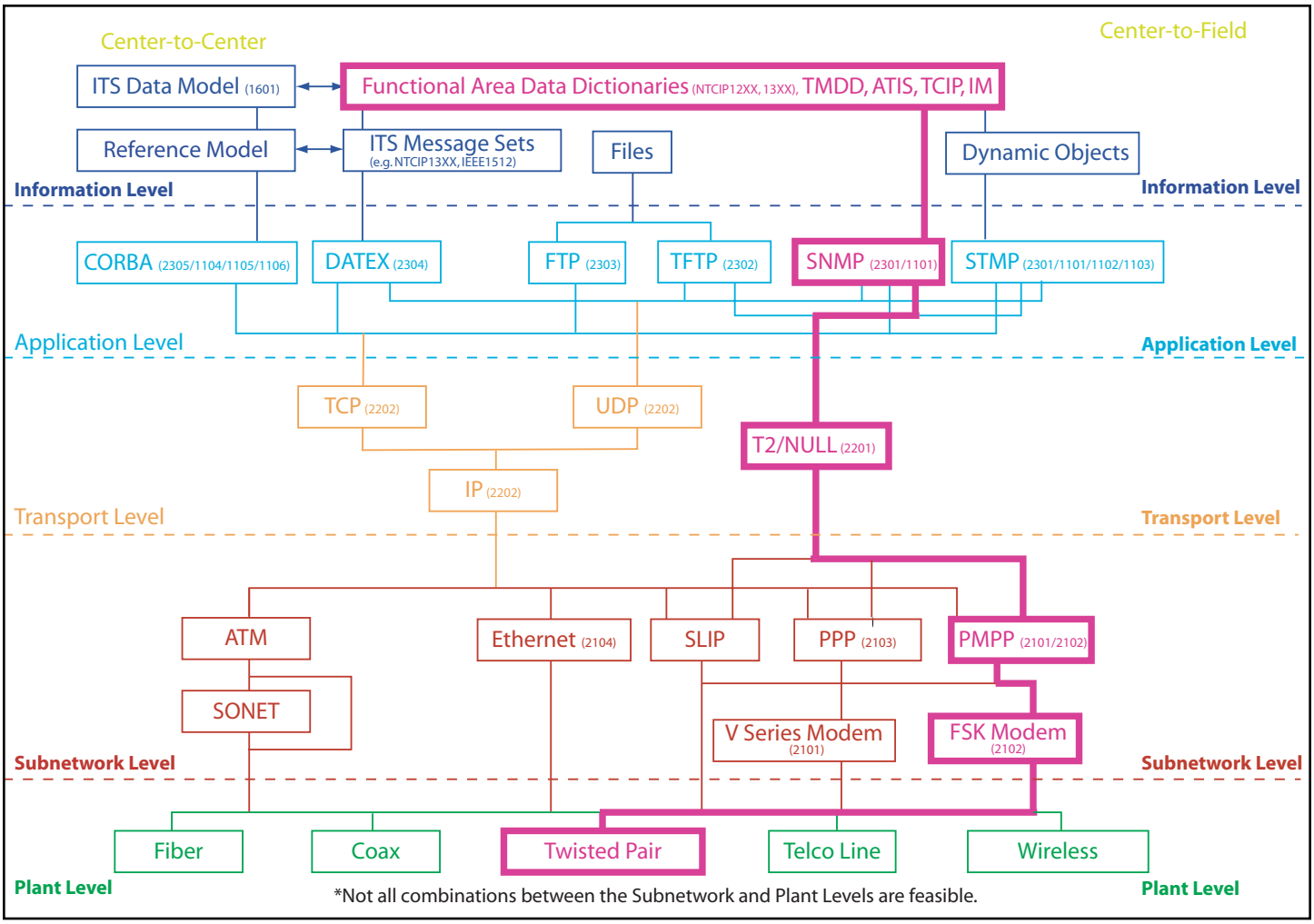
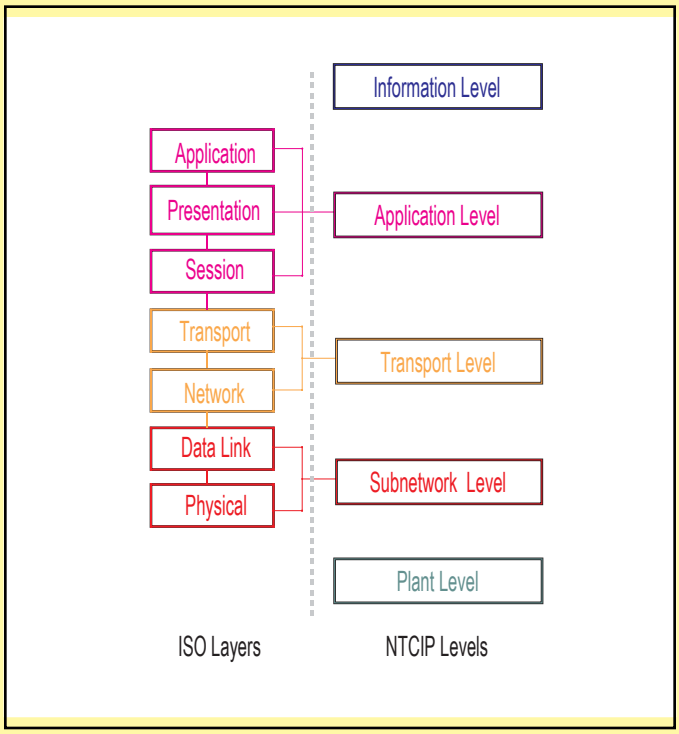


Exhibit 3.4: Example Center-to-Field Stack

OSI Layer to NTCIP Level Mapping



With the many diverse requirements of NTCIP, it is not surprising that we looked at the ISO OSI Basic Reference model to help us define the framework for the new family of standards. Although OSI communications protocols are not widely used, the layered model remains. The OSI model breaks the communications process into seven well-defined layers. Each layer has a defined purpose, generally independent of adjacent layers. This graphic shows how the NTCIP Information, Application, Transport, Subnetwork and Plant Levels loosely relate to the OSI model.

NTCIP Information Level – Information 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 ISO seven-layer model. Information level statndards represent the functionality of the system to be implemented.

NTCIP Application Level – Application 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 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/re-assembly 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 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 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. In most cases, we will have a good idea as to what communications media we will be using in our system implementation early in the design phase.

To ensure a working system, deployers must specify and/or select an NTCIP protocol or profile at each level.

Most of the standards in the lower levels are existing commercially available standards used in the telecommunications industry and were not developed uniquely by NTCIP, although NTCIP often specifies which sub-options within those standards are to be used. The majority of standards unique to Intelligent Transportation Systems are found in the first two levels (Information Level and Application Level) shown at the top of Exhibits 3.3 and 3.4. Each NTCIP protocol stack involves a mixture of standards, with at least one from each level.

3.7 NTCIP Standards and Protocol Stacks

The first NTCIP standards developed were those intended for C2F applications. This involved a *new* application level standard called Simple Transportation Management Protocol (STMP), a *new* transport level standard called the Transportation Transport Profile (T2 or T2/NULL), and several sets of *new* standard data elements called "object definitions" at the information level. The initial NTCIP C2F protocol development also involved references to three *existing* standards:

- Point-to-Point Protocol (PPP)
- A customization of the High-level Data Link Control (HDLC) standard at the subnetwork level, known as the Point-to-MultiPoint Protocol and
- The Simple Network Management Protocol (SNMP) standard at the application level.

SNMP was the basis for the development of STMP, while PPP and HDLC were the basis for the development of the Point-to-MultiPoint Protocol (PMPP).

In 1999, the approach for documenting NTCIP standards and protocol stacks was changed. Previously, NTCIP standards defined the range of options at each level of a protocol stack using "device profile" documents, most notably the *Class B Profile* (NTCIP 2001).

Due to the myriad of possible device profiles, this approach was seen as too confusing, and the following approach was taken. Though it was understood that this would initially create confusion, in the long run this new approach seemed more logical. The numbering scheme for NTCIP publications also changed from the NEMA TS-naming to the NTCIP naming, as shown in the Chapter 10 "NTICP Documents". NTCIP 2001 has been replaced with a series of individual standards publications at each level in the stack.

There are different types of standards publications for the different levels of the stack, as follows:

- ***Information Standards*** define information profiles at the Information Level (1xxx series of NTICP Standards);
- ***Application Standards*** define application profiles at the Application Level (23xx series of NTCIP standards);
- ***Transport Standards*** define transport profiles at the Transport Level (22xx series of NTCIP standards); and
- ***Subnetwork Standards*** define subnetwork profiles at the Subnetwork Level (21xx series of NTCIP standards).

Each standard specifies one or more protocols to be used at a given level, and the sub-options allowed or required within each of those standards. A standards publication will typically reference one or more "normative standard" publications— other publications that contain additional relevant specifications for the standard(s). A referred normative standard may be another NTCIP publication, if the standard was developed by NTCIP, or a publication developed by any other standards development organization. For a particular application of NTCIP, the user must select, in the procurement specifications, which element(s) are desired at each level—for example, select from the options called out in one or more profile publications for each level. The set of selections and options for base standards and protocols for all levels is referred to here as a "protocol stack." Each NTCIP protocol stack will have different characteristics, and a stack that works well for one application or communications environment may not suit another.

Application level standards that NTCIP has defined are briefly described below. As pointed out in Exhibits 3.3 and 3.4, these application profiles can be combined with certain transport profiles.

- ***Simple Network Management Protocol (SNMP)*** – Stacks based on SNMP provide a simple, but bandwidth inefficient, protocol for C2F applications,

based on the Internet protocol of the same name (SNMP). It is suitable only for networks with high bandwidth, or low volumes of messages. SNMP has been designed by the Internet community to run over UDP/IP, but it can be forced to run over TCP/IP or T2/NULL.

- ***Simple Transportation Management Protocol (STMP)*** – STMP was developed specifically for use in the transportation industry. It is an extension of SNMP that allows C2F messages to be sent more efficiently using dynamic composite objects. Stacks based on this protocol are suitable for networks with low bandwidth and high volumes of messages, including such traffic signal systems where a central computer is directly connected to field devices, without the need to route the information through some other device such as an on-street master in a closed loop system. STMP has been designed to run over T2/Null since it supports low bandwidth links, but could also be used over UDP/IP or TCP/IP if sufficient bandwidth is available.
- ***(New) Simple Fixed Message Protocol (SFMP)*** – A need has been expressed for having a bandwidth efficient protocol for low-end field devices, like closed circuit camera controllers. NTCIP is developing SFMP to meet this need. Since SFMP is not yet complete, it is not yet included in the NTCIP Framework (see Exhibits 3.3 and 3.4).
- ***Data Exchange (DATEX)*** – DATEX provides a general-purpose C2C data exchange protocol stack. It uses pre-defined messages transmitted by the base Internet protocols (TCP/IP and UDP/IP) in a peer-to-peer network. The base standard at the application level is an ISO standard, developed by an NTCIP working group called DATEX-ASN.
- ***Common Object Request Broker Architecture (CORBA)*** – CORBA is a general-purpose C2C communications protocol based on the computing industry standard of the same name. For object-oriented systems, it enables a higher degree of integration and some services not provided by DATEX, but it may not be suitable for near real-time applications and loosely coupled systems.

The standards that can be used in each of these categories of protocol stacks are shown in Exhibit 3.3.

Two electronic devices will be better able to communicate interchangeably with each other, if they use the same communications protocol stack, the same information level data dictionaries and message sets, and implement the same desired options defined in each of these selected primary, supporting, and base standards and protocols.

For additional information, please refer to the complete listing of NTCIP related publications in Chapter 10.

3.8 Options and Conformance Levels

In addition to specifying a protocol stack, the system designer must also choose between various options and alternatives available in the selected stack. These options exist in both C2C and C2F protocol stacks. Major options, such as which protocol(s) to support at each level in the communications stack, are sometimes grouped according to conformance levels, while others are individually selectable. Most manufacturers and system suppliers typically offer features that go beyond the standard. To make use of such features, it is necessary to specify the inclusion of manufacturer-specific data elements or messages as extensions of the standards when procuring a management system.

The decision by an agency to use features above and beyond the standard should be taken only with the understanding of the potential impacts. These impacts could be considerable in the long term. These options may, in effect, result in the purchase of proprietary systems. Part of the decision must include how many of these features that will be allowed.

Details on options and conformance levels, and how to specify your selection, are presented in later sections of this *NTCIP Guide*.

3.9 Center-to-Field (C2F) Protocols

NTCIP provides three closely related application level protocol choices for C2F communications: the Internet's Simple Network Management Protocol (SNMP), the Simple Transportation Management Protocol (STMP) and the Simple Fixed Message Protocol (SFMP), which is now in development. These base protocols use the get/set-messaging paradigm used in the SNMP. These choices use the same base data elements, as defined in the NTCIP 1200 series of publications. They differ in the level of complexity to implement and the types of services offered Exhibit 3.5 and Exhibit 3.6 summarize the services offered and implementation requirements. More information on SFMP will be forthcoming in future editions of this *NTCIP Guide*.

Exhibit 3.5: SNMP and STMP Comparisons

	SNMP	STMP	SFMP
Can send any base data element?	Yes	Yes	Currently Under Development
Bandwidth Efficiency – inverse of packet overhead	Worst	Best (uses dynamic objects)	
Supports routing & dial-up	Options	Options	
Message Set	Supported	Limited to 13	
Ease of implementation	Easy	Hard	

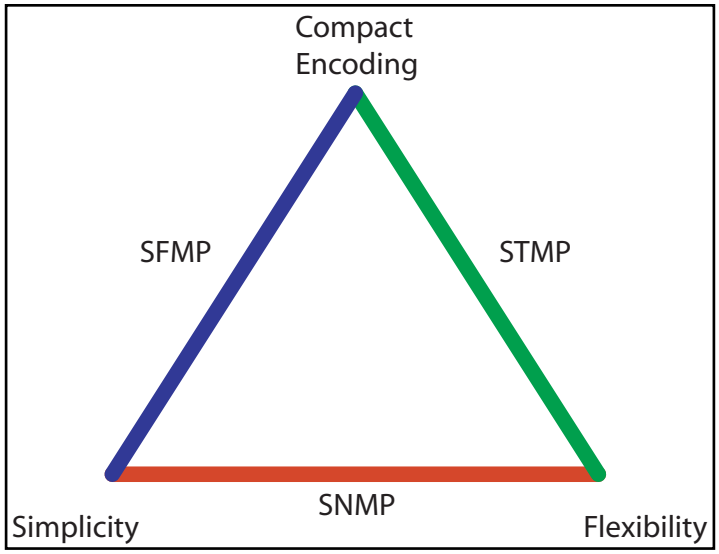


Exhibit 3.6: C2F Protocols

The Simple Transportation Management Protocol (STMP) is the most bandwidth efficient option currently available and includes full support of SNMP for infrequent messaging demands. It includes SNMP as a subset, so that any management system that implements STMP can also communicate with a device that supports only SNMP. It also requires the use of SNMP to define dynamic objects. Occasional messages requiring additional security can be sent using SNMP. The greatest advantage of STMP is its support for dynamic objects which, when combined with a more efficient encoding scheme, dramatically reduce the packet overhead relative to SNMP. Dynamic objects also enable users to define custom messages that are composed of any number of individual data elements. However, these data elements will have to be defined in both the central computer and the field devices in order to work properly. STMP is the most flexible and bandwidth efficient option.

Devices that use any particular subnetwork protocol can share the same communications line with other devices using the same subnetwork protocol. It doesn't matter whether such devices are from different manufacturers or are totally different devices, for example, a traffic signal and a dynamic message sign. Each device is assigned an address that is unique on that line or channel. The management system can communicate with any of the devices at any time by sending a message addressed to that device. However, when using Point-to-MultiPoint Protocol, the management system can communicate with only one of the devices on the line or channel at a time. As a function of SNMP and STMP, devices can only send a message to the management system when requested to do so by the management system. The NTCIP protocols enable broadcast messages intended for all devices, for example, a time clock update. No devices can reply to a broadcast message. At present, NTCIP devices cannot communicate peer-to-peer with each other exclusive of a central facility. The identification of needs and requirements for this capability are under consideration.

The NTCIP C2F protocol stacks can be used in management systems of any configuration or complexity. If the Transmission Control Protocol/User Datagram Protocol Internet Protocol (TCP/UDP IP) transport standards are implemented, then support for message routing through intermediate communications hubs or field masters is inherently included. However, a particular implementation of a C2F protocol stack may not provide support for such immediate or future options unless specifically requested at the time of procurement.

The communications link can use any type of media, such as twisted wire pairs, coaxial cable, optical fibers, or radio, for example, narrow band, spread spectrum, microwave. It does not matter whether the communications media is agency owned, leased, or dial-up. Multiplexers can be used to combine multiple channels on one trunk link. Theoretically, any data transmission rate can be used with NTCIP. However, field devices currently support transmission rates in the range of 1200 to 19,200 bits per second. The only requirement assumes that communication is a half-duplex poll and response, and that the time for transmission, including any delay in intermediate relay devices, and the response time in the end device, be reasonable and within the tolerances needed to allow all devices to communicate within the required time frame. These user operational performance requirements, together with the bit rate, polling rate and quantity of information to be transmitted, determine the maximum feasible number of devices on each communications channel (refer to Chapter 5 for further information).

3.10 Communications Infrastructure for Center-to-Field

When planning a C2F communications network using NTCIP that involves continuous polling of field devices, for example, a traffic signal system or transit fleet AVL system, it is important to consider the relationship between the following key variables:

1. Transmission rate (bit rate);
2. Transmission method, for example, full or half duplex, sequential or overlapping;
3. Transmission delay (including any modem/radio set-up/turn-around time);
4. Response delay in the field device (time from receipt of request to sending response);
5. Time between devices or between polling cycles (if needed);
6. Length of message(s) to be sent (dynamic object definitions);
7. Frequency of each type of message (per second, per minute, per day);
8. Number of devices sharing the same line or channel; and
9. Frequency of communication, for example, polling period.

The first seven of these variables will determine the total time needed to communicate once with each device. If this time is then treated as fixed (T), the number of devices sharing the same line or channel (N) and the frequency of communication with each device (P for polling period, the inverse of frequency) is related by the following equation.

$$P = N \times T$$

This is a very simplified explanation of what can be a quite complex design issue that must be addressed early in project planning.

Although STMP is designed for use with communications channels that use a slow transmission rate, as low as 1200 bits per second, it is not as bandwidth efficient as most proprietary protocols used in the past. With existing communications infrastructure, it may not be possible to maintain the same polling period with the same number of devices per channel. This is due to the fact that proprietary protocols are optimized for each manufacturer's equipment and consist of very few fixed short messages without any flexibility in terms of changing these messages, while standard protocols are flexibly designed to accommodate all needs and a wide variety of information and messages in a multi-manufacturer environment. However, careful design can usually find a reasonable compromise between the principal variables. Higher available bandwidth, bit rate, yields fewer compromises or required trade-offs. If new communications infrastructure can be provided, it should allow for additional channels and/or higher transmission rates.

Such implementation issues are discussed in more detail later in this publication.

3.11 Retrofitting and/or Migration of Existing Center-to-Field Systems

It may not be feasible to retrofit or migrate legacy versions of controllers or controller software to make them NTCIP conformant. Constraints such as computing power, memory availability, cost of modification may well preclude such modifications. If such controllers or software cannot be upgraded or replaced, traffic control systems that continue to make use of older equipment or older software versions will likely have to continue using the protocols unique to communications with those devices. However, current version controllers and software within the system may be capable of modification to use NTCIP, and all future versions should be specified as NTCIP conformant. If in doubt, the equipment manufacturer should be contacted and asked if upgrades for NTCIP conformance are available.

The inability to update older equipment should never stop an agency from replacement or migration strategies to make full use the benefits of NTCIP conformant implementations. For example, a central system whose current field devices cannot be updated could be expanded to run NTCIP protocols on some communications channels while the older equipment is maintained on others.

Exhibit 3.7 illustrates a model for a three-step migration from legacy systems to NTCIP. As shown, initially the details of the proprietary interface may or may not be known (indicated by a cloud showing proprietary ownership of system details). Then, there is some intermediate state and some period of time where the operational system consists of a mixture of the legacy systems and the newer NTCIP hardware. There may be shared use of a common communications channel or not for legacy and NTCIP devices—the figure illustrates these as separate. The central control system may be separate or combined; it may run on the same computer or on separate computers—this is determined by the scope of the project to accomplish these migration steps. Pursuit of a migration strategy towards the use of open standards starts to minimize the use of proprietary communications and begins to maximize the use of NTCIP (as shown by the cloud now being dotted as it starts to fade away). Lastly, at some future point, the migration is completed and NTCIP is fully deployed, having replaced all now retired legacy systems (no proprietary cloud at all).

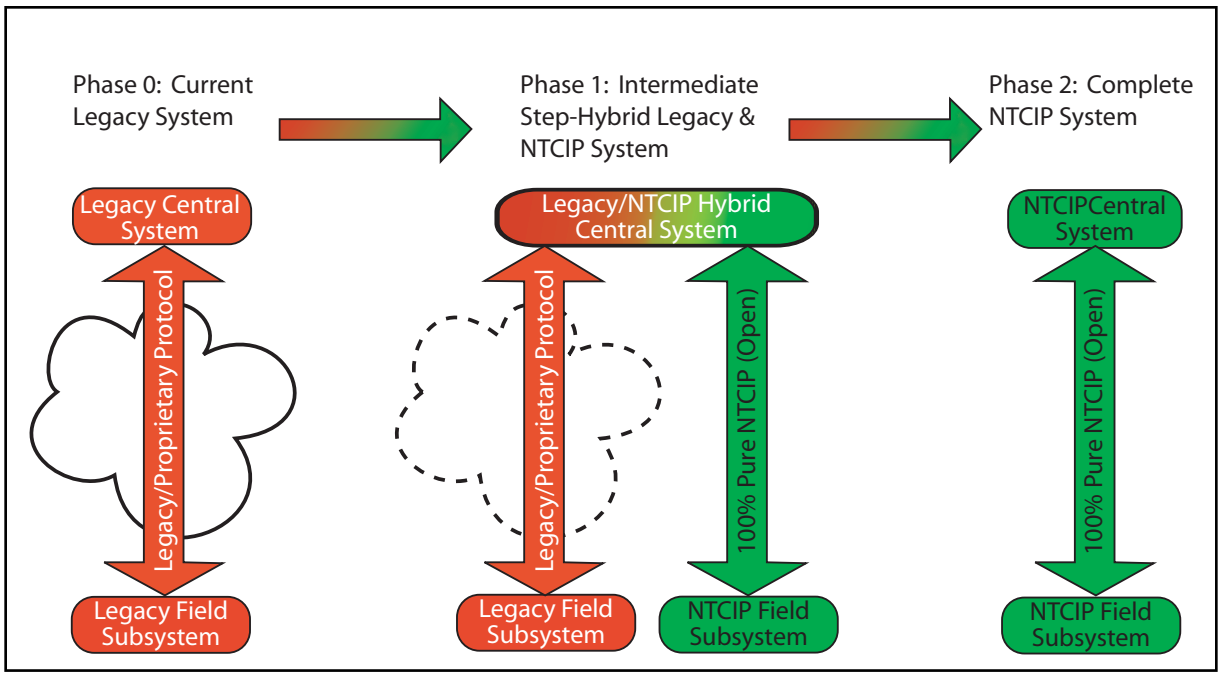


Exhibit 3.7: An Example Three-Phased Migration Process

In general, NTCIP and non-NTCIP devices cannot be mixed on the same communications channel. Therefore, all devices sharing a channel must be upgraded simultaneously. A central computer or on-street master that communicates with both NTCIP and non-NTCIP devices will need to use a different communications port for NTCIP devices and for non-NTCIP devices, and will need to support both protocols. Commensurately, the mixed devices listening on the shared communications channels must recognize and react only to those data elements and commands intended for them individually, and must also not produce unpredictable results in response to any other data traffic on the channel.

A specific example: in traditional closed-loop traffic signal systems, the most likely and simplest solution is to limit each field master to one protocol. Only field masters with NTCIP-compatible controllers would be upgraded to support NTCIP. This avoids the need for field masters to simultaneously support two protocols on two separate ports.

In closed-loop traffic signal systems, the central computer could communicate with field masters using a different protocol than that used by the field master to communicate with controllers. As with the controllers and the field master, the central computer software will need to be modified to add support for an NTCIP protocol, if NTCIP is to be used for communications with field masters.

Any upgrade of an existing system to add support for NTCIP is probably best designed in consultation with the system provider. Each provider will likely adopt an upgrade or migration strategy that is most efficient for the majority of its customers. If a particular customer wants a unique arrangement, that customer will probably have to pay the full cost of the software modifications, whereas the cost of the general solution can be spread among many customers.

One approach to the introduction of NTCIP in a C2F system is to operate two separate systems – one NTCIP and one non-NTCIP – during a transition period (see the middle step in Exhibit 3.7). Field devices can gradually be switched over from one to the other as they are replaced or their software is upgraded. This may be the only choice, if the current system is quite old and upgrading it for NTCIP is not practical. Such a transition would logically be done as part of a general system upgrade.

Legacy Issues and Systems Migration

Migration from proprietary legacy systems to those that are standards based can follow many paths. While this issue is primarily associated with the initial installation of a standards based system, many of the concepts discussed here must also be considered during the life-cycle of a standards based system.

Any migration must consider both hardware and software. While the standards are primarily focused on software, hardware can also be a major consideration. Many of the older existing hardware platforms may not be powerful enough to support the demands of the NTCIP protocols. An agency should take a close look at the hardware and work with the suppliers to determine if it can meet those demands. If the existing hardware platform is more than ten years old, serious consideration should be given to its replacement. In all cases there will need to be changes, to or most likely, a complete replacement of the operating software.

Given that migration will have an impact on both the system software and hardware, and that future changes/improvements in technology are a fact of life, consideration should be given to separating the hardware and software decisions. In many older legacy systems, hardware and software have been provided as an integral package. Just like in the desktop PC world, users typically go through several software upgrades before the hardware is finally replaced. The separation of software from hardware also gives the user flexibility and a larger choice of potential applications software. Many manufacturers and system developers are beginning to structure their systems in a manner that allows such separation.

One caveat, however, is that one should not overlook the condition and capability of the communications infrastructure that will be used to connect these systems. Performing a bandwidth analysis as described in *The NTCIP Guide* will help determine your migration strategy.

There are many paths that can be taken in migrating legacy systems to current standards. The two most likely scenarios are presented as follows:

Replace the entire system at once. For smaller agencies with only a handful of signals, this approach may be possible. If the agency had previously installed field devices that will accept new software, users could easily load the new software during a single off-peak period. However, for many agencies this strategy may prove successful for smaller subsystems, but not an entire system.

Migrate parts of the system. Larger systems will have to be broken down into manageable chunks. The size and shape of these chunks will have to be carefully selected. Some of the constraints on their selection are:

- **Communications channels available**. The bandwidth analysis will identify how many communications channels are needed. Devices are then assigned to available channels. All devices on the same channel ***must*** talk the same language (i.e. use the same communications protocol). The result of this approach is that

two separate systems must be operated, often independently, until the migration is complete. One system will operate using the new communications protocols and the other will operate using the legacy communications protocols.

- **Communications channel capacity.** This constraint is closely related to the previous one. The new communications protocols may not allow as many devices on a channel as the legacy systems. In this case, the communications infrastructure must be altered to accommodate the new channel loading.
- **Staffing.** Staff time will be needed for fieldwork, as well as data entry, for the new system. In many agencies, available staff time suggests that these upgrades will have to take a back seat to emergency maintenance. Contracting strategies will also need to be carefully considered to determine the most expedient approach to performing these activities.
- **Operational considerations.** An agency may want to consider selecting less critical locations for the first deployments. As such, any problems not uncovered during system testing can be corrected with minimal impact. For traffic signal systems, consideration should be given to selecting coordinated groups of signals.

Other items often overlooked include a number of things that can have a big impact on system migration.

- **Data Migration.** System data from the old system may not be easily translated to the new system. Time and resources will have to be dedicated to the input and configuration of data needed for the new system to operate efficiently. This also includes any graphics that are needed.
- **Two Systems?** During this migration period there will be **two** systems in operation. If you can't shut down and replace the entire system at once, a plan will be needed for the care and feeding of the legacy system. Do not forget that system migration may take several years, depending upon the size of the system and funding availability.

At the end of the system migration is a standards based system that will be less costly and less difficult for the next system migration.

Even if a system continues to use a proprietary protocol, new controllers and masters, or new software packages should include the appropriate NTCIP protocol stack as an option, in order to facilitate migration to a standards-based system in the future. However, few providers have implemented support for both their existing protocols and NTCIP in the same software package, while most have required a change of software to switch from one protocol to the other. Regardless of how it is done, the owning agency should ensure that an

appropriate NTCIP protocol stack is available for future use, even if it is not needed immediately. This will maximize the useful service life of the new equipment and enable orderly migration to the introduction of NTCIP at any time in the future without further hardware and software upgrades.

3.12 Center-to-Center Protocols

NTCIP originally provided two alternative application level protocol choices for C2C communications, DATEX-ASN and CORBA. These two different protocols were found necessary to meet the variety of requirements for inter-system data exchanges. More recently, there has been increased interest in using XML and related technologies for C2C links due to its simplicity and the wide accessibility of tools to provide these services. However, it is feasible to use all of these protocols in the same network, with some centers acting as bridges, or translators, between the different protocols. The key is in determining where to deploy each protocol.

DATEX was designed to provide simple, cost-effective solutions for basic needs. It is especially well suited for:

- Systems requiring real-time, fast data transfer, for example traffic signal status data;
- Systems with limited communications bandwidth but high data transfer load;
- Systems with infrequent event driven exchanges over dial-up links; and
- Non-object oriented systems.

Conversely, CORBA provides several features to support networks connecting object oriented systems, and assuming sufficient processing power and communications bandwidth are provided, could be used for all applications between such systems. Object oriented software can take full advantage of CORBA and implement it easily; this is much more difficult to achieve with traditional procedural software.

Its fundamental simplicity, the wide availability of XML tools and a large market of XML-knowledgeable personnel have generated the interest in XML. It is especially well suited for systems requiring limited, simple data exchanges over communications links with sufficient bandwidth and processors with sufficient processing time available. However, there are no current transportation industry standards for the use of XML. The NTCIP effort continues to monitor the maturity of XML in an effort to determine its suitability for future use in the transportation industry.

Current deployments are split fairly evenly between DATEX and CORBA, with very few XML implementations. As of August 2002, it is difficult to suggest how this market will develop.

C2C networks allow each system to request any available information from any or all other systems. Each system can be configured to either accept or reject any request. The "data" sent can be informational or can constitute a "command" to take some action. Consider a message sent from one traffic signal system to another and containing a signal timing pattern number. In DATEX, for example, depending on the message type, it could represent a command to implement that timing pattern at a particular traffic signal or group of signals, or it could represent a status report indicating that this timing pattern was just implemented at a particular traffic signal or group of signals.

The user can also establish standing subscriptions for data, if it wants the same data sent repeatedly. In DATEX, these subscriptions can specify that data be sent one-time-only, periodically, or repeatedly on occurrence of some event as defined in the subscription. Each subscription message has a corresponding publication message. Unless the subscription is a one-time request, the data will continue to be automatically "published" repeatedly until the subscription is cancelled, or until a predefined end date specified in the subscription.

Using CORBA, a system can automatically and dynamically "discover" data availability and shared control options available from other systems. These other systems use the CORBA framework to publish their capabilities and services offered, accept registration requests from authorized clients, and then deliver those capabilities and services to those clients on demand. For example, a CORBA traffic management system that owns a CCTV can offer to provide: (1) the images acquired as (a) snapshot, or (b) streaming video, and/or (2) allow remote control movement of that CCTV. The system owning the CCTV is the "server" and the system asking for the images, and/or control of the CCTV is the "client." This example also serves to illustrate a typical use of a subscription such as "send me a new snapshot image from CCTV123 every minute" stated in the proper terms for that CORBA system—assuming the requester is authorized that service, the expected result is fairly obvious.

C2C communications require a peer-to-peer network connection between the involved computers. This is typically a local area network, a wide area network, or a dial-up connection. Local area networks typically use agency-owned twisted pair cable or fiber optic cable. Wide area networks typically use commercial telecommunications links such as frame-relay, fractional T1 leased lines, packet radio, or leased "virtual private networks". Dial-up connections typically use ISDN, V.90 or similar modems over "plain-old telephone" lines. Any type of communication link can be used, as long as it enables use of the Internet transport and routing protocols (TCP/IP and UDP/IP) and has sufficient bandwidth for the planned communications load to achieve the desired operational performance (this is based upon frequency, size of messages to be exchanged, and latency issues encountered when using C2C systems).

While the NTCIP community recognizes these three solutions, it should be noted that at the time this guide was written, none of the three approaches provided complete solutions to C2C communications. For DATEX and CORBA, the base protocols have been defined, that is, how to exchange data, but the standards defining the data to be exchanged have not reached a state of maturity. The XML approach is even less mature in that the industry has

not agreed on the exact rules on how to exchange the XML documents. Any near-term deployment should consider the impacts that this may have on the long-term maintainability of a system. The best solution is still likely to deploy one of the recognized standards, but the agency should realize that a future project would likely be required to upgrade the software to address any included features affected by revisions in order to achieve the final mature standard.

Chapter 3: Review

Questions:

1. Referring to the National ITS Architecture, NTCIP Center-to-Field protocols link which Subsystems.
   a. Center and Roadside
   b. Roadside and Vehicle
   c. Center and Remote Access
   d. Center and Vehicle

2. A dynamic message sign is an example of a device that can take advantage of Center-to- _____ protocols.
   a. Center
   b. Field
   c. Vehicle
   d. None of the above

3. A transit management center communicating with a traffic management center can take advantage of Center-to- _____ protocols.
   a. Center
   b. Field
   c. Vehicle
   d. None of the above

4. Given the five levels that make up the NTCIP Framework, Plant, Information, Subnetwork, Application, and Transport. Arrange the NTCIP Framework levels in order.
   a. Plant-Subnetwork-Transportation-Application-Information
   b. Information-Application-Subnetwork-Transportation-Plant
   c. All of the above
   d. None of the above

5. Which of the following are not Application Level protocols currently available and commonly used for Center-to-Field communications?
   a. Data Exchange (DATEX)
   b. Simple Network Management Protocol (SNMP)
   c. Simple Transportation Management Protocol (STMP)
   d. Both (b) and (c)

6. The Simple Transportation Management Protocol (STMP) uses _____ to improve bandwidth efficiency.
   a. Data elements
   b. Objects
   c. Dynamic Data
   d. Dynamic Objects

7. Which of the following are Application Level protocol choices currently available for Center-to-Center communications?
   a. Data Exchange (DATEX) and Simple Network Management Protocol (SNMP)
   b. Common Object Request Broker Architecture (CORBA) and Simple Transportation Management Protocol (STMP)
   c. Data Exchange (DATEX) and Common Object Request Broker Architecture (CORBA)
   d. Common Object Request Broker Architecture (CORBA) and Internet Protocol (IP)

8. If message routing through intermediate communications hub or field master is required, what two Transport Level protocol options are available for use with the Internet Protocol (IP)?
   a. Data Exchange (DATEX) and Simple Network Management Protocol (SNMP)
   b. Transmission Control Protocol (TCP) and User Datagram Protocol (UDP)
   c. Transportation Transport Protocol (T2, formerly know as NULL protocol) and User Datagram Protocol (UDP)
   d. Transmission Control Protocol (TCP) and Transportation Transport Protocol (T2, formerly know as NULL protocol)

9. NTCIP and non-NTCIP devices can generally be mixed on the same communications channel.
   a. Always
   b. Usually
   c. None of the time
   d. Routinely

10. True or False. One approach to the introduction of NTCIP in a center-to-field system is to operate two separate systems – one NTCIP and one non-NTCIP – during the transition period.
   a. True
   b. False

Answers:

1. (a) Center and Roadside
2. (b) Field
3. (a) Center
4. (a) Plant-Subnetwork-Transportation-Application-Information
5. (a) Data Exchange (DATEX)
6. (d) dynamic objects
7. (c) Data Exchange (DATEX) and Common Object Request Broker Architecture (CORBA)
8. (b) Transmission Control Protocol (TCP) and User Datagram Protocol (UDP)
9. (c) Not
10. (a) True, operating two separate systems is one strategy for migrating from non-standard legacy systems to standards-based systems.

Chapter 4

Procuring NTCIP

4.1 Introduction

The purpose of this section is to provide guidance to those who are responsible for developing specifications for and procuring NTCIP-conformant devices and systems. This section is written specifically to target the systems planner/specification writer, or that person responsible for preparing procurement, system design and specifications for NTCIP systems, including pre-procurement activities.

NTCIP represents a family of open communication standards for ITS deployments. Standardized communication protocols enable interoperability and interchangeability. Implementing those standards can be difficult without the knowledge of which standards are really needed and how those standards should be specified.

Systems and equipment procurement specifications sometimes include simply a sentence such as *"All components shall be NTCIP compliant,"* or *"The system shall use NTCIP as the communications protocol."* Neither these statements, nor those that simply list the NTCIP publication numbers provide information to manufacturers or systems integrators on the type, scope and functionality of the system or hardware to be implemented. While the manufacturer can derive the matching NTCIP requirements from the specifications, there is no guarantee that the manufacturer/integrator will implement them. Functional requirements that have *no* matches in the NTCIP standards will be addressed as best as possible by the manufacturer/integrator, but this manufacturer-specific approach may not be in the best interest of the agency.

Specifying detailed requirements for NTCIP is not a trivial task. It requires a great deal of study to develop a set of detailed specifications that will ultimately meet the intended needs. This section is intended to guide the systems planner/specification writer through the specification development process, pointing out key considerations along the way. This section also provides additional understanding of NTCIP when coupled with the information provided in previous sections.

It has been said on many occasions that there is no exact specification wording that can simply be copied into procurement documents. The reason for this is that there is no single system design that is standard across the country. Available resources and functionality needs vary from agency to agency and as a result, system designs vary from agency to agency.

Obviously, defining a system that encompasses all the functionality and options that are available would be a costly burden for smaller agencies to bear. Defining a system with minimal functionality would not meet the needs of many larger agencies. This section will focus on a process to follow when developing procurement specifications for systems and equipment using NTCIP.

4.2 Systems Engineering Approach

There are certain steps that should be taken in any systems procurement project to successfully meet the intended goals. Using a systems engineering approach to procurement and implementation provides for the checks and balances needed to ensure that all of the project requirements are identified and documented, and that the correct requirements are correctly implemented. Exhibit 4.1 presents a typical systems engineering model that organizations might use when considering the procurement and implementation of NTCIP devices and/or software.

"Using a systems engineering approach … provides for checks and balances…:

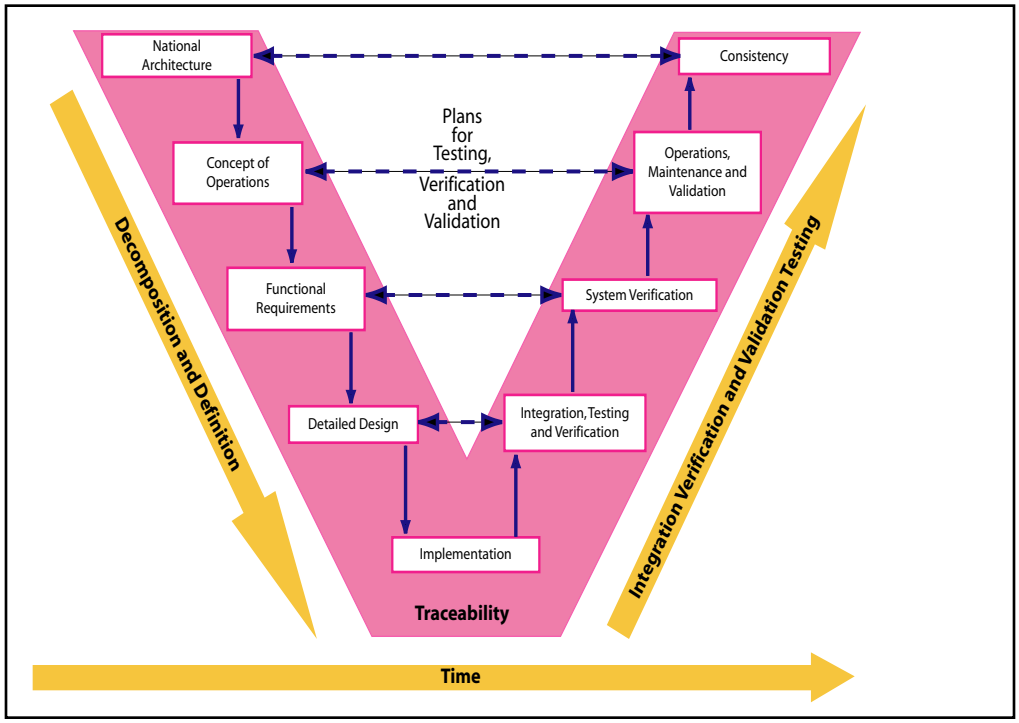


Exhibit 4.1: Example Systems Engineering Model

Systems Engineering Approach

The systems engineering approach can be represented graphically thru the use of a model. The general shape of the model is that of the letter "V", as shown in Exhibit 4.1. It is important to note that this model is simply the graphical representation of a process that should be followed throughout the life-cycle of a project.

Please note that while Exhibit 4.1 shows the model as a simple two-dimensional graphic there is also a third dimension. Thickness can also be used to represent the amount of effort at any given stage. As a result, the bottom of the "Vee" would be thicker than the top as the majority of cost and activity are typically associated with the implementation of the project systems.

The left-hand side of the "Vee" depicts the decision making process that must come before actual system construction and implementation. Notice how each task adds more detail. Part of this detail must also consider and provide for the functions on the right-hand side of the model. For example, during the decomposition and definition process, the designers must also consider how the system will be tested and ultimately operated.

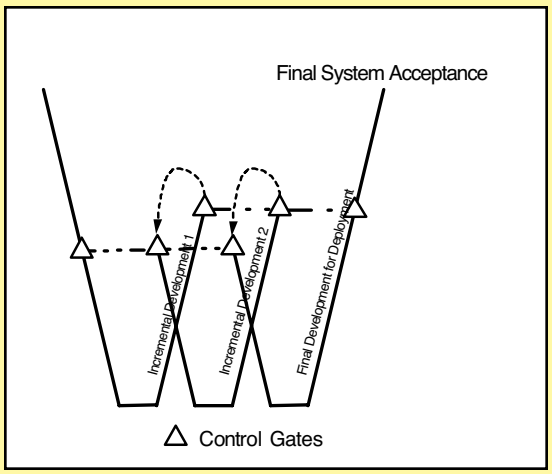
Running through the model is also the element of "Traceability," which helps illustrate that the system requirements developed during the decomposition and definition process are mapped to specific testing and verification procedures. Consider a project requirement that indicates a traffic signal system must accommodate 24 vehicle signal phases. A procedure must also be identified to test and verify that the system can accommodate the required number of phases. Without a systems engineering process testing, validation and verification might be tossed in as part of the final approval of the system rather than being an integral consideration during project development.

The cross-connects between the wings of the "Vee" also links from the integration, verification, and validation testing back to the decomposition and definition. This link is provided thru "traceability." The intent here is to show that the system successfully implements all of the system requirements identified for the project and that these are the correct requirements, correctly implemented.

The various levels shown along each leg of the "Vee" represent control points. This means that documentation of system architecture and requirements must be completed before a detailed design can be completed.

There is also a vertical dimension tied to the "time" line. This illustrates that as time moves forward each successive task builds on previous tasks and looks forward to the next task. The development team should use the Concept of Operations to build the requirements list, and, while building this list, should also be considering any implications to system design and implementation.

In actual use, the "Vee" model typically ends up looking more like a "W". The typical variations are depicted in callout Exhibits A, B and C.



Exibit A Incremental Development Single Delivery

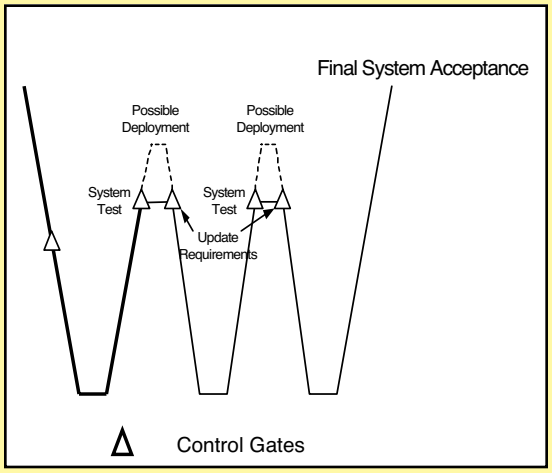


Exhibit B Evolutionary Development with Single or Multiple Deliveries

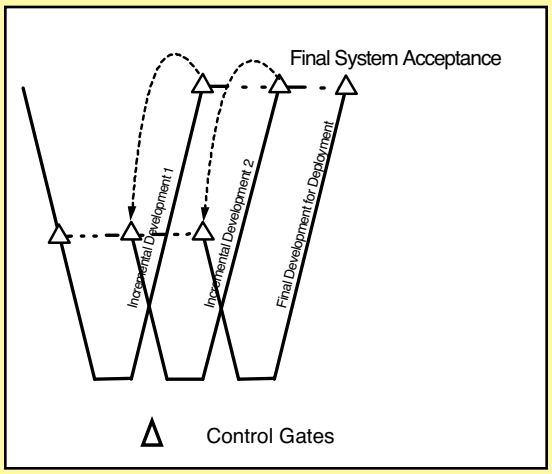


Exhibit C Incremental Development with Multiple Deployments

Configuration Management

Configuration management is a part of the systems engineering process and a critical element in the life of any system. It is particularly important in those systems that are software intensive. To people who are primarily involved in the field of transportation engineering, this is a relatively new concept.

Given today's complex Intelligent Transportation Systems, it is recommended that a plan for configuration management be implemented at the beginning of system development. As with most projects, there are legacy system elements that must be included as part of this configuration management plan.

Configuration management can have significant impact in reducing project life cycle costs. Changes to these complex systems can have a significant impact in many seemingly unrelated systems or subsystems. The time and costs to track down system errors can be reduced through configuration management. Configuration management can also help control project "scope creep" and the resulting cost and schedule impact.

Here are two definitions of configuration management:

Configuration management is the practice of handling changes systematically so that a system can maintain its integrity over time. Another name for it is "change control." It includes techniques for evaluating proposed changes, tracking changes, and keeping copies of the system as it existed at various points in time.[1]; and

Configuration management permits the orderly development of a system, subsystem or configuration item. A good configuration management program ensures that designs are traceable to requirements, that change is controlled and documented, that interfaces are defined and understood, and that there is consistency between the product and its supporting documentation. Configuration management provides documentation that describes what is supposed to be produced, what is being produced, what has been produced and what modifications have been made to what was produced.[2]

Note that both of the above definitions mention controlling and tracking changes to a system. Configuration management addresses that process.

Configuration management is often broken down into four related tasks:

- Identification,
- Control,
- Status Accounting, and
- Audits.

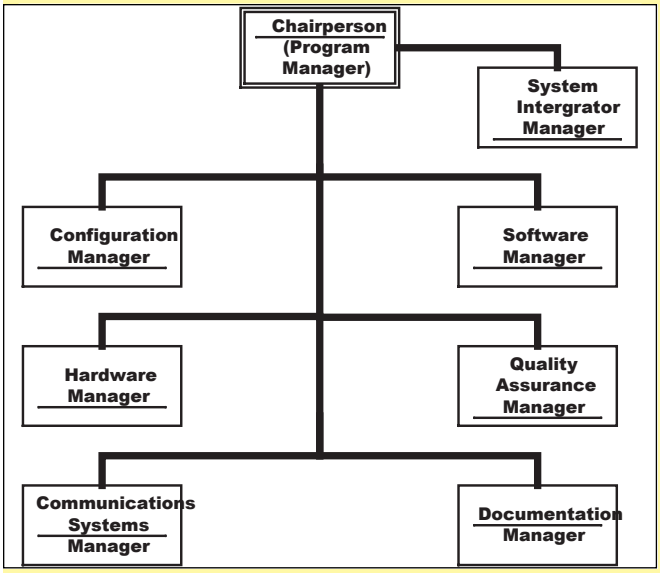
---

1. Steve McConnell, Code Complete, Microsoft Press, 1993
2. Department of Defense Systems Management College, Systems Engineering Fundamentals, Defense Acquisition University Press, December 2000

Identification – This task is often referred to as a systems inventory. It includes a scheme to uniquely identify each element of the system. Included for each unique element would be its structural relationship with each other system element, descriptions of interfaces, functional requirements, physical characteristics, version identification, and configuration identification. This is not limited to software, but must also include details of the hardware. These elements are typically called Configuration Items. With most systems, this effort must begin with legacy systems that will be reused in the system being developed.

One of the first steps would be to document what is required for each element, in detail. Several commercially available software packages are available to facilitate organizing and tracking the elements. Once the inventory has been completed, the next steps in the process are easier.

Control – Control is the systematic process of maintaining and preserving a stable system baseline—in other words, to control changes to the system. This process is typically formalized through submission of documentation of requests for change to a review body.



The change requests are often called Engineering Change Proposals (ECP). They are commonly divided into two classes. Class 1 changes require formal approval as they can result in problems with the baseline requirements, safety, interfaces, operating/servicing capabilities, human interfaces and more. They significantly change the system and often impact cost and schedules. Class 2 changes correct minor conflicts, typos and other "housekeeping" changes to correct the documentation to reflect current configuration. Within each class the request is further broken down in terms of the request type, request priority and request justification.

A formal Configuration Control Board (CCB) acts upon these proposals for change. A Configuration Control Board may be an individual or a group. They can also be multi-level depending on the degree of system or project complexity, and upon the project baseline involved. The ECP submitted to the CCB should include at least the following:

- Identification and documentation of the need for a change,
- The baseline to which the change will be made,
- Analysis and evaluation of the impact of the proposed change.

The CCB also serves a role in overall project management. One of the primary project management roles the CCB provides is to manage "scope creep" by ensuring that changes in the project requirements are truly necessary for the project to be successful.

Status Accounting – This is the record keeping and reporting function of the configuration management process. Status Accounting involves the following tasks:

- Collecting, cataloging and maintaining all configuration documentation,
- Tracking and reporting the status of all proposed changes,
- Tracking and reporting the implementation status of all approved changes, and
- Configuration of all system hardware, include those in operational inventory.

Maintaining a good status accounting operation is critical to the analysis and implementation of all future proposed changes.

Audit and Review – Periodically reviewing and auditing a system and its components' conformance to their configuration documentation should be an integral part of the process. The goal is to verify that the system satisfies their requirements. This is essentially the quality control function of configuration management. There are three common audits in configuration management.

- ***Functional Configuration Audit*** – This audit is done after all the system hardware has been tested. It matches the initial requirements to the implemented system.
- ***Physical Configuration Audit*** – This audit is done following the Functional Configuration Audit to confirm that the plans and specifications match what has been built.
- ***System Verification Review*** – This review evaluates the system engineering process itself to see if it is performing as planned.

Implementation of configuration management requires additional investment. The staff and record keeping efforts are not normally free. However, investment in configuration management must be weighed against the risks of not engaging in configuration management.

Applying configuration management techniques to a particular project requires judgment to be exercised. Too little configuration management and products will be lost, requiring previous work to be redone, while too much configuration management and the organization will be too busy shuffling paperwork to ever produce any products.[1]

The software engineering community initially developed configuration management. However, it should be noted that the biggest users of configuration management also apply it to the hardware that is needed to operate the systems controlledby , or operated on the software. Many of the Information Technology systems using configuration management are similar to the complex hardware and software systems currently being deployed in transportation management systems.

1. F.J. Buckley, Implementing Configuration Management, Hardware, Software, and Firmware, IEEE Computer Society Press, 1984

4.3 Requirements

When considering the implementation of a project, it is a good practice to understand the requirements of the devices and/or systems being implemented. Knowing these requirements up front in the project life-cycle will help to alleviate potential problems during subsequent phases. Successful projects rely on the understanding of functional, design, and testing requirements before any procurement, development or implementation.

4.3.1 Functional Requirements

The first aspect of a project should be to determine the exact requirements for the system. This will often require the development of a Concept of Operations, describing the intended operations. Afterwards, a detailed set of Functional Requirements can be developed, against which the end product will be judged. The functional requirements typically begin with the documentation of any existing operational requirements, adding any new requirements. It is important to understand that the concept of "Traceability" runs throughout the systems engineering approach. Traceability provides a linkage between each element in the systems engineering model—meaning that Verification and Validation Testing can be traced back through Implementation, Detailed Design, Functional Requirements and Concept of Operations.

In recognition of a need to provide additional information in the area of requirements for NTCIP standards, the NTCIP project will be incorporating a new format in new standards and future updates to existing standards. This new format more closely aligns with the Systems Engineering process. The main topic areas of the new NTCIP standard format are as follows:

- Concept of Operations
- Functional Requirements
- Dialogues and Sequences
- Data Dictionary (including a Management Information Base (MIB) and other items, as necessary)
- Traceability Matrix
- Conformance Clause
- Test Procedures

Note: *These topic areas would focus on the scope of the NTCIP standard itself and would not be implementation specific.*

The Concept of Operations and Functional Requirements are tools to assist the buyer agency in understanding the intent of the standard, and in determining if this particular standard is needed or not in the planned implementation. If the Concept of Operations includes all or part of what is needed operationally, and/or the Functional Requirements address some, many, or all of the project requirements—then this standard is needed!

The Concept of Operations and Functional Requirements of the NTCIP standards would then become one part of an overall implementation specific Concept of Operations and Functional Requirements. The result of the requirements definition effort, from the ITS project viewpoint, should be a detailed requirements document with which both the agency and developer can agree and be satisfied. Additional details of this investigation are given below. As a minimum, the document should address those issues identified throughout this section.

How NTCIP Standards Fit Together

Ideally, there would only be one NTCIP standard that met everyone's needs—that is collectively suitable, effective and contributes positively to the development of interoperable and interchangeable ITS implementations. However, reality requires a large number of options to meet the unique needs of specific system deployments. For example, some agencies have a large amount of twisted pair copper that they want to continue to use. Other agencies are installing new systems and want to take advantage of fiber optic cable and/or other technologies. Likewise, some agencies have fairly simple data exchange needs with field devices, whereas other centers need to exchange large amounts of information with other centers. The NTCIP accommodates these various needs by providing a family of standards, with each standard providing unique features.

Exhibit 4.2 depicts the NTCIP Standards Framework. Chapter 3 discussed how the framework is based upon five levels, including Information, Application, Transport, Subnetwork, and Plant Levels. The middle three of these five levels loosely relate to layers within the seven-layer OSI model. The Plant Level is included as a reference to show the relationship to field infrastructure. The figure shows all the various standards that reside on each level and represents the various choices that must be made during the specification development process. The connecting lines represent the compatibility linkages between the various standards.

- ***Information Level*** – Information 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.
- ***Application Level*** – Application 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

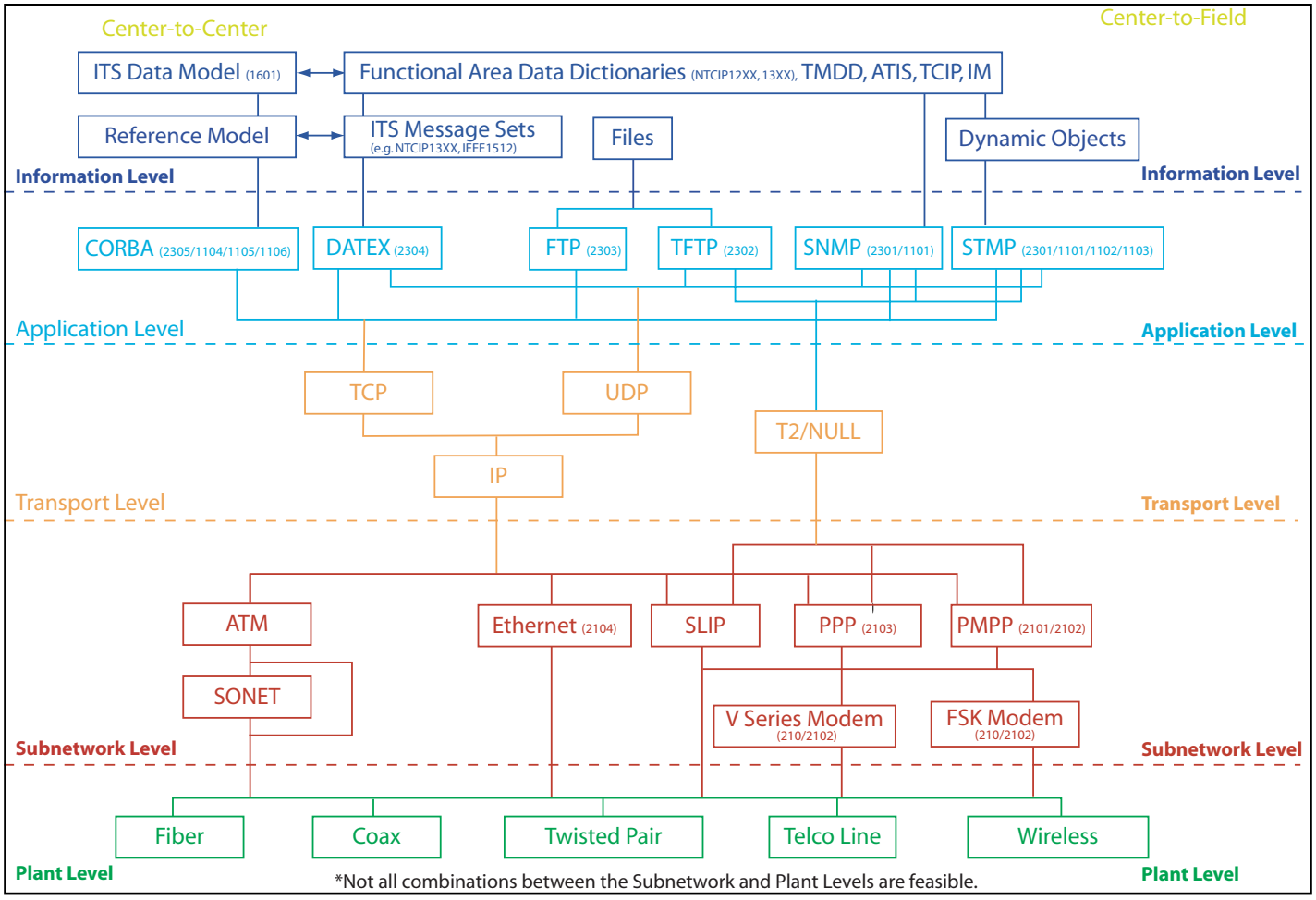


Exhibit 4.2: NTCIP Standards Framework

or a complete thought, and defining the rules for greeting each other, and exchanging information.

- ***Transport Level*** – Transport Standards define the rules and procedures for exchanging the Application data between point 'A' and point 'X' on a network. This includes any necessary routing, message disassembly/re-assembly and network management functions. This is similar to the rules and procedures used by the telephone company to connect two remotely located telephones;
- ***Subnetwork Level*** – Subnetwork 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; and
- ***Plant Level*** – The Plant Level is shown in the NTCIP Framework as a means of providing a point of reference to those learning about NTCIP. The Plant Level

includes the communications infrastructure over which NTCIP communications are intended. The NTCIP standards do not prescribe any one media type over another. The plant level is an infrastructure choice and not a standards selection choice. However, the plant level selection will have an impact on the subnetwork protocol selection to which it must interface.

Any data exchange requires the use of standard(s) taken from each of the five levels. In theory, a standard from one level should be designed such that it can be combined with any standard from another level. However, in practice, standards will often require certain services from other levels. Thus, only certain combinations are desirable and recognized by the NTCIP effort—other combinations are atypical or bad practice, and are therefore mutually exclusive.

Selecting Standards and Conformance Statements

The selection of standards for implementation is dependent on the specific requirements and design of each system. Subsequent sections in this chapter will provide some additional insight as to how to select the applicable standards for implementation. As a matter of course, agencies should work closely with manufacturers, systems developers and integrators to determine details specific to particular implementations.

One method for doing this is through the use of a proposal request that is part of the procurement process. Essentially, an early deliverable in the procurement process should be a proposal from the systems developer or integrator showing applicable details specific to the procurement. This might also include specific criteria that the agency has set forth for the expansion of existing NTCIP systems. However, the customer needs to have a solid understanding of their requirements *before* beginning any negotiations, and preferably before developing any procurement documents. The proposal request topics should cover the specific standards to be implemented, applicable mandatory and optional conformance groups, applicable data elements and their associated range values, and any other information pertinent to the procurement or implementation. If applicable, the proposal should also show any discrepancies between the new offering and the agency requirements for expanding an existing NTCIP system. The agency should provide an approval of the proposal prior to proceeding with device or software development and delivery.

"The selection of standards for implementation is dependent on the specific requirements and design of each system."

Manufacturer Extensions—Benign or Malignant

Users, manufacturers, and systems integrators have traditionally implemented functionality based upon the requirements or needs of the system being implemented. Often, these features and enhanced functionality have been implemented in different ways, depending on the manufacturer, user, or system. As such, there are a variety of alternative methods of performing some functions and accessing these enhanced features.

In many cases the standard may not support all of the features supported by a manufacturer's device or software. The NTCIP standards have been explicitly designed to allow for innovations to keep pace with advances in technology. It is recognized that the NTCIP standards do not currently define standardized data elements for every technology or functional feature of every device. Thus, there could be special features or requirements in the procurement that are not yet standardized by the NTCIP. If such features are present, then the systems developer or integrator would need to determine precisely how these features are to be supported without conflicting with the standardized implementations. Agencies should be aware of the fact that manufacturer-specific extensions might serve to lock them into that manufacturer's proprietary software.

Usually, this adaptation is accomplished by simply extending the capabilities of existing features of the standard, or by defining additional data elements or features under a developer-specific or an agency-specific node for these specific MIB extensions. It is important that the agency be aware of the use of these benign extensions and request that the systems developers or integrators clearly identify these in their proposal. Another style of extending the standard might be based on complete replacement of a partially incomplete feature with a complete custom feature. This would be considered a malignant extension, as it defeats the purpose and goals of any open standardization effort—interoperability and interchangeability. An ITS implementation that uses benign extensions is likely to achieve a level of conformity with known exceptions, for example, the specific extensions are listed. While an ITS implementation that uses malignant extensions (that is, replacement of the standard's features with custom features) should not achieve conformity as this would mislead customers, and would negatively impact the ability to achieve interoperable and interchangeable ITS.

In any case, if specific benign or malignant extensions have been introduced and the user wants to have the associated functions available in future purchases of the same device type, it is imperative that these extensions are made part of the agency's specifications and documentation deliverables. This necessity also requires that the user agency obtain re-distribution and/or re-use rights to these (MIB) extensions, even if the original manufacturers/vendors/integrators developed and implemented them. Additionally, the agency should obtain both electronic and paper copies of the entire MIB, including the manufacturer-specific extensions. It is much easier to successfully negotiate the rights for re-distribution and/or re-use, along with documenting the requirements for MIB delivery, up front in the procurement process rather than after the fact.

Software Licensing and Intellectual Property Rights

In a report prepared for the U.S. Department of Transportation by the John A. Volpe Nations Transportations Center, entitled "Successful Approaches to Deploying a Metropolitan Intelligent Transportation System, "intellectual property is described as follows for transportation systems:

> "Intellectual property refers to patentable inventions, copyrights, and trade secrets, as well as compilations of data derived from the operation of ITS technologies, which may or may not be subject to copyright protection."

The term software may take on a variety of different meanings. It is important to understand that software may include a variety of different things, including source code, executables (object code) and documentation. The rights that are associated with each of these software components may be different and should be explicitly addressed in any procurement documents.

With regard to a software procurement and/or development project, we must ask ourselves a couple of questions:

- Who owns the software being implemented?
- What rights do I have as a user?

It is important to understand the difference between ownership and right to use. *Right to Use* licensing implies restricted rights of use and distribution, whereas ownership may only be minimal or non-existent. On the other hand, it is impractical to assume that *Ownership* rights will be granted for software development unless your project fully funds such development. Obtaining ownership rights for software can be an expensive proposition. Those procuring software should be aware of the fact that their right to ownership does not extend beyond development that is wholly funded within their project, unless the software developer is adequately compensated for his intellectual property. There are important cost implications to consider when evaluating which approach is right for your agency. It is important to remember that resolving intellectual property rights must be done *prior* to contract signing.

> Example: A medium-sized city is about to enter into a contract with a systems integrator to provide central software for a traffic signal system, and a field hardware supplier to upgrade their traffic signal controllers. The city has included in their procurement requirements for the "…systems integrator to provide a copy of the source code along with the software…" for their project. Also, they have added another requirement that gives them "…the right to give the software to peers within their state."

Question – Has the city adequately addressed the software licensing and intellectual property rights in this project?

Answer – No, the city has only addressed the project deliverables and not the intellectual property rights issues associated with the project. The city will need to ultimately negotiate the rights that they will have for source code, executables (object code) and documentation. These rights will need to address access to these software components by themselves and future contractors, use of these software components by themselves and future contractors, and delivery to others. This process is referred to as a negotiation because obtaining these rights is not free. The city will need to carefully weigh their needs against the cost of obtaining the necessary software licenses and intellectual property rights.

Question – What can the city do with the source code?

Answer – Unknown, the intellectual property rights are not defined in the excerpt for the source code. Many system procurement projects add a clause requesting delivery of source code as a means of "protecting themselves" without a clear understanding of what the component is, what it is good for and what liabilities are incurred if it is ever modified. The source code represents a listing of a computer program in its native programming language. In order for source code to be used, it must first be compiled and the city would need to have access to the appropriate software tools and expertise to accomplish this task. Obtaining the source code does not really offer much protection, since it often requires the original software developer to understand the nuances of how it is put together. The city would need to employ sufficient staff with the technical expertise to potentially maintain and modify the software. Then, if the city is to ever modify it for their use, it is likely that warranties would be voided and product liability would be shifted to the modifying agency. Obtaining the source code on a transportation system project may only prove to be a hollow victory.

Question – Are there issues associated with sharing software to peers?

Answer – Yes, the city must understand the cost impacts that are associated with making the software product available to others and providing technical support to those recipients. The city should carefully weigh the costs associated with buying the rights to software that they will generously provide to their peers against their available budget. In some cases, it may make sense for one agency to take the lead in procuring software for the implementation of a regional management system that comprises a few multiple jurisdictions. The city must also understand that they may be called upon to provide support and technical assistance to the peers to whom they have provided software. In some cases, sharing software to partners in a regional management system may make sense, however, incurring the costs associated with a statewide procurement may be overly generous for a medium-sized city.

While many of us understand the importance of dealing with software licensing and intellectual property rights on large software development, systems integration, and C2C communications projects, we often overlook these issues on smaller system and field hardware procurements. Addressing software licensing and intellectual property rights are important, regardless of the scope of the project. This even includes the MIB in field hardware that is used for C2F communications.

In the case of C2F communications, it is important that agencies address access, handling and distribution of MIBs. Systems integrators and other device manufacturers will need to be able to use current MIBs to expand agency systems. The following questions need to be addressed in C2F procurement documents:

- What rights do I have in using the MIB (for both the standards portion and the manufacturer-specific portion)?
- Do I own this MIB or do I simply have the right to use it?
- What rights do I have to utilize the MIB in future system expansions?
- Do I have the right to give the MIB to my systems integrator or another device manufacturer who is working on a project within my system?
- In what form will the MIB be delivered to me (electronic and/or hardcopy)?

Regardless of the magnitude or scope of the transportation system project being developed or procured, it is important to address software licensing and intellectual property rights as quickly as possible. These issues should certainly be addressed prior to the signing of any contracts.

4.3.2 Design Requirements

The systems planner/specification writer should consider the various levels of the NTCIP Framework when preparing procurement specifications. Appropriate choices from each of the five levels that make up the NTCIP Framework will need to be made as soon as possible during either the operational concept, requirements analysis, or design specification development process, or subsequently during the procurement process. One alternative that has been presented in this section, places much of the responsibility on the systems developer or integrator to assist agencies in making the appropriate standards selections. This approach requires a mechanism for agency approval. Another alternative puts the burden for detailed specification development on the procuring agency.

It is important to understand that if the agency is planning to prepare detailed procurement specifications for NTCIP-conformant systems, there are several issues that must be addressed in order to satisfy basic specification requirements. These basic requirements consist of making the appropriate choice of standards for each level within the NTCIP Framework. To effectively make these selections, a good understanding is necessary of what resources, like existing communications infrastructure and equipment, might be available from an existing system. Additionally, a good understanding of what functionality is needed from the NTCIP-conformant system is required. Exhibit 4.3 presents an overview of a basic

checklist for use in preparing detailed specifications for NTCIP systems. Detailed procurement specifications will first require knowledge that is specific to the system implementation, such as infrastructure media; communication, processing and data needs; and, intended system functionality.

Exhibit 4.3: Procurement Check-List Overview

- ❑ Consider specific communications needs by developing functional requirements
- ❑ Analyze available resources
- ❑ Define an entire NTCIP Stack for intended system(s)
- ❑ Gather appropriate standards for each level within the NTCIP Stack by matching functional requirements with NTCIP standard functions and options
- ❑ Determine required Conformance Groups
- ❑ Determine required Data Elements (objects)
- ❑ Define realistic Range Values for implementation
- ❑ Determine all functional requirements that could not be matched
- ❑ Develop tailored specifications to meet intended needs not addressed by the NTCIP standards
- ❑ Do not allow exceptions for subsequent proposal if the existing central systems is to be used without modification

In order to effectively prepare detailed specifications for an NTCIP-conformant system, the systems planner/specification writer should consider the functional and operational performance impacts on the communication needs and available resources specific to the system being deployed. Important considerations for determining specific communications needs include communications data and timing, channel loading, and device latency issues. An entire NTCIP *stack* should be defined, along with an identification of standards required at each level.

In his book Understanding SNMP MIBs, Perkins defines MIBs as follows:

MIBs are specifications containing definitions of management information so that networked systems can be remotely monitored, configured, and controlled.

The next step in the process would then be to determine the required optional and mandatory Conformance Groups within each standard that are needed to ensure that the intended functionality needs are met. These conformance groups contain the objects, which in turn define the "features" of the standards. These features of the standards are what enable the requested functionality within the implementation. Each feature derives from one or more objects within the standard—a one-to-many relationship. Some objects are used with a single feature; others are reused across several features. Using a bottom-up approach, the selection of conformance groups pre-determine, may limit, what functionality is enabled as a consequence of the choices made. PA better process of selection might be to use a a top-down approach, where the required end system functionality determines which conformance groups are needed to provide the features that enable that stated functionality.

Additionally, once the selection of conformance groups and their included data element/object sets are made, realistic Range Values need to be defined for each of these data elements, or data objects, within each of the MIBs. These range value choices are made based upon the functional requirements of specific device specifications. It is important to remember that detailed NTCIP design specifications can, and should be, tailored to meet the intended needs of the system being implemented. It costs more to acquire more functionality than is truly needed.

The project scope, deliverables and procurement specifications should also include information related to hardware and/or devices, systems integration, testing and device configuration. These specifications should also address the ownership, re-distribution and/or re-use rights of the MIB, as well as the requirements for documenting and obtaining the MIB. It is recommended that procuring agencies obtain final electronic and paper copies of the MIB(s) used in their system including both standardized data elements and manufacturer-specific data elements. Re-distribution and/or re-use rights should be clearly spelled out at the onset of the project so that future expansion and integration issues can be minimized. Overall, a comprehensive set of system requirements, design and procurement specifications will help the system/hardware implementation proceed more smoothly and with less ambiguity.

4.3.3 Testing Requirements

Testing for NTCIP conformance is a subject that has been on the minds of many of those going through the process of implementing NTCIP. The biggest question that often arises is: "How do I know that my device is NTCIP conformant?" Other concerns include how to do testing and what tools are available for testing. Testing is a critically important and inherent part of any systems engineering, acquisition and procurement process, that cannot be overlooked. However, before any testing can be done, it is imperative that there exists a detailed definition of how conformance will be judged.

Testing for NTCIP conformance can take several forms. The simplest being from the perspective of determining if a device will accept data elements transmitted using NTCIP, to the more complex notion of ensuring that the device provides the appropriate functional response for the message that was received. Complex testing also ensures that it does not produce false errors or unpredictable results for messages and data it does not understand or that are addressed to another device, for example, when sharing a communications channel with other devices of the same or a different type. While it is not the purpose of this publication to define functionality or specific testing procedures, it is important for agencies to plan for, and then rigorously test devices and systems to ensure NTCIP conformance. Early implementation life-cycle testing will avoid future heartache when the need for interoperability and/or interchangeability arises. Testing for NTCIP conformance will likely need to address message structure and content, as well as the appropriate functionality responses to the messages transmitted.

One tool that is available for use in NTCIP C2F testing is the NTCIP Exerciser. This software tool was developed for testing the ability to properly transmit and receive NTCIP data elements. The tool is designed to verify the C2F communications process by allowing the user to determine if the messages are in a transportable NTCIP format. Functionality testing to determine if the appropriate operations occur as a result of the transmitted message is left to the user and is not a function of the Exerciser. It is stressed that the NTCIP Exerciser is a primitive yet very powerful tool at the disposal of testing agencies for use in a comprehensive testing program.

Other commercially available tools, such as protocol analyzers and line monitors, provide a view of the communications channel between the central facility and the devices. Line monitors will provide a bit-by-bit or byte-by-byte view of all data exchanged, leaving the analysis of the data (for a determination of conformance) up to the tester. Protocol analyzers not only provide a bit-by-bit or byte-by-byte view of the exchanged data, but also provide the user with an analysis of the observed data for making a determination of conformance somewhat easier. For example, the observed data might be a valid SNMP packet from the device with contents equal to "123". These tools can be connected between the controlling computer and the field device in a typical C2F environment.

While most off-the-shelf protocol analyzers will not allow analysis of the transportation-specific protocols (such as NTCIP 2101/2102 and NTCIP 2201), they will allow analysis of common computer industry protocols such as SNMP (NTCIP 2301), UDP/IP (NTCIP 2202) and PPP (NTCIP 2103). The advantage of using protocol analyzers over the NTCIP Exerciser is that the tester can test systems by executing commands from the NTCIP-conformant central computer and observe the results on the field device. An appropriate protocol analyzer will do an analysis of the exchanged data and report the results. This method avoids the requirement of a detailed knowledge of the NTCIP protocols. However, testing might be limited by the capabilities of the central computer. Most central software operator interfaces are not likely to allow entry of illegal data values or improper commands. Negative testing on these systems by sending wrong checksums or value-out-of-range checking would not be allowed.

4.3.4 Procurement Request

The procurement request can take many forms. Devices are often purchased through a low-bid process administered by the agency. Software is routinely procured through service-oriented contracts. As such, the specifications and requirements that are made part of the procurement package can range from detailed specifications to more general requirements documents. The procurement of NTCIP-conformant devices and software does not change the normal procurement methods that most agencies use. Additional steps may need to be added to traditional procurement processes to ensure an adequate understanding of the intended requirements for NTCIP related procurements, and adherence to the standards and specifications.

4.4 Design

After the identification and documentation of Functional Requirements, Detailed Design can commence. This element focuses on the specific design issues encountered when preparing the procurement documents, or plans and specifications.

4.4.1 Implementation Alternatives

The agency should be aware that manufacturers, systems developers and integrators have a variety of hardware and software resources available to implement desired features and the proposal should address these alternatives. For example, the developer may be able to acquire off-the-shelf software to minimize the effort required to implement the features. If this needs to be computer, operating system, or database specific to be compatible with an existing system infrastructure or support staff capabilities—that needs to be specified in the contract requirements for the implementation. A layered hardware and software system design will minimize the effort required to maintain the code and to implement and introduce different standards in the future. However, these benefits may impose other constraints on the system. A related phenomenon is that over-specification can significantly limit or degrade the expected competitive response time.

The NTCIP has used widely recognized standards whenever possible. For example, the NTCIP standards reference the Transmission Control Protocol (TCP), Internet Protocol (IP), Simple Network Management Protocol (SNMP), Common Object Request Broker Architecture (CORBA) and High Level Data Link Control Protocol (HDLC) standards to name just a few.

In many cases, private industry has developed off-the-shelf tools to aid system developers in implementing these protocols. Being aware of what products are available off-the-shelf, inherent in an operating system or browser, and their associated cost will allow the agency to set a reasonable expectation, and the developer to provide a more realistic estimate of development costs. For example, some developers may use an off-the-shelf implementation of TCP/IP rather than creating their own. Standards for which there are known products include:

- File Transfer Protocol (FTP)
- Trivial File Transfer Protocol (TFTP)
- SNMP
- CORBA
- XML
- TCP/IP and UDP/IP
- Point-to-Point Protocol (PPP)
- Ethernet

While off-the-shelf software can save a considerable amount of development time and greatly simplify maintenance of the software, it may not always provide the most efficient implementation. Off-the-shelf software has generally been designed in a layered fashion for easy maintenance and fully generic use. However, real-time system performance can frequently be improved by violating the strict rules of a true layered-design and by embedding customized optimization code for a specific purpose. The agency should be aware of the benefits and detriments of each approach before approving such a development approach and cost estimate.

It should also be recognized that the availability of off-the-shelf tools might affect the selection of features to be included in the requirements document.

4.4.2 Other Issues

There may be a variety of other issues to be addressed in order to finalize a proposal request. Each of these issues may impact the proposed budget, schedule and/or scope. They should be explicitly addressed in the proposal in order to manage expectations. Without the management of expectations early in the process, a product that the developer believes is conformant may be perceived to be lacking by the agency. A sample of these issues is provided in the following subsections.

Stability of the Standard

The NTCIP standards are still relatively new and all standards are subject to amendments and revisions. For some standards, efforts are underway to develop a Version 2 that expands the coverage of functions addressed by the standard. Amendments typically result from developers attempting to implement the subject standard and recognize either a technical inconsistency or completeness problem, ambiguous wording, or the technology itself has advanced. Thus, new standards are frequently amended to solve these problems and the standards become more mature and more stable over time. Requiring the use of unproven standards can be risky. If an agency intends to pursue early adoption and implementation of emerging standards they should work closely with manufacturers, systems integrators and developers in order to make informed choices. It should be noted that a degree of risk will remain until more manufacturers and system providers have fully implemented the NTCIP standards.

Support of Amendments

Because the NTCIP standards are relatively new, the agency must consider what will happen if an amendment or a new version to the standard is approved during the life of the project. As a general rule, it may be difficult to require developers to support amendments or revisions that are made late in the systems engineering life cycle. However, many times a draft amendment may be present during the initial procurement stages and the agency should require developer proposals to address the existence of any amendments or proposed amendments. If a subsequent batch of field devices are accepted based upon

conformity to amendments and/or revisions, it should be expected that some new functions will not likely be available from these new devices when using existing central system software that only conforms to a previous version of the standard. If this "backward conformance" is required, those requirements need to be clearly stated in the procurement specifications—in any case, backward compatibility may, or may not be achievable depending on the advancement in the standard, and/or the advances in the related hardware or software technologies.

Agency/Developer Understanding

Another factor to consider is whether the procurement requirements provide realistic expectations at the start of the project. This will ultimately help ensure that the project is perceived as a success. While the NTCIP provides a standardized interface that is flexible enough to meet various needs, it may be more bandwidth intensive than previous systems and/or it may use a slightly different database design. The use of a proven systems engineering life-cycle process will assist in managing these expectations.

Additionally, it may be possible that any off-the-shelf product cannot meet certain detailed NTCIP requirements. In this case, the agency should work with the manufacturers/vendors and system developers/integrators to determine the acceptable exceptions to strict conformance, and how those exceptions apply, for example, no impact, negative impact, consequences, in their operation and functional situation. Explanations from the agency perspective as to why more fully compliant implementations are needed might also need to be provided.

Conformance and Certification Process

The agency must also consider how the procured devices and software are to be tested for NTCIP standards conformance, interoperability, and interchangeability. Many agencies currently perform in-house testing and approval of products meeting their specifications. Otherwise, consideration should be given to the manner in which conformance testing will be performed. In any event, details of test procedures should be clearly stated in the procurement documentation.

The ongoing overall ITS standards development effort is determining the spectrum of user testing needs, This includes, what support is needed for testing, testing tools, conformity assessment, certification, and user testing. It is likely that the standards, especially the NTCIP standards, will be amended to include suggested test cases and procedures in an informative annex to the standard, for example, helpful but not required. These anticipated test cases will be independent of the keystrokes or mouse clicks that operators will ultimately use in the standard; but, they will be easily reusable in constructing the project-specific test procedures for implementations that eventually use the standard.

Each NTCIP standard contains a "Conformance Clause" which clearly states the requirements for conformance to the standard by implementations that embody that standard. Depending on the complexity of the standard and the resulting implementation, it can be fairly easy or it can be very difficult to determine conformance.

The outcomes or a "conformity assessment" are limited to: pass, pass with exceptions, and fail. This determination is based on examination of the implementation through testing with a well-defined test suite. This test suite embodies the test cases, procedures, and expected results for exhaustive examination of the implementation against the requirements for conformance to the standard. If an implementation meets all requirements exactly—then "Pass." If it meets most requirements with a few exceptions—then "Pass with Exceptions" and these exceptions would be listed in a test report. Lastly, if the implementation does not meet a majority of the requirements—then it should "Fail" to achieve conformance.

When an ITS implementation achieves conformance to the standards it embodies, it then becomes a candidate for "Certification." Certification might be awarded by an accredited industry forum as an official recognition that the product meets the stated requirements for conformity to the standards.

Conformance testing and assessment of NTCIP devices can be accomplished in three ways: 1st-Party, 2nd-Party and 3rd -Party. 1st-Party certification is when a manufacturer or system provider performs their own well-defined conformity assessment and then asserts the implementation is certified as conformant to the standard(s) embodied. Next, a 2nd-Party certification is similar, but is performed by an agency performing their own conformity assessment and then asserting their certification of that conformance.

Lastly, 3rd-Party certification is done by an independent service provider. This 3rd-Party approach is typically an accredited laboratory that provides a well-established and robust capability for conformity assessment and reporting of test results to the industry certification authority or forum. A 3rd-Party lab benefits from a centralized, consistent approach with repeatable results. It does not obviate the conduct of 1st- and 2nd-Party processes, but rather it can supplement them through harmonization and configuration management of the approved conformance test suites and technical support provided to those who endeavor to do 1st or 2nd-Party testing.

The development of test suites for the determination of NTCIP conformance is under discussion as of August, 2002. It is anticipated that the actual development and fielding of initial conformity assessment tools will follow in the near-term. The NTCIP Exerciser, mentioned in this guide, is one available tool for low-level C2F 1st - or 2nd-Party conformity assessment.

Conformance differs from Compliance—the former is based upon and judged with respect to specific and unambiguous exact usage of the standard. The latter, compliance, is often used ambiguously to mean conformance, but it is less exact in its requirement to adhere to the standard. The term compliance is most often used in contractual language to assess the legal determination of meeting or not meeting the specifications of the contract.

Performance Issues

The agency should also realize that the flexibility of NTCIP also comes at the price of a more complex system than the industry has traditionally deployed and used. The NTCIP system may trend toward more sophisticated processors or better communication facilities than traditional systems in order to provide the same performance level (such as, operational response times). If the agency overlooks these issues during the early stages of the requirements analysis process, there could be significant implementation problems or setbacks late in the project to gain the necessary acceptable performance.

4.5 Bridging Between Detailed Design and Implementation

Bridging the gap between Detailed Design and Implementation is the release of the actual procurement documents. The selection of the most appropriate procurement method is traditionally made prior to the completion of the detailed design phase in the project life-cycle. On the other hand, receipt of the procurement response is traditionally part of the Implementation element shown in the systems engineering model.

4.5.1 Procurement Methods

Two alternative approaches can be used when considering the preparation of procurement documents for NTCIP systems and devices. One approach is for the agency to solicit a proposal during the procurement process that allows the manufacturer, vendor, developer, or systems integrator to present detailed information on how the intended system or device conformance with NTCIP standards are to be achieved. This method of procurement relies on the preparation of general requirements documents during the initial stages of the procurement process. These requirements should be as detailed as possible to better ensure that resulting responses provide sufficient information to make a fair and even comparison of competing alternatives. At some point thereafter, either during selection or after award, the agency solicits for their approval, a detailed proposal from the systems developer or integrator that presents detailed information as to which specific standards, conformance groups, data elements and range values can be provided to meet the procurement requirements. Additionally, any other pertinent information should be included. The

proposal submission and approval process described here might be somewhat iterative, depending on the specific requirements of the agency. This approach, however, is not appropriate for the procurement of a subsequent batch of field devices where the existing central system software is to be re-used.

Another method of preparing procurement specifications is the development of detailed NTCIP system or device specifications, in addition to any detailed functional specifications. This route requires knowledge of both NTCIP standards and the device or system functionality required to meet the intended needs. Pursuit of this alternative would require the agency to make the necessary selections at all levels within the NTCIP Framework and determine an NTCIP stack that will meet their needs. Specific NTCIP standards, conformance groups, data elements and range values will need to be identified as well. This method of procurement document preparation will require some expertise in both communications and systems design, in addition to knowledge of the intended device or system functionality. While procurement specifications can use either approach for an initial procurement, the latter approach is appropriate when existing central system software is to be re-used without modifications.

4.5.2 Procurement Response

In order to ensure a thorough understanding of the procurement requirements, the agency should request that the systems developer or integrator submit a proposal for agency approval that acknowledges the various issues addressed through the development of detailed design plans and specifications using the systems engineering approach. This proposal should also specifically address issues such as conformance requirements statements and range values as appropriate. Additionally, any compliance requirements that are unique to the specific procurement or implementation should also be addressed in the proposal. The proposal provides an opportunity for the agency, device supplier and the systems developer or integrator to form a better understanding of the NTCIP implementation and reach consensus on issues that might be unique to the specific procurement.

If the proposal responses included any conformance or compliance deviations to the specifications, the agency will have to decide whether or not to allow them. If exceptions are allowed, the agency should identify the impact of these exceptions. Granted exceptions will need to be reflected in the agency's specifications to ensure that future procurements will be interoperable and/or interchangeable. It is considered a good practice to include a review of any exceptions by all those involved in the project, such as agencies, manufacturers, vendors, developers and/or integrators.

Exceptions could come in the form of those specifically allowed within the standard and those that render an implementation non-conformant. Working within the context of what is allowed within the standard will promote and enhance future interoperability and interchangeability. As stated in "Manufacturer Extensions—Benign or Malignant" on page 4-11, malignant extensions are exceptions that detract from the intent of the standard and should be avoided.

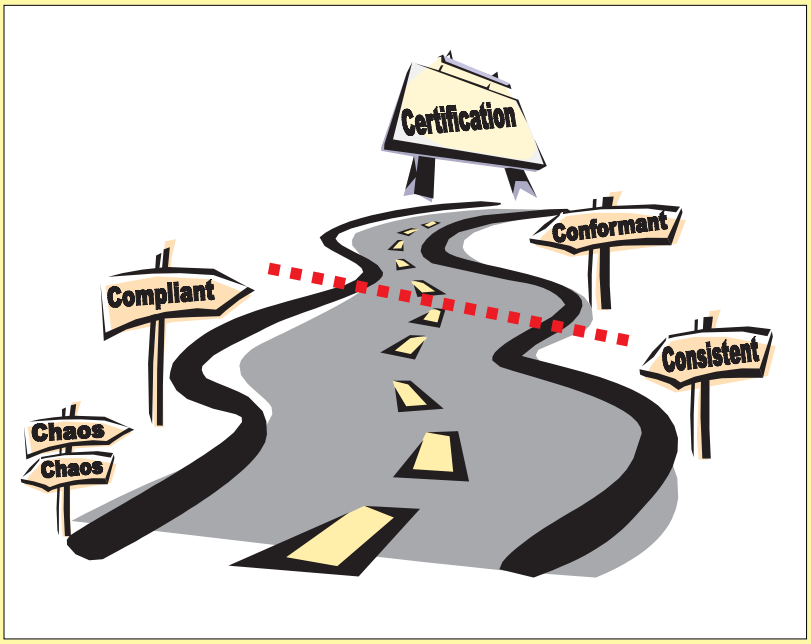
4.6 Testing

Another important aspect of the systems engineering model is delivery and acceptance testing. The agency should be aware of any time constraints that might be required for the development of new software that comes as a result of implementing a new standard. Before any testing begins, there must be a clear statement and understanding of the requirements that must be met and the minimum acceptable performance levels. All testing should then be based upon, and derived *only* from, these agreed upon requirements. Each requirement has a test, and each test traces to a requirement. In the case of NTCIP, test procedures should be aligned with the accepted NTCIP requirements.

Upon delivery, the agency should conduct acceptance testing to ensure that the device or software conforms to the functional and contractual procurement requirements (or accepted manufacturer responses) and is conformant with the applicable standards. The agency should require that acceptance testing be covered in the system developer's or integrator's proposal. It should be realized that the NTCIP is a very complex set of standards and it is impractical to perform 100% exhaustive testing. Well-designed test plans can be produced to provide comprehensive testing, reduce acquisition risk, and provide a high level of confidence for a reasonable cost. Agencies should be aware that this testing should involve more than a test of the user interface. All tests should have quantitative and measurable results. In some cases, the agency may want to include any applicable test plans as part of the procurement documents.

There are three levels of testing considered in *The NTCIP Guide*: (1) unit testing, (2) integration testing, and (3) system testing. Agencies might also require and specify "Burn-In" testing to identify and reduce the risk of infant-mortality failures, and/or "Stress Testing" to operate the system at capacity to identify any peculiarities or affects on operational performance or functional capability. If needed, the burn-in test can be associated as a subset of the integration test, and the stress test can be associated as a subset of the system test.

Testing and Product Conformity



Achieving interoperability can be seen as a passing of milestones along a road toward increasing adherence to standardization concepts. As we see in the figure, our journey along the "road-to-certification" begins with chaos, where there is essentially no standardization. Moving beyond this chaotic state, there are increasing degrees of standards adherence that result in the pinnacle of certification. Some have theorized that the milestones preceding the dotted line represent project level assessments of components and subsystems, while the milestones lying beyond pertain mainly to the degree of exactness between the implementation and the specifications of the standards themselves.

When referring to the "road-to-certification" exhibit, it is believed that the crossing of the dotted line and moving from the compliant milestone to the conformant milestone requires strict adherence to standards. In this discussion, we will concentrate on the application of these principles as they pertain to the development of a testing program for implementations that embody standards being developed for the transportation community.

Defining the requirements for conformance and placing a statement of such in each standard is something that NTCIP has been doing since the publication of our first standard. As we learn from the implementation of these standards, we have added additional information in this area and we are now including a Profile Implementation Conformance Statement (PICS) in newer documents. Overall, an explicit definition of conformance, a "Conformance Clause" must be contained in each standard.

```
VALIDATION:
Am I building the right thing?

VERIFICATION:
Am I building the right thing right?
```

The next step in the evolution of NTCIP standards documents will be to develop appropriate conformance tests for judging adherence of an implementation to the standards. When we talk about judging adherence to standards, the concepts of validation and verification

come to mind. Validation is the process of determining the degree to which a model is an accurate representation of the real world from the perspective of the required and intended uses of the model. In other words, have we built the right thing? Verification is the process of determining that a model implementation accurately represents the developer's conceptual description of the model and the solution to the model. In other words, have we built the thing right? The Joint Committe on the NTCIP is dedicated to ensuring that these concepts are the basis for any testing program that we pursue.

With all this said, where do we go from here? The Joint Committe on the NTCIP has taken steps toward facilitating effective and efficient testing for real-world implementations of NTCIP C2F and C2C standards. The Joint Committee believes that the highest priority item is the development of standards-based test cases, which can be reused to construct testing procedures and plans. The more atomic level test cases help in the quality design of the standard itself, the test procedures and plans assist in the product and systems testing done by the manufacturers and buyers of ITS. At their December 2001 meeting, the Joint Committe on the NTCIP affirmed the following recommendations for how these testing procedures will evolve and be packaged:

- A Testing Working Group will be established and tasked with the responsibility for creating a framework within which test cases can be developed by individual functional area working groups. The Testing Working Group is also tasked with the responsibility of investigating suitable testing tools for use in conjunction with the implementation of NTCIP test cases, and resultant testing procedures.
- Specific test cases will be developed with defined variables and with a sampling of what those variables should be in a conformant implementation.
- The test cases will most likely be packaged as an Informative Annex in each standard.
- A single separate document may be developed for any generic material as needed (possibly in the 8000 series of NTCIP documents).
- *The NTCIP Guide* will seek to include guidance on how to put all of the testing pieces together, as the testing activities evolve.

These initial steps are envisioned to move the NTCIP standards effort further down the road, toward ITS interoperability and interchangeability. System acceptance testing is seen as a critical component of successful systems deployment. While the testing of ITS products to determine their conformance to the standards continues to be a topic that is on the minds of many within the transportation industry, the establishment of the NTCIP Testing Working Group is seen as the first step toward initiating suitable guidance for the full spectrum of testing within the NTCIP community.

4.6.1 Unit Testing

Unit testing focuses on comparing an implementation against the standards and specified options. This may be performed by inspecting the code to use "proven" software to send test messages to the device. This process should be formalized by documenting a specific test procedure that will be followed, and the result of each step of the procedure should be recorded during the test. Unit testing is most effective when field conditions are duplicated to the greatest extent possible.

Unit testing provides a basic level of validation and verification that a product is conformant to a standard. Often, the test plan will be designed so that the failure of one procedure will provide a clear indication of what problem resides within the implementation, thereby minimizing the cost of finding and fixing the error or "bug." A device that fails such a test plan would almost certainly not be able to interoperate or be interchangeable with other systems. A device that passes such a test has less risk, and a reasonable probability of interoperating and interchanging with others. However, any performance issues encountered during unit testing must also be considered and weighed against the overall operational system requirements.

4.6.2 Integration Testing

Integration testing consists of connecting two or more devices together and exchanging data. Assuming that the individual devices and subsystem components have previously passed a sufficiently designed unit test plan, and the devices or subsystem components support the same ITS operational and/or functional features, the devices should integrate together fairly easily. However, a few problems may arise during this phase of testing. Examples include two different interpretations of a specific requirement, which is typically a problem of newer standards, problems related to system timing between the two implementations, and implementations of manufacturer-specific extensions.

In theory, the unit test should be thorough enough to prevent any problems in integration testing. However, the integration testing phase provides a higher level of confidence that the system devices and subsystem components will interoperate and that nothing has been overlooked.

If burn-in testing is desired, it can begin and continue concurrently with integration testing. A general rule-of-thumb for burn-in testing criteria might be that all devices or subsystem components must survive the first 30-60 days of testing and/or operational use. Further, the agency may specify that any failures that occur during that period will be declared as "infant-mortality" and must be repaired/replaced by the system provider or manufacturer.

4.6.3 System Testing

A final level of testing is system testing. At this level, each device on the system is integrated together to form the final complete and operational system. This level of testing should identify any global problems with the new systems as well as any issues with legacy systems, site infrastructure, power, and signal.

Agencies should note that there could be great similarity or great diversity in the conditions of integration testing versus system testing. Systems testing must be done in the actual site operational environment. This introduces nuances of the site's quality of service for power and signal telecommunications, which can have a significant negative affect on the system. This may also be the first time that the real operations staff have been able to have hands-on time with the system, and they may discover system anomalies or training issues. The same would be true for agency maintenance staff—they may discover problems with system problem identification, diagnosis and troubleshooting tools.

On the other hand, integration testing is very likely to begin in the factory, then continue and conclude on site. The in-factory phase is appropriate to minimize the introduction of site-specific issues when ironing out that last few remaining "bugs" as the system components are integrated for the first time. It is suggested that agencies should require that final integration testing must be completed on site prior to the start of system testing.

Once again, in theory, devices that successfully pass unit testing and integration testing should pass the system level testing as well, given that the system was properly designed. However, the final check is only provided when this system test is performed and any problems that arise at this stage are corrected.

It may also be desirable to include a stress test as part of system testing. A stress test attempts to operate the ITS devices and/or component subsystems at their maximum capacities to determine if there are any remaining hidden interactions that affect operational performance or functionality. It may, or may not be possible to operate the system at maximum capacity; for example, will the drivers cooperate? An alternative may be available through simulated stimulation of the system, for example, insertion of maximum traffic counts from the field. While it may not be conclusive, a well-designed simulation for stress testing can reduce risks and provide assurances that there are no remaining performance "bugs" in the system.

4.7 Maintenance

Agencies should be aware of the fact that system requirements, design and procurement specifications may need to address operational maintenance, version maintenance and subsequent device and/or software upgrades. Operational maintenance requirements take into account the reality that ITS devices and component subsystems are often deployed over a wide geographical area. This necessitates a need, and requirements for fault detection, remote troubleshooting and diagnosis to avoid costly travel to a device site without the proper tools or replacement parts.

With respect to version maintenance and upgrades, it should be recognized that the NTCIP standards are still relatively new and changes may occur to the standards. Further, as there are relatively few implementations available, ambiguities may still be discovered in the standard, and the standards may be modified in order to correct these problems. In addition, standards will evolve over time with advancements in technology. Any such change may require a modification to deployed equipment if the equipment is to maintain conformance with the newer version of the standard. A basic understanding of requirements for version maintenance and subsequent upgrades should be addressed early during the procurement process with the systems developer or integrator.

4.8 Center-to-Field

Exhibit 4.4 builds on the preceding discussion by expanding on the considerations that should be addressed during the initial planning and development stages for procurement documents. The checklist includes items that the device manufacturer and/or systems developer/integrator should provide as part of their proposal submission. In the case of an agency pursuing the detailed specification route, these items should be addressed in the procurement documents. The checklist also points to additional resources that are available in further refining detailed specifications.

Example 4.1 Example of a C2F Stack using SNMP

This example shows one possible path through the NTCIP Framework for the commonly referred to and published Class B Profile. It should be noted that the preferred terminology for this path is "stack", rather than profile.

Exhibit 4.5 graphically depicts an example C2F NTCIP Stack and is one variation of what was originally published as the Class B Profile. The stack is shown as it relates to the NTCIP Framework. Combining appropriate selections from each of the Information, Application, Transport, Subnetwork and Plant Levels creates the stack. The figure shows the choices at each NTCIP Framework level that are required to create one variation of Class B, as it was originally published. For example, the SNMP protocol selection is made at the Application Level within the NTCIP stack.

Exhibit 4.4: Procurement Check-List Overview

- ❑ Consider specific communications needs by developing the functional requirements, including:
  - ❑ Communications data and timing
  - ❑ Channel loading
  - ❑ Device latency
- ❑ Analyze available resources
  - ❑ New system with no existing resources
  - ❑ Existing system with available resources
- ❑ Define an entire NTCIP Stack for intended system(s)
  - ❑ See Exhibit 4.6
- ❑ Gather appropriate standards for each level within the NTCIP Stack
  - ❑ See Exhibit 4.7
- ❑ Determine required Conformance Groups
  - ❑ Mandatory
  - ❑ Optional
  - ❑ See specific standards that relate to needed functionality
- ❑ Determine required Data Elements (objects)
  - ❑ Mandatory
  - ❑ Optional
  - ❑ See specific standards that relate to needed functionality
- ❑ Define realistic Range Values for system implementation
  - ❑ See functionality requirements
  - ❑ See specific standards that relate to needed functionality
- ❑ Determine all functional requirements that could not be matched
- ❑ Develop tailored specifications to meet intended needs not addressed by the NTCIP standards
- ❑ Define how manufacturer-specific items, if allowed, will be addressed

Note: *NTCIP has moved away from denoting the various stacks with alphanumeric characters and moved towards the designation of specific standards at each level within the NTCIP Framework. As a result, Class B should be regarded as a legacy term that will be phased out in-lieu of an array of specific NTCIP Framework level standards.*

The Class B stack that was originally published includes only the Application, Transport and Subnetwork Levels of the NTCIP Framework. The choices that are offered at the Application Level include SNMP and STMP. The only choice that is defined for the Transport Level is T2/NULL. The Subnetwork Level option includes Point-to-Multi-Point, using either commercial standards EIA/TIA-232 or for off-the-shelf FSK-1200bps modems. The Plant Level is assumed to be agency owned twisted pair wire.

In working through this example, it is easy to see that these options are quite limited. Extrapolating for all the various system configurations, one can see where publishing distinct documents for all possible system configurations could be quite exhausting. As a result, the presentation of NTCIP standards have moved away from the Class Profile presentation and toward a presentation of standards specific to each stack layer. This enables the user to better specify choices specific to the system being deployed.

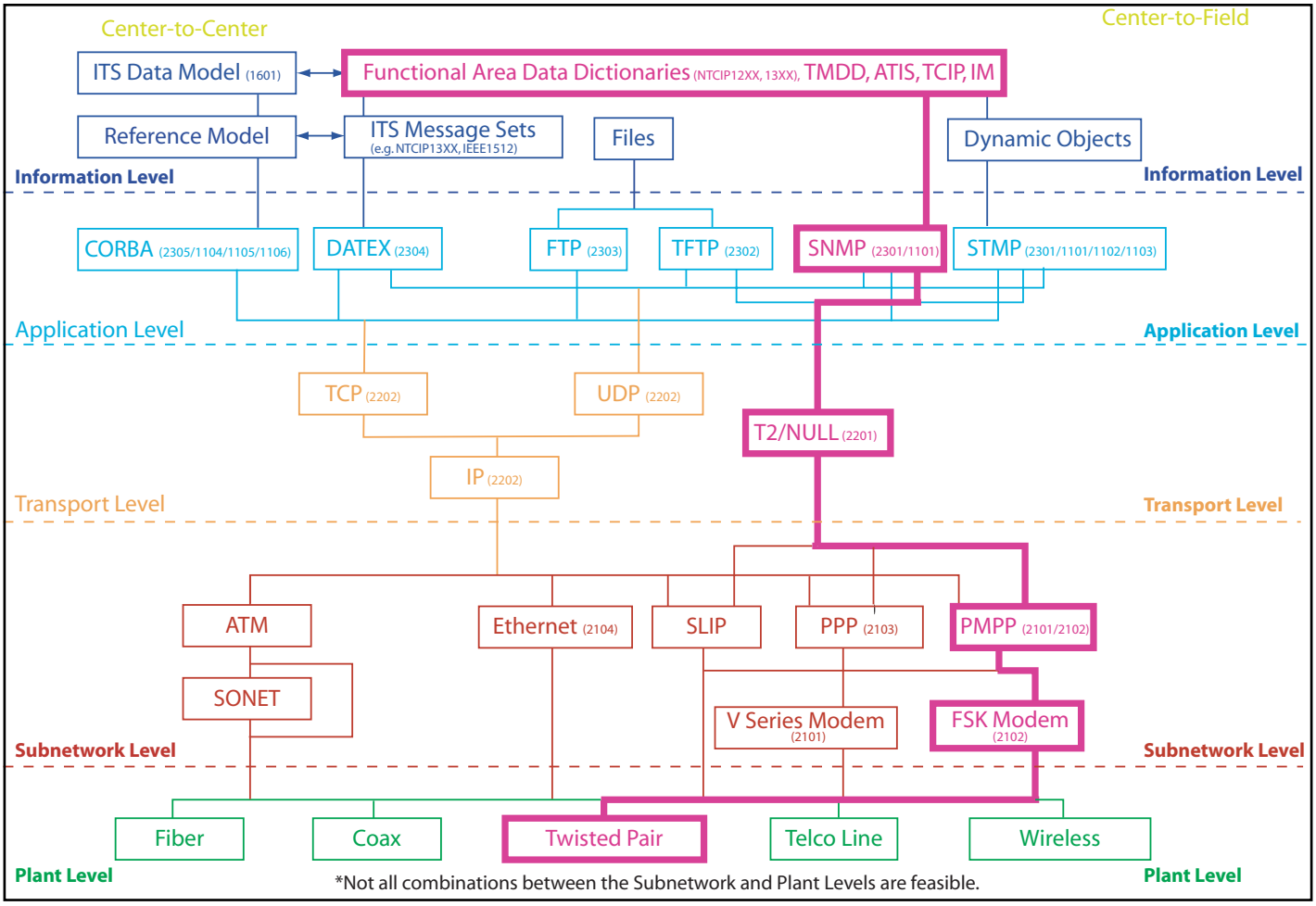


Exhibit 4.5: Example Center-to-Field Stack

4.8.1 NTCIP Stack Options

The Information, Application, Transport, Subnetwork and Plant Levels of the NTCIP Framework present a variety of options that can be selected to form an NTCIP stack. Exhibit 4.6 presents an expanded view of the available C2F options that are available at the time *The NTCIP Guide* was prepared.

The Information Level of the NTCIP Framework specifically focuses on the informational requirements of the NTCIP device or system to achieve its desired functionality. A thorough discussion of the available Information Level options will be presented later in this section.

In the case of C2F, the selection of an appropriate Application Level protocol is an important consideration. There are several choices for C2F protocols:

- Simple Network Management Protocol (SNMP) that is commonly used in Internet and computer industry applications.

Exhibit 4.6: Center-to-Field Options

- ❑ *Information Level*
  - ❑ Select applicable standards
    - ❑ NTCIP 1201 – Global Object Definitions (typically always used with a device specific standard)
    - ❑ Device specific standard(s) (see also specific conformance requirements for NTCIP 1201)
  - ❑ Specify Conformance Groups based on the PICS statement in device specific standards
    - ❑ Mandatory
    - ❑ Optional
    - ❑ Based upon device functionality
  - ❑ Specify Data Elements
    - ❑ Mandatory
    - ❑ Optional
    - ❑ Determine appropriate Range Values
- ❑ *Application Level*
  - ❑ Simple Network Management Protocol
    - ❑ Internet Standard
    - ❑ Support is Mandatory in Conformance Level 1 and 2
  - ❑ Simple Transportation Management Protocol
    - ❑ More efficient protocol
    - ❑ Defines dynamic objects (multiple data element request in single message)
    - ❑ Support is Mandatory in Conformance Level 2
- ❑ *Transport Level*
  - ❑ TCP
    - ❑ IP
  - ❑ UDP
    - ❑ IP
  - ❑ T2/Null
- ❑ *Subnetwork Level*
  - ❑ ATM
    - ❑ SONET
  - ❑ Ethernet
  - ❑ PPP
    - ❑ V Series Modem
    - ❑ FSK Modem
  - ❑ PMPP
    - ❑ EIA/TIA-232-E
    - ❑ FSK Modem
- ❑ *Plant Level*
  - ❑ Fiber
  - ❑ Coax
  - ❑ Twisted Pair
  - ❑ Telco Line

- The more efficient Simple Transportation Management Protocol (STMP) that allows the user to access multiple data elements using a single request.
- The Trivial File Transfer Protocol (TFTP) and the File Transfer Protocol (FTP) are commonly used protocols in the Internet industry.

Transport Level options are essentially comprised of a choice between the use of routable and non-routable protocols. The Transportation Transport Protocol (T2, formerly known as NULL protocol) at the Transport Level is used with non-routable protocols. In the case of routable protocols, an additional choice is required between connection-oriented and connectionless. The Transmission Control Protocol (TCP) is connection-oriented protocol that is used in conjunction with the internetworking protocol simply known as Internet Protocol (IP). The User Datagram Protocol (UDP) is a connectionless protocol that is also used in conjunction with the Internet Protocol (IP). UDP is commonly used in conjunction with the SNMP, STMP and TFTP Application Levels, while TCP is typically used in conjunction with the FTP Application Level.

The Subnetwork Level presents a series of networking, Point-to-Point and Point-to-MultiPoint protocols. ATM, SONET and Ethernet are all examples of broadband networking protocol options. PPP and PMPP are also available options at the Subnetwork Level.

The Plant Level of the NTCIP Framework does not denote specific NTCIP communications standards, but offers the user of this *NTCIP Guide* with a more complete relationship to the physical infrastructure that would typically be deployed in modern systems. The Plant Level includes fiber, coax, twisted pair wire and telco lines.

In the cases of protocol selection, it would be advisable to consult equipment and system manufacturers for assistance in the selection of the most appropriate supported protocol(s) that meet the overall requirements of the system. STMP should be considered essential for traffic signal systems operating over traditional media, but other devices may not need it.

The functionality needs of particular devices, equipment and systems are important when considering the selection of appropriate conformance statements. While the NTCIP communication standards do not specifically prescribe functionality requirements, such can be inferred by data element construction. The NTCIP communications requirements should be consistent with the functional specifications for the device. As in the case of a C2F traffic signal system, selection of appropriate standard data element sets that yield the functionality required for a specific implementation might include data elements from two NTCIP standards, Global Object Definitions and Actuated Signal Control Objects. Exhibit 4.7 lists the NTCIP standards that are published at the time this *NTCIP Guide* was produced. Lastly, specific range values associated with these data elements would also need to be consistent with the functional requirements of the device.

Upon reviewing the standards that might be applicable to a specific implementation, attention should be drawn to the Conformance Statement section of the document. Data elements are arranged in groupings based upon the data associated with various levels of functionality. Some groups are mandatory, while many are optional. Specific data elements within each conformance group, regardless of the conformance group being optional or

Exhibit 4.7: Currently Published NTCIP Standards

Information Level Standards

- ❑ NTCIP 1201 – Global Object Definitions
- ❑ NTCIP 1202 – Object Definitions for Actuated Traffic Signal Controller Units
- ❑ NTCIP 1203 – Object Definitions for Dynamic Message Signs
- ❑ NTCIP 1204 – Environmental Sensor Stations
- ❑ NTCIP 1207 – Ramp Metering Control Units*

Application Level Standards

- ❑ NTCIP 2301 – Simple Transportation Management Framework (including SNMP and STMP)*
- ❑ NTCIP 2302 – Trivial File Transfer Protocol (TFTP)*
- ❑ NTCIP 2303 – File Transfer Protocol (FTP)*
- ❑ NTCIP 2304 – DATEX-ASN*
- ❑ NTCIP 2305 – CORBA

Transport Level Standards

- ❑ NTCIP 2201 – Transportation Transport Protocol (T2, formerly known as NULL Protocol)*
- ❑ NTCIP 2202 – Internet (TCP/UDP/IP) Profile*

Subnetwork Level Standards

- ❑ NTCIP 2101 – Point-to-MultiPoint Protocol over EIA/TIA-232*
- ❑ NTCIP 2103 – Point-to-MultiPoint Protocol over FSK Modem*
- ❑ NTCIP 2103 – Point-to-Point Protocol (dial-up)*
- ❑ NTCIP 2104 – Ethernet*

Other Protocol and Profile Standards

- ❑ NTCIP 1101 – Simple Transportation Management Framework
- ❑ NTCIP 1102 – Octet Encoding Rules*
- ❑ NTCIP 2001 – Class B Profile (to be replaced by NTCIP 2101/2102, 2201, 2301)

Process, Control, and Information Management Policies

- ❑ NTCIP 8001 – Standards Development Process
- ❑ NTCIP 8002 – Standards Publication Format
- ❑ NTCIP 8003 – Framework and Classification of Profiles

Transit Related Standards

- ❑ NTCIP 1400 – Transit Communications Interface Profiles (TCIP) Framework Standard**
- ❑ NTCIP 1401 – TCIP Standard on Common Public Transportation (CPT) Objects**
- ❑ NTCIP 1402 – TCIP Standard on Incident Management (IM) Objects**
- ❑ NTCIP 1403 – TCIP Standard on Passenger Information (PI) Objects**
- ❑ NTCIP 1404 – TCIP Standard on Scheduling/Runcutting (SCH) Objects**
- ❑ NTCIP 1405 – TCIP Standard on Spatial Representation (SP) Objects**
- ❑ NTCIP 1406 – TCIP Standard on On-Board (OB) Objects**
- ❑ NTCIP 1408 – TCIP Standard on Control Center (CC) Objects**
- ❑ NTCIP 1408 – TCIP Fare Collection Business Area Standard**

* publication in progress

** for more information on TCIP standards, please refer to the TCIP Guide

Please note that the above Standard number designations refer to those publications that have been published to-date. The numbering scheme for NTCIP publications has been revised and the new designations are shown in Section 9 of this *NTCIP Guide*. Please visit the NTCIP Homepage (www.ntcip.org/) for updates.

mandatory, may also be mandatory or optional. The specific implementation and functionality requirements will dictate the selection of appropriate conformance groups and data elements. Once the Data Elements are identified, a determination of appropriate range values can be assigned to each to represent the desired level of functionality.

It is advisable to consult equipment and system manufacturers for assistance in the selection of the most appropriate supported Conformance Groups and Data Elements that meet the overall requirements of the specific procurement or implementation. Special considerations in respect to this statement must be given to subsequent purchases in a standards-based system. Those who seek to expand their systems through subsequent procurements will need to carefully consider the use of any manufacturer-specific extensions and verify whether it is possible to integrate such features into the subsequent procurement.

4.8.2 Available Resources for Additional Information

Ultimately, specifying NTCIP does not make life easier for the systems planner and specification writer. Detailed specifications must be carefully thought out and a more thorough knowledge of operation and functionality is needed early on (in the specification preparation stage) in order to adequately specify equipment and systems that meet the required needs. For these reasons, an agency might want to consider a procurement method that outlines the desired functionality as part of the procurement package and solicit a proposal from the manufacturer, provider, developer, or integrator addressing the specific implementation details.

There are a variety of resources available for the user when preparing an NTCIP specification. The NTCIP web site (www.ntcip.org/) and the ITS standards web site (www.its-standards.net/) are valuable tools for reviewing what standards are now available and any amendments that might be associated with those standards. The various sections of *The NTCIP Guide* provide additional detailed information and further explanations of how the standards fit together. In addition, the standards themselves represent a valuable resource for learning about NTCIP.

Ongoing NTCIP deployments are a valuable resource for learning what works and what doesn't. There is an ongoing effort to capture some of this information specific to deployments using NTCIP, in the form of Case Studies. These Case Studies will focus on lessons learned from recent deployments. There are a variety of case studies available that have topic areas such as traffic signal control, dynamic message signs, environmental sensor stations, and C2C.

NTCIP Specification Development Examples

This section is devoted to examples of how the system planner/specification writer would step through a process to develop detailed procurement specifications for NTCIP systems. Examples are provided for determining:

- An appropriate NTCIP Stack based upon the NTCIP Framework,
- An appropriate optional and mandatory conformance groups and data elements needed to achieve a desired functionality, and
- The range values that might be needed for a specific implementation.

NTCIP Stack for Center-to-Field Traffic Signal Controller

Example 4.1 An appropriate NTCIP Stack is needed for a typical traffic signal controller application. In this example, the controller is to be located in a field cabinet and is one device on a multi-drop communication channel. The central transportation management system constantly communicates directly to the traffic signal controller(s) over agency owned twisted-pair wire cable. The central management system is to communicate on a once-per-second basis with the traffic signal controller.

The system planner/specification writer can start by determining the appropriate selections for each level using the NTCIP Framework, as shown in Exhibit 4.8. It is a given that an agency owned twisted-pair wire communications plant will provide the physical infrastructure for C2F communications. The selection at the ***Plant Level*** should reflect the selection of *twisted-pair* wire cable.

The selections made at the ***Transport*** and ***Subnetwork Levels*** can now be made based upon the type of communications desired between the central transportation management system and the field traffic signal controller(s). In this example, a dedicated Point-to-MultiPoint communications link without routing through higher-level devices is the desired alternative. As such, the selections of *NTCIP 2102 – PMPP and FSK Modem* can be made at the Subnetwork Level. And, the selection of *NTCIP 2201 – T2/NULL* can be made at the Transport Level.

For the appropriate selections at the ***Application Level,*** the system planner/specification writer is referred to the NTCIP publications describing the Simple Transportation Management Framework (STMF). The Simple Transportation Management Framework publication describes two conformance levels. The original publication has been amended to reflect the use of the following protocols:

- ***Conformance Level 1***
  - ❖ Simple Network Management Protocol (SNMP)
- ***Conformance Level 2***
  - ❖ Simple Network Management Protocol (SNMP)
  - ❖ Simple Transportation Management Protocol (STMP)

Exhibit 4.8: NTCIP Framework Example for a Center-to-Field Traffic Signal Controller

- ☑ *Information Level*
  - ☑ Select applicable standards
    - ☑ NTCIP 1201 – Global Object Definitions (typically always used with a device specific standard)
    - ☑ Device specific standard(s) (see also specific conformance requirements for NTCIP 1201)
      - ☑ NTCIP 1202 – Object Definitions for Actuated Traffic Signal Controller Units (ASC)
  - ☑ Specify Conformance Groups based on the PICS statement in device specific standards
    - ☑ Mandatory
    - ☑ Optional
    - ☑ Based upon device functionality
  - ☑ Specify Data Elements
    - ☑ Mandatory
    - ☑ Optional
  - ☑ Determine appropriate Range Values
- ☑ *Application Level*
  - ❑ Simple Network Management Protocol
  - ☑ Simple Transportation Management Protocol
- ☑ *Transport Level*
  - ❑ TCP
    - ❑ IP
  - ❑ UDP
    - ❑ IP
  - ☑ T2/Null
- ☑ *Subnetwork Level*
  - ❑ ATM
    - ❑ SONET
  - ❑ Ethernet
  - ❑ PPP
    - ❑ V Series Modem
    - ❑ FSK Modem
  - ☑ PMPP
    - ❑ EIA/TIA-232-E
    - ☑ FSK Modem
- ☑ *Plant Level*
  - ❑ Fiber
  - ❑ Coax
  - ☑ Twisted Pair
  - ❑ Telco Line

SNMP is a commonly used Internet Standard that is very well supported. STMP is a more efficient protocol for use by the transportation industry that allows the use of dynamic objects. The preferred selection at the Application Level for traffic signal systems is *NTCIP 2301 – STMP* because of the low data rates and high frequency rates (here, once-per-second) that are common to most traffic signal systems.

The selection of ***Information Level*** standards, conformance groups and data elements is based upon the desired functionality of the system being implemented. In the case of this example where a traffic signal system is being implemented, the system planner/specification writer will need to look specifically at the requirements of primary standard *NTCIP 1202 – Object Definitions for Actuated Traffic Signal Controller Units* standard for

specific conformance criteria and data elements. Additionally, the supporting standard *NTCIP 1201 – Global Object Definitions* defines a series of cross-cutting data elements for configuration, database management, time management, time base event schedules, reports, STMP and PMPP. As a result, standards for both Global Object Definitions and Actuated Signal Control will be needed to achieve the desired level of functionality. NTCIP has initiated an effort to add Profile Implementation Conformance Statements (PICS) to newer standards as a means of providing a more user-friendly presentation of conformance. NTCIP 1202 version 2 (which is in draft form and expected to be released 2002-2003) is one of the first standards to implement the PICS statement and it defines the data elements from both NTCIP Standard 1201 and NTCIP Standard 1202 that are required to be supported for signal controllers claiming conformance to NTCIP 1202. The PICS statement, with the device-specific standards, defines a series of optional and mandatory conformance groups and data elements. The appropriate selection criteria for these optional and mandatory conformance groups and data elements will be the subject of subsequent examples.

Conformance Group and Data Element Selection for Traffic Signal Controllers

Example 4.2 An appropriate selection of conformance groups and data elements are needed for a typical traffic signal controller application. In this example, the controller will be based upon the NEMA TS-2-Type 2 Actuated Traffic Controller standards. The Type 2 NEMA controller is one that is backwardly compatible to the NEMA TS-1 Traffic Controller Cabinets with the MS A, B, and C connectors.

The NEMA TS 2 – 1998 Standard for Traffic Controller Assemblies describes a functional specification for traffic controller assemblies, including the controller unit, malfunction management unit, terminals and facilities, auxiliary devices, cabinet and bus interface unit. The NEMA TS 2-1998 also incorporates the NTCIP standards that relate to traffic signal controllers. The notable NTCIP standards that are referenced are the NTCIP 1201 – Global Object Definitions and NTCIP 1202 – Object Definitions for Actuated Traffic Signal Controller Units (previously referred to as TS 3.4 and TS 3.5 respectively).

NEMA TS 2 – 1998 describes traffic signal controllers in terms of being either Actuated or Pretimed. Also, there are two interface options cited as Type 1 and Type 2. The Type 1 interface is a new performance-based standard using serial communications and the Type 2 interface utilizes the MS A, B and C connectors to provide backwards compatibility to TS – 1-style cabinets.

Exhibits 4.9 and 4.10 show how the NTCIP group and data element conformance statements relate to the NEMA TS 2 – 1998 Standard for Traffic Controller Assemblies. The Level 1 actuated TS 2 traffic controller is intended to support only the mandatory NTCIP data elements from NTCIP 1201 – Global Object Definitions and NTCIP 1202 – Actuated Signal Control. The mandatory data elements of these two NTCIP standards do not address the advanced functions relative to coordination, time base, preemption, system control,

overlaps, or the TS 2 port 1. A user requesting Level 1 conformance should not expect these features unless the user specification includes a definition of additional conformance groups from the standard, or defines and lists specific alternates. A user specifying Level 2 conformance is requesting that all of the mandatory and most of the optional data elements within NTCIP 1201 – Global Object Definitions and NTCIP 1202 – Actuated Signal Control be supported.

Exhibit 4.9: Global Object Definitions Conformance Table

Conformance Group/Data Element	Reference	Conformance Requirement	NEMA TS 2 (A2N)	Conformance Group/Data Element
			M – Mandatory O – Optional	
			Level 1	Level 2
Configuration	NTCIP 1201	**Mandatory Group**	M	M
globalSetIDParameter	NTCIP 1201	Optional	O	M
globalMaxModules	NTCIP 1201	Mandatory	M	M
globalModuleTable	NTCIP 1201	Mandatory	M	M
moduleNumber	NTCIP 1201	Mandatory	M	M
moduleDeviceNode	NTCIP 1201	Mandatory	M	M
moduleMake	NTCIP 1201	Mandatory	M	M
moduleModel	NTCIP 1201	Mandatory	M	M
moduleVersion	NTCIP 1201	Mandatory	M	M
moduleType	NTCIP 1201	Mandatory	M	M
Database Management	NTCIP 1201	**Optional Group**	O	M
dBCreationTransaction	NTCIP 1201	Mandatory	O	M
dBErrorType	NTCIP 1201	Mandatory	O	M
dBErrorID	NTCIP 1201	Mandatory	O	M
dBTransactionID	NTCIP 1201	Mandatory	O	M
dBMakeID	NTCIP 1201	Optional	O	M
Time Management	NTCIP 1201	**Optional Group**	O	M
globalTime	NTCIP 1201	Mandatory	O	M
globalDaylightSaving	NTCIP 1201	Mandatory	O	M
Timebase Event Schedule	NTCIP 1201	**Optional Group**	O	M
maxTimeBaseScheduleEntries	NTCIP 1201	Mandatory	O	M
timeBaseScheduleTable	NTCIP 1201	Mandatory	O	M
timeBaseScheduleNumber	NTCIP 1201	Mandatory	O	M
timeBaseScheduleMonth	NTCIP 1201	Mandatory	O	M
timeBaseScheduleDay	NTCIP 1201	Mandatory	O	M
timeBaseScheduleDate	NTCIP 1201	Mandatory	O	M
timeBaseScheduleDayPlan	NTCIP 1201	Mandatory	O	M
maxDayPlans	NTCIP 1201	Mandatory	O	M
maxDayPlanEvents	NTCIP 1201	Mandatory	O	M
timeBaseDay PlanTable	NTCIP 1201	Mandatory	O	M
dayPlanNumber	NTCIP 1201	Mandatory	O	M
dayPlanEventNumber	NTCIP 1201	Mandatory	O	M
dayPlanHour	NTCIP 1201	Mandatory	O	M
dayPlanMinute	NTCIP 1201	Mandatory	O	M
dayPlanActionNumberOID	NTCIP 1201	Mandatory	O	M
dayPlanStatus	NTCIP 1201	Mandatory	O	M

Exhibit 4.9: Global Object Definitions Conformance Table (Continued)

Conformance Group/Data Element	Reference	Conformance Requirement	NEMA TS 2 (A2N)	Conformance Group/Data Element
			M – Mandatory O – Optional	
			Level 1	Level 2
Report	NTCIP 1201	**Optional Group**	O	M
maxEventLogConfigs	NTCIP 1201	Mandatory	O	M
eventLogConfigTable	NTCIP 1201	Mandatory	O	M
eventConfigID	NTCIP 1201	Mandatory	O	M
eventConfigClass	NTCIP 1201	Mandatory	O	M
eventConfigMode	NTCIP 1201	Mandatory	O	M
eventConfigCompareValue	NTCIP 1201	Mandatory	O	M
eventConfigCompareValue2	NTCIP 1201	Mandatory	O	M
eventConfigCompareOID	NTCIP 1201	Mandatory	O	M
eventConfigLogOID	NTCIP 1201	Optional	O	M
eventConfigAction	NTCIP 1201	Optional	O	M
maxEventLogSize	NTCIP 1201	Mandatory	O	M
eventLogTable	NTCIP 1201	Mandatory	O	M
eventLogClass	NTCIP 1201	Mandatory	O	M
eventLogNumber	NTCIP 1201	Mandatory	O	M
eventLogID	NTCIP 1201	Mandatory	O	M
eventLogTime	NTCIP 1201	Mandatory	O	M
eventLogValue	NTCIP 1201	Mandatory	O	M
maxEventClasses	NTCIP 1201	Mandatory	O	M
eventClassTable	NTCIP 1201	Mandatory	O	M
eventClassNumber	NTCIP 1201	Mandatory	O	M
eventClassLimit	NTCIP 1201	Mandatory	O	M
eventClassClearTime	NTCIP 1201	Mandatory	O	M
EventClassDescription	NTCIP 1201	Optional	O	M
eventClassNumRowsInLog	NTCIP 1201	Mandatory	O	M
STMP	NTCIP 1201	**Optional Group**	O	M
dynamicObjectPersistence	NTCIP 1201	Mandatory	O	M
PMPP	NTCIP 1201	**Optional Group**	O	M
maxGroupAddresses	NTCIP 1201	Mandatory	O	M
hdlcGroupAddressTable	NTCIP 1201	Mandatory	O	M
hdlcGroupAddressIndex	NTCIP 1201	Mandatory	O	M
hdlcGroupAddress	NTCIP 1201	Mandatory	O	M

Exhibit 4.10: Actuated Traffic Signal Controller Unit Data Element Definitions Conformance Table

Conformance Group/Data Element	Reference	Conformance Requirement	NEMA TS 2 (A2N)	Conformance Group/Data Element
			M – Mandatory O – Optional	
			Level 1	Level 2
Configuration	**NTCIP 1201**	**Mandatory Group**	**M**	**M**
Database Management	**NTCIP 1201**	**Optional Group**	**O**	**M**
Time Management	**NTCIP 1201**	**Optional Group**	**O**	**M**
Timebase Event Schedule	**NTCIP 1201**	**Optional Group**	**O**	**M**
Report	**NTCIP 1201**	**Optional Group**	**O**	**M**
STMP	**NTCIP 1201**	**Optional Group**	**O**	**M**
PMPP	**NTCIP 1201**	**Optional Group**	**O**	**M**
Phase	NTCIP 1202	**Mandatory Group**	M	M
maxPhases	NTCIP 1202	Mandatory	M	M
phaseTable	NTCIP 1202	Mandatory	M	M
phaseNumber	NTCIP 1202	Mandatory	M	M
phaseWalk	NTCIP 1202	Mandatory	M	M
phasePedestrianClear	NTCIP 1202	Mandatory	M	M
phaseMinimumGreen	NTCIP 1202	Mandatory	M	M
phasePassage	NTCIP 1202	Mandatory	M	M
phaseMaximum1	NTCIP 1202	Mandatory	M	M
phaseMaximum2	NTCIP 1202	Mandatory	M	M
phaseYellowChage	NTCIP 1202	Mandatory	M	M
phaseRedClear	NTCIP 1202	Mandatory	M	M
phaseRedRevert	NTCIP 1202	Optional	O	O
phaseAddedInitial	NTCIP 1202	Mandatory	M	M
phaseMaximumInitial	NTCIP 1202	Mandatory	M	M
phaseTimeBeforeReduction	NTCIP 1202	Mandatory	M	M
phaseCarsBeforeReduction	NTCIP 1202	Optional	O	O
phaseTimeToReduce	NTCIP 1202	Mandatory	M	M
phaseReduceBy	NTCIP 1202	Mandatory	M	O
phaseMinimumGap	NTCIP 1202	Mandatory	M	M
phaseDynamicMaxLimit	NTCIP 1202	Optional	O	O
phaseDynamicMaxStep	NTCIP 1202	Optional	O	O
phaseStartup	NTCIP 1202	Mandatory	M	M
phaseOptions	NTCIP 1202	Mandatory	M	M
phaseRing	NTCIP 1202	Mandatory	M	M
phaseConcurrency	NTCIP 1202	Mandatory	M	M
maxPhaseGroups	NTCIP 1202	Mandatory	M	M
phaseStatusGroupTable	NTCIP 1202	Mandatory	M	M
phaseStatusGroupNumber	NTCIP 1202	Mandatory	M	M

Exhibit 4.10: Actuated Traffic Signal Controller Unit Data Element Definitions Conformance Table

Conformance Group/Data Element	Reference	Conformance Requirement	NEMA TS 2 (A2N)	Conformance Group/Data Element
			M – Mandatory O – Optional	
			Level 1	Level 2
phaseStatusGroupReds	NTCIP 1202	Mandatory	M	M
phaseStatusGroupYellows	NTCIP 1202	Mandatory	M	M
phaseStatusGroupGreens	NTCIP 1202	Mandatory	M	M
phaseStatusGroupDontWalks	NTCIP 1202	Mandatory	M	M
phaseStatusGroupPedClears	NTCIP 1202	Mandatory	M	M
phaseStatusGroupWalks	NTCIP 1202	Mandatory	M	M
phaseStatusGroupVehCalls	NTCIP 1202	Mandatory	M	M
phaseStatusGroupPedCalls	NTCIP 1202	Mandatory	M	M
phaseStatusGroupPhaseOns	NTCIP 1202	Mandatory	M	M
phaseStatusGroupPhaseNexts	NTCIP 1202	Mandatory	M	M
phaseControlGroupTable	NTCIP 1202	Optional	O	M
phaseControlGroupNumber	NTCIP 1202	Mandatory	O	M
phaseControlGroupPhaseOmit	NTCIP 1202	Mandatory	O	M
phaseControlGroupPedOmit	NTCIP 1202	Mandatory	O	M
phaseControlGroupHold	NTCIP 1202	Mandatory	O	M
phaseControlGroupForceOff	NTCIP 1202	Optional	O	O
phaseControlGroupVehCall	NTCIP 1202	Mandatory	O	M
phaseControlGroupPedCal	NTCIP 1202	Mandatory	O	M

Exhibit 4.10: Actuated Traffic Signal Controller Unit Data Element Definitions Conformance Table

Conformance Group/Data Element	Reference	Conformance Requirement	NEMA TS 2 (A2N)	Conformance Group/Data Element
			M – Mandatory O – Optional	
			Level 1	Level 2
Detector	NTCIP 1202	**Mandatory Group**	M	M
maxVehicleDetectors	NTCIP 1202	Mandatory	M	M
vehicleDetectorTable	NTCIP 1202	Mandatory	M	M
vehicleDetectorNumber	NTCIP 1202	Mandatory	M	M
vehicleDetectorOptions	NTCIP 1202	Mandatory	M	M
vehicleDetectorCallPhase	NTCIP 1202	Mandatory	M	M
vehicleDetectorSwitchPhase	NTCIP 1202	Mandatory	M	M
vehicleDetectorDelay	NTCIP 1202	Mandatory	M	M
vehicleDetectorExtend	NTCIP 1202	Mandatory	M	M
vehicleDetectorQueueLimit	NTCIP 1202	Optional	O	M
vehicleDetectorNoActivity	NTCIP 1202	Mandatory	M	M
vehicleDetectorMaxPresence	NTCIP 1202	Mandatory	M	M
vehicleDetectorErraticCounts	NTCIP 1202	Mandatory	M	M
vehicleDetectorFailTime	NTCIP 1202	Optional	O	M
vehicleDetectorAlarms	NTCIP 1202	Mandatory	M	M
vehicleDetectorReportedAlarms	NTCIP 1202	Optional	O	M
vehicleDetectorReset	NTCIP 1202	Mandatory	M	M
maxVehicleDetectorStatusGroups	NTCIP 1202	Mandatory	M	M
vehicleDetectorStatusGroupTable	NTCIP 1202	Mandatory	M	M
vehicleDetectorStatusGroupNumber	NTCIP 1202	Mandatory	M	M
vehicleDetectorStatusGroupActive	NTCIP 1202	Mandatory	M	M
vehicleDetectorStatusGroupAlarms	NTCIP 1202	Mandatory	M	M
maxPedestrianDetectors	NTCIP 1202	Mandatory	M	M
pedestrianDetectorTable	NTCIP 1202	Mandatory	M	M
pedestrianDetectorNumber	NTCIP 1202	Mandatory	M	M
pedestrianDetectorCallPhase	NTCIP 1202	Mandatory	M	M
pedestrianDetectorNoActivity	NTCIP 1202	Mandatory	M	M
pedestrianDetectorMaxPresence	NTCIP 1202	Mandatory	M	M
pedestrianDetectorErraticCounts	NTCIP 1202	Mandatory	M	M
pedestrianDetectorAlarms	NTCIP 1202	Mandatory	M	M
Volume Occupancy Report	NTCIP 1202	**Optional Group**	O	M
volumeOccupancySequence	NTCIP 1202	Mandatory	O	M
volumeOccupancyPeriod	NTCIP 1202	Mandatory	O	M
activeVolumeOccupancyDetectors	NTCIP 1202	Mandatory	O	M
volumeOccupancyTable	NTCIP 1202	Mandatory	O	M
detectorVolume	NTCIP 1202	Mandatory	O	M
detectorOccupancy	NTCIP 1202	Mandatory	O	M

Exhibit 4.10: Actuated Traffic Signal Controller Unit Data Element Definitions Conformance Table

Conformance Group/Data Element	Reference	Conformance Requirement	NEMA TS 2 (A2N)	Conformance Group/Data Element
			M – Mandatory O – Optional	
			Level 1	Level 2
Unit	NTCIP 1202	**Optional Group**	O	M
unitStartUpFlash	NTCIP 1202	Mandatory	O	M
unitAutoPedestrianClear	NTCIP 1202	Mandatory	O	M
unitBackupTime	NTCIP 1202	Mandatory	O	M
unitRedRevert	NTCIP 1202	Mandatory	O	M
unitControlStatus	NTCIP 1202	Mandatory	O	M
unitFlashStatus	NTCIP 1202	Mandatory	O	M
unitAlarmStatus2	NTCIP 1202	Mandatory	O	M
unitAlarmStatus1	NTCIP 1202	Mandatory	O	M
shortAlarmStatus	NTCIP 1202	Mandatory	O	M
unitControl	NTCIP 1202	Mandatory	O	M
maxAlarmGroups	NTCIP 1202	Optional	O	M
alarmGroupTable	NTCIP 1202	Mandatory	O	M
alarmGroupNumber	NTCIP 1202	Mandatory	O	M
alarmGroupState	NTCIP 1202	Mandatory	O	M
Special Function	NTCIP 1202	**Optional Group**	O	M
maxSpecialFunctionOutputs	NTCIP 1202	Mandatory	O	M
specialFunctionOutputTable	NTCIP 1202	Optional	O	M
specialFunctionOutputNumber	NTCIP 1202	Mandatory	O	M
specialFunctionOutputState	NTCIP 1202	Mandatory	O	M
Coordination	NTCIP 1202	**Optional Group**	O	M
coordOperationalMode	NTCIP 1202	Mandatory	O	M
coordCorrectionMode	NTCIP 1202	Mandatory	O	M
coordMaximumMode	NTCIP 1202	Mandatory	O	M
coordForceMode	NTCIP 1202	Mandatory	O	M
maxPatterns	NTCIP 1202	Mandatory	O	M
patternTableType	NTCIP 1202	Mandatory	O	M
patternTable	NTCIP 1202	Mandatory	O	M
patternNumber	NTCIP 1202	Mandatory	O	M
patternCycleTime	NTCIP 1202	Mandatory	O	M
patternOffsetTime	NTCIP 1202	Mandatory	O	M
patternSplitNumber	NTCIP 1202	Mandatory	O	M
patternSequenceNumber	NTCIP 1202	Mandatory	O	M
maxSplits	NTCIP 1202	Mandatory	O	M
splitTable	NTCIP 1202	Mandatory	O	M
splitNumber	NTCIP 1202	Mandatory	O	M
splitPhase	NTCIP 1202	Mandatory	O	M
splitTime	NTCIP 1202	Mandatory	O	M
splitMode	NTCIP 1202	Mandatory	O	M
splitCoordPhase	NTCIP 1202	Mandatory	O	M
coordPatternStatus	NTCIP 1202	Mandatory	O	M
localFreeStatus	NTCIP 1202	Mandatory	O	M
coordCycleStatus	NTCIP 1202	Mandatory	O	M
coordSyncStatus	NTCIP 1202	Mandatory	O	M
systemPatternControl	NTCIP 1202	Mandatory	O	M
systemSyncControl	NTCIP 1202	Mandatory	O	M

Exhibit 4.10: Actuated Traffic Signal Controller Unit Data Element Definitions Conformance Table

Conformance Group/Data Element	Reference	Conformance Requirement	NEMA TS 2 (A2N)	Conformance Group/Data Element
			M – Mandatory O – Optional	
			Level 1	Level 2
Time Base	NTCIP 1202	**Optional Group**	O	M
Time Management Conformance Group	NTCIP 1202	Mandatory	O	M
timebasePatternSync	NTCIP 1202	Mandatory	O	M
maxTimebaseAscActions	NTCIP 1202	Mandatory	O	M
timebaseAscActionTable	NTCIP 1202	Mandatory	O	M
timebaseAscActionNumber	NTCIP 1202	Mandatory	O	M
timebaseAscActionPattern	NTCIP 1202	Mandatory	O	M
timebaseAscActionAuxillaryFunction	NTCIP 1202	Mandatory	O	M
timebaseAscActionSpecialFunction	NTCIP 1202	Mandatory	O	M
timebaseAscActionStatus	NTCIP 1202	Mandatory	O	M
Preempt	NTCIP 1202	**Optional Group**	O	M
maxpreempts	NTCIP 1202	Mandatory	O	M
preemptTable	NTCIP 1202	Mandatory	O	M
preemptNumber	NTCIP 1202	Mandatory	O	M
preemptControl	NTCIP 1202	Mandatory	O	M
preemptLink	NTCIP 1202	Mandatory	O	M
preemptDelay	NTCIP 1202	Mandatory	O	M
preemptMinimumDuration	NTCIP 1202	Mandatory	O	M
preemptMinimumGreen	NTCIP 1202	Optional	O	M
preemptMinimumWalk	NTCIP 1202	Optional	O	M
preemptEnterPedClear	NTCIP 1202	Optional	O	M
preemptTrackGreen	NTCIP 1202	Mandatory	O	M
preemptDwellGreen	NTCIP 1202	Mandatory	O	M
preemptMaximumPresence	NTCIP 1202	Mandatory	O	M
preemptTrackPhase	NTCIP 1202	Mandatory	O	M
preemptDwellPhase	NTCIP 1202	Mandatory	O	M
preemptDwellPed	NTCIP 1202	Optional	O	O
preemptExitPhase	NTCIP 1202	Mandatory	O	M
preemptState	NTCIP 1202	Optional	O	M
preemptControlTable	NTCIP 1202	Optional	O	M
preemptControlNumber	NTCIP 1202	Mandatory	O	M
preemptControlState	NTCIP 1202	Mandatory	O	M

Exhibit 4.10: Actuated Traffic Signal Controller Unit Data Element Definitions Conformance Table

Conformance Group/Data Element	Reference	Conformance Requirement	NEMA TS 2 (A2N)	Conformance Group/Data Element
			M – Mandatory O – Optional	
			Level 1	Level 2
Ring	NTCIP 1202	**Optional Group**	O	M
maxRings	NTCIP 1202	Mandatory	O	M
maxSequences	NTCIP 1202	Mandatory	O	M
sequenceTable	NTCIP 1202	Mandatory	O	M
sequenceNumber	NTCIP 1202	Mandatory	O	M
sequenceRingNumber	NTCIP 1202	Mandatory	O	M
sequenceData	NTCIP 1202	Mandatory	O	M
maxRingControlGroups	NTCIP 1202	Mandatory	O	M
ringControlGroupTable	NTCIP 1202	Mandatory	O	M
ringControlGroupNumber	NTCIP 1202	Mandatory	O	M
ringControlGroupStopTime	NTCIP 1202	Mandatory	O	M
ringControlGroupForceOff	NTCIP 1202	Mandatory	O	M
ringControlGroupMax2	NTCIP 1202	Optional	O	M
ringControlGroupMaxInhibit	NTCIP 1202	Optional	O	M
ringControlGroupPedRecycle	NTCIP 1202	Mandatory	O	M
ringControlGroupRedRest	NTCIP 1202	Optional	O	M
ringControlGroupOmitRedClear	NTCIP 1202	Optional	O	M
Channel	NTCIP 1202	**Optional Group**	O	M
maxChannels	NTCIP 1202	Mandatory	O	M
channelTable	NTCIP 1202	Mandatory	O	M
channelNumber	NTCIP 1202	Mandatory	O	M
channelControlSource	NTCIP 1202	Mandatory	O	M
channelControlType	NTCIP 1202	Mandatory	O	M
channelFlash	NTCIP 1202	Mandatory	O	M
channelDim	NTCIP 1202	Mandatory	O	M
maxChannelStatusGroups	NTCIP 1202	Mandatory	O	M
channelStatusGroupTable	NTCIP 1202	Mandatory	O	M
channelStatusGroupNumber	NTCIP 1202	Mandatory	O	M
channelStatusGroupReds	NTCIP 1202	Mandatory	O	M
channelStatusGroupYellows	NTCIP 1202	Mandatory	O	M
channelStatusGroupGreens	NTCIP 1202	Mandatory	O	M

Exhibit 4.10: Actuated Traffic Signal Controller Unit Data Element Definitions Conformance Table

Conformance Group/Data Element	Reference	Conformance Requirement	NEMA TS 2 (A2N)	Conformance Group/Data Element
			M – Mandatory O – Optional	
			Level 1	Level 2
Overlap	NTCIP 1202	**Optional Group**	0	M
maxOverlaps	NTCIP 1202	Mandatory	0	M
overlapTable	NTCIP 1202	Mandatory	0	M
OverlapNumber	NTCIP 1202	Mandatory	0	M
OverlapType	NTCIP 1202	Mandatory	0	M
overlapIncludedPhases	NTCIP 1202	Mandatory	0	M
overlapModifierPhases	NTCIP 1202	Mandatory	0	M
overlapTrailGreen	NTCIP 1202	Mandatory	0	M
overlapTrailYellow	NTCIP 1202	Mandatory	0	M
overlapTrailRed	NTCIP 1202	Mandatory	0	M
maxOverlapStatusGroups	NTCIP 1202	Mandatory	0	M
overlapStatusGroupTable	NTCIP 1202	Mandatory	0	M
overlapStatusGroupNumber	NTCIP 1202	Mandatory	0	M
overlapStatusGroupReds	NTCIP 1202	Mandatory	0	M
overlapStatusGroupYellows	NTCIP 1202	Mandatory	0	M
overlapStatusGroupGreens	NTCIP 1202	Mandatory	0	M
TS 2 Port 1	NTCIP 1202	**Optional Group**	0	M
maxPort1Addresses	NTCIP 1202	Mandatory	0	M
port1Table	NTCIP 1202	Mandatory	0	M
port1Number	NTCIP 1202	Mandatory	0	M
port1DevicePresent	NTCIP 1202	Mandatory	0	M
port1Frame40Enable	NTCIP 1202	Mandatory	0	M
port1Status	NTCIP 1202	Mandatory	0	M
port1FaultFrame	NTCIP 1202	Mandatory	0	M

Data Element Range Values for an Actuated Traffic Signal Controller

Example 4.3 An appropriate selection of range values are needed for a typical traffic signal controller application. In this example, the controller will be an 8-Phase controller based upon the NEMA TS-2-Type 2 Actuated Traffic Controller standards.

As in Example 4.2, reference is made to the *NEMA TS 2 – 1998 Standard for Traffic Controller Assemblies*. The NEMA TS 2 – 1998 standard provides a listing of minimum NTCIP data element range values to be supported by the conformant traffic signal controller.

Exhibit 4.11 shows a typical data element from the *NTCIP 1202 – Object Definitions for Actuated Traffic Signal Controller Units* standard. The data element shown is the Maximum Number of Phases from the mandatory Phase Parameters conformance group. The Maximum Phases data element has a

status of mandatory. The range value of this data element is denoted as integer values from 0 to 255. This means that the device may support any value within that range. Additionally, the data element indicates that this is a read-only data element, where writing a new value is prohibited. Also, included in the data element is a description of what this data element means.

Exhibit 4.11: Sample Actuated Traffic Signal Controller Data Element

NTCIP 1202 – Phase Parameters Conformance Group – Maximum Phase

```
maxPhases OBJECT-TYPE
SYNTAX INTEGER (0…255)
ACCESS read-only
STATUS mandatory
DESCRIPTION
"The Maximum Number of Phases this Actuated Controller
   Unit supports. This object indicates the maximum
   rows which shall appear in the phaseTable object."
::={phase1}
```

The Exhibit 4.11 example also provides an opportunity to mention the concurrent discussion of developing test cases for the NTCIP standards, and how conformance of the implementation on this single dimension would be determined. For example, in this case the "test case(s)" would need to address and exhaustively determine if the data element *maxPhases*: (1) can be set to all values 0 through 255 without error, (2) returns a specific set value correctly each time, and (3) returns an error if set to a value less than "0" or greater than "255." If a project deployment specified a value of "32" as the desired upper limit, then those same informative test cases could be reused for acceptance testing, except they would be limited to examination of values 0 to 32, and check for errors on values less than "0," and greater than "32."

With the same example (Exhibit 4.11), additional complexity is added when performing a "conformity assessment" that included this data element because it determines the device upper limit for signal phases. This limit is used by several other related objects to deliver the features that enable the more complete observable functionality of the device. In short, any other feature of the standard that works with *maxPhases* must itself be thoroughly tested on the range 0 to *maxPhases* to ensure that this upper limit constraint is properly observed in all cases.

Exhibit 4.12 shows all of the minimum ranges values that are defined as part of the NEMA TS 2 – 1998 Traffic Controller Assembly Standard. The range values shown are based upon the minimum functionality requirements of the NEMA standard. In the case of the Maximum Phases value, we can see that the minimum range value to be supported is 8. The NEMA standard requires a minimum of 8 phases to meet the functionality requirements of the NEMA TS 2 – 1998 standard. Unless requirements for more phases are identified, the

minimum number of phases would equal the maximum number of phases and the value to be communicated using NTCIP for the Maximum Number of Phases would be 8. Similarly, other range values can be related to the level of functionality that is either required by specification or provided by the manufacturer.

Exhibit 4.12: Data Element Range Values for Actuated Traffic Signal Controller Units

Data Element	Minimum Project Requirements
TS 3.4 – 1996 Global Object Definitions	
moduleType	Value 3
dBCreateTransaction dBErrorType	All Values All Values
globalDaylightSaving	Values 2 and 3
maxTimeBaseScheduleEntries maxDayPlans maxDayEvents	16 15 10
maxEventLogCongifs mventConfigMode mventConfigAction maxEventLogSize MaxEventClasses	50 Values 2 thru 5 Values 2 and 3 255 7
maxGroupAddress	2
TS 3.5 – 1996 Actuated Traffic Signal Controller Units	
maxPhases pPhaseStartup phaseOptions maxPhaseGroups	8 Values 2 thru 6 All Values 1
maxVehicleDetectors vehicleDetectorOptions maxPedestrianDetectors	64 All Values 8
unitAutoPedestrianClear unitControlStatus unitFlashStatus unitControl maxAlarmGroups	All Values All Values All Values All Values 1
maxSpecialFunctionOutputs	8
coordCorrectionMode coordMaximumMode coordForceMode maxPatterns patternTableType maxSplits splitMode localFreeStatus	Values 2 thru 4 Values 2 thru 4 Values 2 and 3 48 Either 2, 3, or 4 16 Values2 thru7 Values 2 thru 11
maxTimebaseAscActions	48

Exhibit 4.12: Data Element Range Values for Actuated Traffic Signal Controller Units

Data Element	Minimum Project Requirements
maxPreempts preemptControl preemptState	6 All Values Values 2 thru 9
maxRings maxSequences	2 16
maxChannels channelControlType channelFlash channelDim maxChannelStatusGroups	16 Values 2 thru 4 Values, 0, 2, 4, 6, 8, 10, 12 and 14 Values 0 thru 15 2
maxOverlaps overlapType maxOverlapStatusGroups	4 Values 2 and 3 1
maxPort1Addresses port1Status	18 Values 2 and 3

4.9 Center-to-Center

The ITS industry is currently deploying three different ***Application Level*** solutions for inter-system communications. Two of these solutions have been defined by the NTCIP: **DAT**a **EX**change in **ASN**.1 (DATEX-ASN, commonly referred to as simply DATEX) and **C**ommon **O**bject **R**equest **B**roker **A**rchitecture (CORBA). Another potential C2C protocol, e**X**tensible **M**arkup **L**anguage (XML), is not a complete solution, rather it is only a data-structuring format and it does not define the rules for exchanging the data structures. However, ongoing work within the Internet community will likely produce a standardized way to exchange this data in the near future. In the meantime, projects have been deploying a variety of simplistic approaches to exchange this data as a stopgap measure.

All three approaches provide the same basic functionality, but they differ in the method of implementation and each has some unique features (refer to "3.12 Center-to-Center Protocols"). A particular system may support one, two, or all three of these protocols. Gateways or translators can be developed to pass messages between them when necessary. The Internet Protocol (IP) and both UDP and TCP are used at the transport level for all three solutions.

Regardless of the application level protocol, C2C communications requires participating systems to exchange standard messages at the information level. The content of these messages are derived from following a systems engineering process to identify the system requirements for data exchange. An example of a systems engineering process model is shown in Exhibit 4.5. Much of the effort to define these data exchanges can be performed independently from a protocol selection. This results in a generic definition of the messages

used by all protocols. This generic definition ensures that different implementations all share a common logical process of data exchange. Even if different implementations use different protocols, it should be possible to produce protocol translators to allow the two implementations to interoperate.

There are still a variety of protocol-specific details that must be standardized if interoperability is to be achieved when implementing these data exchanges over any specific protocol. In addition to the generic definition, there must be a protocol-specific definition for each recognized protocol.

The various C2C message sets that have been developed to date are essentially generic definitions of the messages. These include:

- Traffic Management Center External Messages;
- Transit Communications Interface Profiles;
- Incident Management Messages; and
- Traveler Information Messages;

There are no existing standards defining the details of how to implement a given message over a given protocol. All existing deployments of these standards have made interpretations as to how best to implement over a given protocol, and through these deployments the transportation industry has gained valuable experience into how we can improve our existing generic standards, as well as how to best approach the topic of protocol-specific standards. The standards community is now leveraging this experience to produce updates of the generic message sets and develop the first versions of the protocol-specific message sets.

The choice of protocol and message sets/object model depends on the application and environment. The following factors are relevant:

Note: *C2C communications take place between computer systems, and those computers or systems may be within the same "center" or in separate centers.*

The following questions really apply to each *system*, including multiple systems within one center where relevant.

- Is the procurement for just one center, or multiple centers?
- Is there an immediate need for C2C communications, or is the procurement for future use?
- Do other centers with which this one is likely to interact already have a DATEX, CORBA, or XML interface?
- What types of information will this center likely need to send or receive traffic signal, freeway, other traffic management, transit, emergency, traveler information?

- Is the procurement part of a new or upgraded system implementation, or an add-on to an existing system?
- Does the center use object-oriented software?
- Can one or more connected centers now or in the near future provide gateway/ translation services?

If multiple centers are to have C2C support added as part of the procurement, or in the near future, then these questions need to be considered for each such center. It is desirable for agencies within a region to jointly consider these issues and make coordinated procurements where feasible to minimize costs and facilitate rapid achievement of all needed C2C links in the region.

The NTCIP C2C protocols and both related generic and protocol-specific message definitions are necessary, but not sufficient for two centers to usefully exchange data. Application software is needed to gather, process, display, interpret, act on and generate the incoming or outgoing data. The same is true of any protocol. For example, the Internet's *Simple Mail Transfer Protocol* is a standard for e-mail transfer between computers, but a computer needs more than the protocol, it also needs an e-mail program that enables a user to compose and send mail, retrieve and read mail, and to archive both sent and received messages.

C2C communications between computer systems will work only if the computers have suitable application software. This software does not have to be standardized, just as Microsoft's Outlook e-mail program works quite differently from Netscape's Communicator program, but e-mail can be sent between the two because they both use the Simple Mail Transfer Protocol.

Some of the functions that a center may need in a C2C communications management software package include the following:

- User interface, for example, subscription form, data display, status reports;
- Interpretation and appropriate disposition of incoming messages;
- Databases for storing subscriptions and other administrative data;
- Interfaces with existing transportation databases and programs;
- Network performance monitoring and management; and
- Event logging and reporting.

None of these functions are specified or provided by the C2C protocols or message sets, since they do not have to be standardized. Some will at least need to be provided for a system to manage and make use of C2C communications. A system may have a very elaborate and sophisticated C2C communications management package, or a basic one. The former will provide more functions and be easier to use, but will cost more.

C2C protocol software and C2C communications management software are most easily provided as part of the initial development/implementation of a system, or during a system upgrade. However, it is possible to add on C2C software at any time.

Adding C2C software to an existing system can be achieved in either of two basic ways:

1. Keep the C2C protocol and management software separate from the existing transportation management software – usually on a separate computer and with a separate user interface. This involves a *loosely coupled* connection between the two software packages, which may make use of an existing data interface available in the transportation management system, avoiding or minimizing the need for changes to the existing software.
2. *Tightly couple* the C2C protocol and management software with the existing transportation management software – usually on the same computer, and usually with an integrated user interface. This involves alteration of the existing software to provide the integration. This option provides a more integrated application for ease of use and added functionality, but costs more.

The loosely coupled option allows use of a generic C2C "server" software package that can be replicated at multiple centers, with different interfaces to each local system. This may minimize costs, but it will likely mean users have to deal with two separate user interfaces. Incoming data may not be viewable on the same dynamic displays as local data, data from other centers may not be able to be easily combined with local data in analysis and reports, and some remote control functions may not be supported. The tightly coupled approach and its functional benefits can often be obtained much more economically if it is provided as part of a new system development or upgrade and is part of the overall system requirements and specifications.

"…NHI offers an excellent course on ITS software acquisition…"

For C2C communications to operate, a computer network connection is needed between the centers. Any local or wide area network that supports the Internet Protocol is adequate. The Internet can be used, but many centers are reluctant to do this until better security measures are available. Latency is also an issue when considering use of the Internet. Private wide area network services are readily available from telecommunications companies, including virtual private networks that use the Internet infrastructure. As explained in Chapter 5, there are bandwidth considerations if low speed WAN links, for example 56 kbps, are being considered. Dial-up access may be appropriate for remote or occasional data exchanges. Other than these introductory comments, the design and specification of the network connection is beyond the scope of the *NTCIP Guide*.

In summary, C2C procurements are essentially software acquisitions. The National Highway Institute (NHI) offers an excellent course on ITS software acquisition entitled *The Road to Successful ITS Software Acquisition*. Please consult the NHI course for additional information on procuring software.

Software Acquisition

When agencies move to implement central systems or upgrade their systems for C2C communications, the bulk of this work will involve the acquisition of software. In the case of C2C communications, software is developed to provide a means of communicating between two central system components. The National Highway Institute (NHI) has developed an ITS software acquisition course based upon *The Road to Successful ITS Software Acquisition* that lays out a successful approach to acquiring software.

The ITS software acquisition course presents a variety of themes that are useful in any project, but are especially important in a software acquisition project. The main themes presented in the NHI course include:

- System Themes – relating directly to the final product
  - ❖ Break the project up into "bite-size" pieces
  - ❖ Consider commercial-off-the-shelf (COTS) software whenever possible
- Management Themes – managing the acquisition
  - ❖ Up-front planning is essential
  - ❖ Maintain flexibility throughout the process
  - ❖ There are no "sliver bullets" or magical cures for troubled software projects
- People Themes – partnering and team building
  - ❖ Maintain active customer involvement
  - ❖ Maintain good collaboration
  - ❖ Open communications is essential
  - ❖ Team building is important

The NHI – ITS software acquisition course also presents the concept of a *requirements walkthrough* as a means of describing essential elements of the acquisition that must be well documented at the onset of the project.

Requirements

It is important that everyone involved in the software acquisition have an understanding of what capabilities the system must have. These capabilities should be described at a functional level and not used to prescribe a solution. Required functions should use "shall" in the sentence, and above all, the requirement should be testable. Functions should be defined in a manner reflective of the nature of the operation, such as being manual, automated, or semi-automated. Appropriate algorithms and equations should be mentioned. While we survived Y2K, it may be appropriate to make sure that legacy systems are upgraded as appropriate.

The documented requirements should address performance, inputs and outputs for the system being delivered. *The Road to Successful ITS Software Acquisition* presents the following list as some specific items that may also need to be addressed in the requirements document.

- Performance Requirements
  - ❖ Response time definitions (such as averages, standard deviations, 90 percentile, etc.)
  - ❖ Loading requirements (such as simultaneous inputs from X sensors)
  - ❖ Throughput (such as number of transactions per hour)
  - ❖ Capacity (such as storage for *X* days of reports)
  - ❖ False alarm rates
  - ❖ Accuracy
  - ❖ Reliability
  - ❖ Security
  - ❖ Safety
  - ❖ Interfaces, both external and internal
  - ❖ To/From field devices
  - ❖ To/From displays
  - ❖ To/From users
  - ❖ To/From other systems, including legacy systems
  - ❖ To/From other jurisdictions
  - ❖ Between major subsystem components
  - ❖ Between software components
- Inputs
  - ❖ Identify its source (automated or human)
  - ❖ Arrival frequency
  - ❖ Valid ranges and units of measure
  - ❖ Each one should have a unique name and identifier
- Outputs
  - ❖ Include both real-time outputs (alerts to display) and non-real-time outputs (printable summary report)
  - ❖ Identify its destination (devices or users)

- ❖ Generation frequency
- ❖ Valid ranges and units of measure
- ❖ Each one should have a unique name and identifier

In specifying NTCIP C2C standards it is important to consider the need for a modular and incremental approach. C2C is essentially a large software development effort and oftentimes can be of significant magnitude. These large software projects are best handled in small "bite-sized" pieces. Certainly, working towards an ultimate goal is best.

Important factors affecting ITS standards-based implementations include:

- ***Property Rights and Permissions*** – Who owns the software being implemented? What rights do I have as a user? It is important to understand the difference between ownership and right to use. Right to use licensing implies restricted rights of use and distribution, while ownership may only be minimal or non-existent. There are important cost implications to consider when evaluating which approach is right for your agency. It is important to remember that resolving intellectual property rights must be done prior to contract signing.
- ***Delivery*** – What is my timeline for system delivery? Does the schedule adequately reflect time needed for software development (hurried software development can lead to implementation problems)? What is my method of contacting and delivery (such as software delivery is often best handled through professional services contacts)?
- ***Acceptance Testing*** – How will I test the system? How can I tell if my specifications are met? How can I tell if the requirements of the pertinent standards are met? Will staff resources do system testing or will this be outsourced? Do I have a good test plan generated from my procurement specifications and the associated ITS standards? What tools do I have available and what tools will I need to perform adequate testing?

Other important factors to consider in the procurement of ITS standards-based systems that may have a profound affect on post implementation include:

- ***Maintenance and Support*** – Once the system is built, how do I maintain it in good working order? What kind of support is needed to maintain the system (e.g. additional staff, vendor contracts, etc.)? One must keep in mind that many standards are emerging and the use of draft standards bring along risks of change – how can I upgrade to the final standard if my agency was involved in a lead deployment using draft standards?
- ***Documentation and Training*** – What documentation do I need to have on hand to ensure that the staff adequately understands the system? What are my training needs (consider both operations and maintenance)? Do I need additional staff resources with specialty training?

- ***Warranty considerations*** – What is the warranty period? What costs are associated with extended warranties?

Please see the NHI – ITS Software Acquisition Course based upon *The Road to Successful ITS Software Acquisition* for additional information on software acquisition.

Chapter 4: Review

Questions:

1. New NTCIP standards documents are moving toward a new format consisting of six main topic areas. What are those six main topic areas?
   a. Foreword, General, Object Definitions, Conformance Statement, and Appendix
   b. Executive Summary, Introduction, Data Elements, Conformance Statement, and Profile Implementation Statement
   c. Concept of Operations, Functional Requirements, Dialogues and Sequences, Data Dictionary, Traceability Matrix, and Test Procedures
   d. None of the above

2. True or False. An agency does not need to have a solid understanding of their project requirements before entering into contract negotiations, and preferably before developing any procurement documents.
   a. True
   b. False

3. When manufacturers/developers define data elements for specific functions that are not covered by the NTCIP device standard and add them to the MIB, these additional data elements are called: _____
   a. MIB extensions
   b. Other functions
   c. Overhead
   d. None of the above

4. True or False. Before any testing begins, there must be a clear statement and understanding of the requirements that must be met and the minimum acceptable performance levels.
   a. True
   b. False

5. Name one software tool that is available for use in NTCIP testing and is freely available for download from the NTCIP website.
   a. Field Profile Test Suite
   b. NTCIP Exerciser
   c. Field Simulation Suite
   d. No software tools exist for testing

6. What Transport Level protocol selection is used with non-routable protocols (no routing of messages through an intermediate hub or field master)?
   a. Simple Network Management Protocol (SNMP)
   b. Transmission Control Protocol (TCP)
   c. User Datagram Protocol (UDP)
   d. Transportation Transport Protocol (T2, formerly know as NULL protocol)

7. The_____ section of an NTCIP standards document shows data elements arranged in groupings based upon the data associated with various levels of functionality.
   a. Overview
   b. Concept of Operations
   c. Dialogs
   d. Conformance Statement

8. Can there be an Optional data element within an Optional conformance group.
   a. Yes
   b. No
   c. All of the above
   d. None of the above

9. What documents can be found in the Library on the NTCIP website that focus on lessons learned from recent NTCIP deployments?
   a. NTCIP Guide
   b. Project Status Reports
   c. NTCIP Case Studies
   d. NTCIP Standards

10. The Simple Transportation Management Framework (STMF) defines two Conformance Levels. Conformance Level 1 includes the Simple Network Management Protocol (SNMP). What Application Level protocols are included in Conformance Level 2?
   a. Transmission Control Protocol (TCP) and User Datagram Protocol (UDP)
   b. Simple Network Management Protocol (SNMP) and Simple Transportation Management Protocol (STMP)
   c. Simple Network Management Protocol (SNMP) and Simple Transportation Management Framework (STMF)
   d. Simple Transportation Management Protocol (STMP) and Transportation Transport Protocol (T2, formerly know as NULL protocol)

11. The selection of Information Level standards, conformance groups and data elements is based upon the desired_____ of the system being implemented.
   a. Manufacturer
   b. Functionality
   c. Communications media
   d. Procurement method

12. Newer NTCIP standards have added a_____ as a means of providing a more user-friendly presentation of conformance.
   a. Data Element Summary
   b. Concept of Operations
   c. Profile Implementation Conformance Statement (PICS)
   d. Glossary

13. An agency is developing a set of procurement documents. The project requirements call for a traffic signal controller to have a minimum of 16 phases and they have duly noted this as a functional requirement for the device

procurement specifications. What is the minimum Range Value that must be supported by the NTCIP Actuated Signal Controller maxPhases data element?

a. 16
b. 8
c. 12
d. 40

14. Can Center-to-Center communications occur within the same building?
    a. Yes
    b. No
    c. Always
    d. Never

15. Center-to-Center procurements are essentially _____ acquisitions.
    a. Hardware
    b. Software
    c. Equipment
    d. Service

Answers:

1. (c) Concept of Operations, Functional Requirements, Dialogues and Sequences, Data Dictionary, Traceability Matrix, and Test Procedures

2. (b) False, an agency does need to have a solid understanding of their requirements before entering into negotiations, and preferably before developing procurement documents.

3. (a) MIB extensions

4. (a) True

5. (b) NTCIP Exerciser

6. (d) Transportation Transport Protocol (T2, formerly know as NULL protocol)

7. (d) Conformance Statement

8. (a) Yes, regardless of the conformance group being optional or mandatory, specific data elements with each conformance group may also be mandatory or optional.

9. (c) NTCIP Case Studies

10. (b) Simple Network Management Protocol (SNMP) and Simple Transportation Management Protocol (STMP)

11. (b) Functionality

12. (c) Profile Implementation Conformance Statement (PICS)

13. (a) 16 is the minimum Range Value for the maxPhases data element that must be supported in order for the communication requirements to agree with the functional requirements.

14. (a) Yes, Center-to-Center communications take place between computer systems, and those computers or systems may be within the same building or in separate buildings.

15. (b) Software

Chapter 5

Designing NTCIP

5.1 Introduction

This chapter is intended to provide an overview of communication bandwidth calculations and some of the issues that should be considered when designing an NTCIP communications system. While the title of this section is *Designing NTCIP*, the focus of the material presented deals with how to design a communications system for use with NTCIP. This section is intended for those system designers, system integrators and manufacturers who are tasked with determining communication system design and performance criteria.

5.2 Calculate Bandwidth Requirements

The NTCIP standards do not address issues related to specifying bandwidth requirements or how bandwidth is allocated. Bandwidth is basically how much information can be sent through a connection. It is usually expressed as bits-per-second. Most communications networks permit multiple applications, users, and/or devices to access a common communications link. Sharing the link must be equitable. Some NTCIP standards address the requirements of several communications links or subnetworks, but do not state which ones will be used for specific applications. These are application and implementation specific issues. Planners and implementers must decide these issues. This leads to the question of whether a communications link or subnetwork has enough bandwidth to support the desired information exchanges.

"The NTCIP standards do not address issues related to specifying bandwidth requirements or how bandwidth is allocated."

An implementation of a system must include a specific choice of a subnetwork or subnetworks. This choice must be able to accommodate the information exchanges that are needed for proper setup, operation and monitoring of a system. Planners and implementers must understand that a specific media may limit what can be sent. This section provides several examples of how to estimate what can be sent, the overhead associated with sending it, and the organization of the physical media to support the information exchanges.

5.2.1 Center-to-Field Bandwidth Requirements

In C2F communications, bandwidth considerations are of great concern to planners and implementers. Unlike an office environment, C2F communications links are generally less than 56 Kbps. Hundreds of existing systems use multi-drop, 1200 bps modems. Compounding the issue, these links tend to be dedicated to the transportation application and are the full responsibility of the transportation personnel to design, implement and maintain. The following bandwidth analyses should help to understand the factors and thinking that go into understanding bandwidth requirements and calculating an appropriate communications data rate.

Note: *Many devices, such as dynamic message signs, advisory radio transmitters, ramp meters, traffic detector stations and weather stations are usually much less sensitive to timing and latency issues due to much less frequent communication between center and device. Communications to these devices can typically be operated satisfactorily using SNMP, even at 1200 bps.*

The following two analyses will be used to discuss a few of the many alternative techniques that can be used in a C2F multi-drop communications system using NTCIP. Examples (by no means a complete list) of options available include:

- Use SNMP for all or some messages
- Use STMP for all or some messages
- Use only standard data elements, or also use some manufacturer specific data elements
- Use a bit rate of 1200, 2400, 4800, 9600, 19200, or other bit rate
- Use half duplex or full duplex communications
- For full duplex, overlap or do not overlap outgoing with incoming messages
- Use twisted pair, fiber, radio, leased lines, or other media
- For twisted pair and leased lines, use one or two pairs per channel
- Use modems that are fast or slow to reach the ready state when communication is to be established
- Limit the maximum number of devices on a channel to 2, 4, 6, 8, 10, or other number
- Gather detector data on a clock time basis, for example every minute, or signal cycle basis
- Request each type of data every second, every minute, or every hour.
- Use a fixed or variable polling cycle duration
- Use a fixed or variable device sequence in the polling cycle

- Use a fixed or variable message sequence for each device
- Wait for response in same poll or get it in next poll
- Interleave upload/download messages or suspend status and get it over with ASAP
- Use the same status message all the time, or different status messages
- Insert occasional non-status requests in place of or in addition to status request
- Allow spare time in a polling cycle for additional non-status messages, or allow the cycle to expand when non-status messages added

With the exception of manufacturer-specific data elements, any controller that meets all mandatory, optional and recommended requirements of the relevant NTCIP C2F standards for that field device type will support all of the relevant functions and operations suggested above and many more, without any software change.

5.2.2 Center-to-Field Bandwidth Analysis

For purposes of discussion, let's say it is desired to use NTCIP C2F communications in an imaginary traffic control system. The system consists of a central management application that is used to setup, monitor and control a network of intersection traffic signal controllers. The primary communications requirements of the imaginary system are:

1. Synchronize the time and date in all field devices.
2. Provide a map display of the status of all intersections.
3. Control the overall coordination timing pattern to be put into effect.
4. Control the operation of two lane-closed signs.
5. Monitor all intersections for any abnormal conditions.
6. Accumulate volume and occupancy data for 16 detectors to perform off-line optimization.
7. Provide full upload and download of the complete database or programming data in each field device.
8. Support 24 signalized intersections in the system.

This example will be used to:

- Discuss what data element definitions support this functionality;
- Characterize the overhead of sending the information via various protocols;
- Compare and contrast modems;
- Define the number of drops on a communications channel; and

- Calculate appropriate modem speed to accommodate the information and timing characteristics.

A slightly modified set of requirements will be used to describe a polling sequence approach to define when message exchanges take place.

Estimate Message Exchanges and Frequency

The first step in this analysis is to define what information exchanges will be used to meet the required functionality and how often they occur.

To synchronize the time and date in all field devices, the following data element from NTCIP 1201 will be used:

globalTime - Section 2.4.1

This data element can be used in a message to set or retrieve the current date and time in a remote device. Typical usage is to send the command to all intersections at least once a day. The time in each individual intersection is checked (read) at least once a day, as well.

To provide a map display of an intersection the following data elements defined in NTCIP 1202 will be used:

phaseStatusGroupGreens - Section 2.2.4.4

phaseStatusGroupYellows - Section 2.2.4.3

phaseStatusGroupWalks - Section 2.2.4.7

phaseStatusGroupPedClrs - Section 2.2.4.6

phaseStatusGroupVehCalls - Section 2.2.4.8

phaseStatusGroupPedCalls - Section 2.2.4.9

overlapStatusGroupGreens - Section 2.10.4.4

overlapStatusGroupYellows - Section 2.10.4.3

cordPatternStatus - Section 2.5.10

shortAlarmStatus - Section 2.4.9

These data elements provide green and yellow indications for up to 8 vehicle phases and 8 overlaps, walk and pedestrian clearance indications for up to 8 pedestrian movements, the current coordination pattern (cycle, split and offset) in effect, and an indication of preemption, problems with the coordination pattern, any detector fault, or some other type of fault condition. This information is intended to provide a real-time display and is typically read from each intersection controller on a once-per-second basis.

To control the timing pattern to put into effect and turn on and off the lane closed signs, the following data elements from NTCIP 1202 will be used:

systemPatternControl - Section 2.5.14

specialFunctionOutputState (1) - Section 2.4.14.2

specialFunctionOutputState (2) - Section 2.4.14.2

This information is intended to be sent to all intersections about once per minute.

To retrieve volume and occupancy data from two volume/occupancy detectors at a time, the following data elements from NTCIP 1202 will be used:

volumeOccupencySequence - Section 2.3.5.1

detectorVolume (1) - Section 2.3.5.4

detectorOccupency (1) - Section 2.3.5.4

detectorVolume (2) - Section 2.3.5.4

detectorOccupency (2) - Section 2.3.5.4

The volume and occupancy data would be read approximately once-per-minute. It is typical to have "count stations" spread out over several intersections. This type of information would be asked for from the intersections that have one or more count stations.

To provide additional information about the status of an intersection, the following data elements will be used:

unitAlarmStatus1 - Section 2.4.8

localFreeStatus - Section 2.5.11

These data elements are to read only when the shortAlarmStatus indicates some type of fault condition. They provide more detail about any potential fault condition. Typically this would occur no more than once-per-hour.

To provide complete upload and download of a controller's database, the following block objects as defined in NTCIP 1202 (version 2) are used:

Data ID & Type Data – Section 3.1

Phase Data – Section 3.2

Vehicle Detector Data – Section 3.3

Pedestrian Detector Data – Section 3.4

Pattern Data – Section 3.5

Split Data – Section 3.6

Timebase Control Data – Section 3.7

Preempt Data – Section 3.8

Sequence Data – Section 3.9

Channel Data – Section 3.10

Overlap Data – Section 3.11

Port 1 Data – Section 3.12

Schedule Data – Section 3.13

Day Plan Data – Section 3.14

Event Configuration Data – Section 3.15

Dynamic Object Configuration Data – Section 3.16

Dynamic Object Owner Data – Section 3.17

Dynamic Object Status Data – Section 3.18

Miscellaneous Data – Section 3.19

These block objects are defined as `OCTET STRING` [an ASN.1 data type that is used to specify octets (eight-bit bytes) of binary or textual information] objects consisting of anywhere between 10 and 128 discrete objects. The NTCIP 1202 Standard (version 2) defines block objects by grouping previously defined data element definitions into larger blocks (hence, the term 'block objects') enabling a faster transmission. Additionally, each manufacturer will most likely define additional data element definitions and proprietary block objects to enable special features that set them apart from other manufacturers. The block objects could define the entire "database" of a device. They would only be sent and retrieved on an as-needed basis and would, at most, occur no more than once-per-day. They could represent the records in file upload or download. While these data elements are not currently defined in an NTCIP standard, they represent real system requirements.

In the course of fine-tuning an intersection, numerous programming entries for phase timing and coordination might be sent once or twice a day. The following data elements would be typical:

phaseWalk - Section 2.2.2.2

phaseMinumumGreen - Section 2.2.2.4

phasePassage - Section 2.2.2.5

patternCycleTime - Section 2.5.7.2

patternOffsetTime - Section 2.5.7.3

splitTime - Section 2.5.9.2

The typical intersection is set up for 5-phase operation and has only 6 timing patterns defined. It is assumed that only one phase or pattern would be adjusted at any one time. Therefore, the number of data elements associated with this type of operation is assumed to be 5.

Exhibit 5.1 summarizes the messages and the how often they occur.

Exhibit 5.1: Frequency of Messages

Message Exchange	Frequency
Date and Time	1 per day - all
Intersection Map Data	1 per second X 24 intersections
Pattern Command	1 per minute - all
Detector Data	1 per minute X 8 intersections
Detailed Status	1 per hour X 8 intersections
Upload Download	1 per day X 24 intersections
Tuning	2 per day X 24 intersections

Estimate Application Message Size

The following two rules of thumb can be used to estimate SNMP and STMP messages (not including Block Objects):

1. SNMP Message Size = 26 bytes of header + 23 bytes per data element
2. STMP Message Size = 1 byte of header + 1 byte per data element

These rules are approximations and do not include lower layer protocol overhead. The rules are based upon the assumption that most exchanges deal with status and control data elements that can be expressed in one byte. The majority of set up data elements can also be expressed in one byte. The rules of thumb would not apply to exchanges involving `OCTET STRING`s or `OBJECT IDENTIFIER`s. If you are willing to accept the rules as such, you can skip the next two sections. If you're into technical details, then the following sections provide an in depth explanation on how exact sizes of messages can be derived.

SNMP Application Message Bits and Bytes

The actual bits and bytes of an SNMP message are defined using the *Tag-Length-Value* representation method defined in ISO 8825, Basic Encoding Rules (BER). All data elements can be expressed as *Tag* (or *Type*) of either `SEQUENCE`, `INTEGER`, `OCTET STRING`, or `OBJECT IDENTIFIER`. The *Tag* indicates how to think of the *Value* component. It indicates that it may be number, string (or text), or the identifier of something. It can also indicate that what follows is a series of data that is expressed as a *Tag-Length-Value* of something. There are several derived types that represent subsets of `SEQUENCE`, `INTEGER`, `OCTET STRING`, or `OBJECT IDENTIFIER` but any derived type resolves to one of the aforementioned ones. The second component of a data element is its *Length*. For

example, the *Length* of the INTEGER "1" when represented in computer terminology is one. It represents how many bytes it takes to store "1" in memory. The OCTET STRING "public" has a *Length* of 6 because it is expressed in 6 bytes. The third component of a data element is its *Value*. The *Value* of INTEGER "112" is expressed as 0x70 in computer terminology [decimal 112 = 70 hexadecimal = 0111 0000 binary]. The OCTET STRING "p" is also expressed as *Value* 0x70. The reason a computer can differentiate the 0x70 as either "112" or "p" is because of the *Tag*.

An SNMP message is defined as a SEQUENCE and Length of two predefined fields that describe the protocol, plus a field that defines the data carried by the protocol. The predefined fields consist of version and community name. Both the version and community name are expressed in the *Tag-Length-Value* form. A data field that follows it describes the operation that is to be performed. The **SetRequest PDU** field at the end of row is expanded in the row below. This is illustrated in the **SNMP Message Fields** row of Exhibit 5.2.

Note that the expanded **SetRequest PDU** field starts with the *Tag* of the operation, is followed by the *Length* of the data that follows, and consists of *Value*s of three *Tag-Length-Value* fields. The last field of **SetRequest PDU** consists of the **Variable Bindings** field. It is expanded on the next row.

As before, it begins as a *Tag-Length-Value* of a SEQUENCE and Length of one or more **Bindings**. The last row in the figure is getting closer to defining the actual data is, but we have to go through another *Tag-Length-Value* sequence to describe the *identity* and *value* of a single data element or **Bindings**.

From the communications perspective, each of the data elements defined in one of the Object Definitions Standards such as NTCIP 1201 or NTCIP 1202 has two components: an *identity* and a *value*. The *identity* part of the globalTime data element is its OBJECT IDENTIFIER (OID). The full OID of globalTime is:

```
<iso.org.dod.internet.private.enterprises.nema.transportation.dev
ices.global.globalTimeManagement.1>
or
<1.3.6.1.4.1.1206.4.2.6.3.1.0>
```

The *value* component of globalTime is an INTEGER with a value such as 925997608. This particular value represents May 6, 1999 at 2:33 PM UCT expressed as the seconds since Midnight January 1, 1970. For a more detailed discussion on OID, please refer to Chapter 6.

The actual number of bytes that are used to encode the *identity* and *value* of the globalTime data element varies with protocols used. For SNMP, each component of the data element is expressed in the form of *Tag-Length-Value*. For globalTime, the *identity Tag* is OID (0x06). The *identify Length* value is 13 (0x0D). The *identity Value* is 1.3.6.1.4.1.1206.4.2.6.3.1.0 (0x2B06010401893604020603010 0). For the *value* component, the *value Tag* is INTEGER (0x02). The *value Length* is 4 (0x04). The *value* Value is 925997608 (0x37319A28).

If one goes through this exercise with various data elements, one can derive some general characteristics about the data elements used in this analysis. Most data elements are organized into tables and the OIDs of these data elements are 15 to 16 bytes long. Unlike `globalTime`, most data elements are defined as `INTEGERs` that, in the traffic signal controller application, have a value between 0 and 255. Most values are therefore expressed in one or two bytes. Compared to the example of `globalTime`, a typical identity would 2-3 bytes longer and the value would be 2-3 bytes shorter. The average binding for an individual data element is therefore 23 bytes, as shown in Exhibit 5.2. The fixed overhead of SNMP messages that are used to get or set one or more data elements is 26 bytes, as shown in Exhibit 5.2.

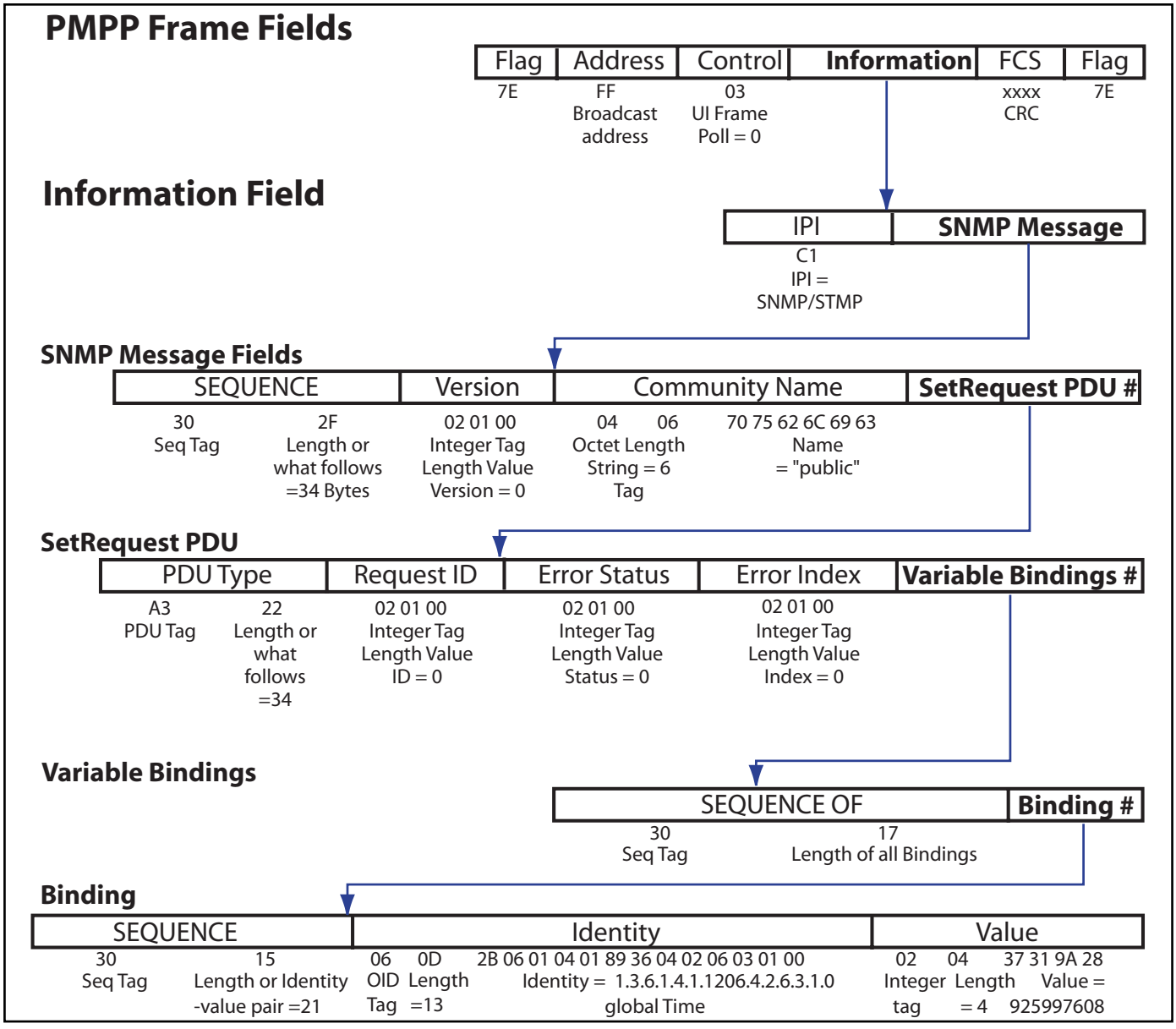


Exhibit 5.2: Set Time operation using SNMP over PMPP

ASN.1 Data Element Format and OID Decomposition

NTCIP functional area data dictionaries follow a consistent structure, known as an OBJECT- TYPE Macro developed by the Internet Community using Abstract Syntax Notation One (ASN.1). This structure defines data elements using a variety of descriptive fields. The macro is an existing well-accepted standard for describing data, and the NTCIP effort adopted it as the descriptive language of choice.

```
dmsNumPermanentMsg        OBJECT-TYPE
SYNTAX                    INTEGER (0...65535)
ACCESS                    read-only
STATUS                    mandatory
DESCRIPTION               "Indicates the current number of Messages
    stored in non-volatile, non-changeable memory (e.g. EPROM).
    For CMS  and BOS, this is the number of different messages
    that can be assembled."
 ::={dmsMessage 1}
```

The example data element is typical of such elements found in the NTCIP standards. This example identifies the number of messages held in non-volatile memory. The name of the data element is **dmsNumPermanentMsg**. *The macro structure also describes the syntax of the data element. In this case,* **dmsNumPermanentMsg** *is a two-byte integer with a designated range between 0 and 65,535.* Information as to how this data element is to be accessed is also provided. For this example, read-only access indicates that the management station is not allowed to write to the data element. A data element with read-write access would indicate that the data element could be used to either read values from a database or write values to a database, while other options include write-only and not-accessible. The macro status field indicates whether the data element is mandatory or optional within its conformance group. It is important to also note that conformance groups can either be mandatory or optional. Individual NTCIP standards should be reviewed to determine the appropriate conformance requirements. The description field provides a clear and unambiguous definition of the intended use of the data element. In this case, the **dmsNumPermanentMsg** data element *"Indicates the current number of Messages stored in non-volatile, non-changeable memory…"*. The last macro field indicates both the "parent" group and the number assigned to this "child" (data element) of the parent. The parent–child numbering scheme follows a tree structure for uniquely identifying data elements.

Object Identifier 1.3.6.1.4.1.1206.4.2.3.5.1 is for the dmsNumPermanentMsg Data Element

The above OID decomposes as follows:

1	3	6	1	4	1	1206	4	2	3	5	1
iso	org	dod	internet	private	enterprise	nema	transportation	devices	dms	dmsMessages	dmsNumPermanentMsg

Decomposition of the OID shows exactly where the **dmsNumPermanentMsg** data element can be found on the ISO "tree". All NTCIP data elements are under the NEMA node on the ISO "tree". NEMA has identified four nodes under its control and they are described as follows:

- ***mgmt(1)*** – The *mgmt(1)* subtree is used to identify data elements which are defined in NEMA-approved documents.
- ***experimental(2)*** – The *experimental(2)* subtree is used to identify data elements used in NEMA experiments. This is where new MIBs are placed prior to being assigned to the transportation node.
- ***private(3)*** – The *private(3)* subtree is used to identify data elements defined unilaterally. Enterprise specific data is defined under the private node.
- ***transportation(4)*** – The *transportation(4)* subtree is used by NEMA specifically for different classes of transportation equipment.

The NTCIP standards are represented under the transportation node. Under the Transportation node there are *protocol(1), devices(2)* and *tcip(3)* subtree structures. The devices group has additional subtrees for each of the supported device data dictionaries: actuated signal controllers, ramp meters, dynamic message signs, closed circuit television, environmental sensor stations, globals, etc. New branches are added to the "tree" structure when new devices are included in the NTCIP family of standards.

STMP Application Message Bits and Bytes

The actual bits and bytes of an STMP message are defined using Octet Encoding Rules (OER), as described in NTCIP 1102 – NTCIP Octet Encoding Rules (OER). Because the content of an STMP message is defined within both the sending device and the receiving device prior to being sent, it is possible to eliminate a number of fields and reduce overhead significantly. OER starts out with the *Tag-Length-Value* representation method used by SNMP. However, if the *Tag*, *Length*, or *Value* is known, the component is eliminated. If a data element is always an `INTEGER`, the fact that it is an `INTEGER` is not sent (*tag*). If a data element is always 2 bytes long, the fact that it is 2 bytes long is not sent (*length*). Since all data are expressed as a `SEQUENCE`, all `SEQUENCE` *Tags* and `SEQUENCE` *Lengths* are eliminated as well. This all boils down to the fact that only the *Value* of a data element is sent. However, if the SYNTAX of a data element indicates that the value can be of variable length such as `INTEGER` (as opposed to `INTEGER` (0…255)), then the length could be either 1 byte, 2 bytes, 3 bytes or 4 bytes requiring the sending device to indicate the number of bytes used to transmit the value.

In Exhibit 5.2, the **Binding** for `globalTime` consisted of Sequence, Length and Value of the Identity and Value pair where the Identity and Value pair were each encoded as *Tag-Length-Value*. The **Binding** in STMP would be the Value-*Value* or simply 0x37 31 9A 28 as shown in the last row of Exhibit 5.7. It is worth noting here that the same principle of eliminating any known *Tag*, *Length*, or *Value* was applied to the **SNMP Message Fields, Set Request PDU, and Variable Bindings** fields in Exhibit 5.2. This resulted in the one-byte **STMP Message Fields and Set Request PDU** field shown in Exhibit 5.3.

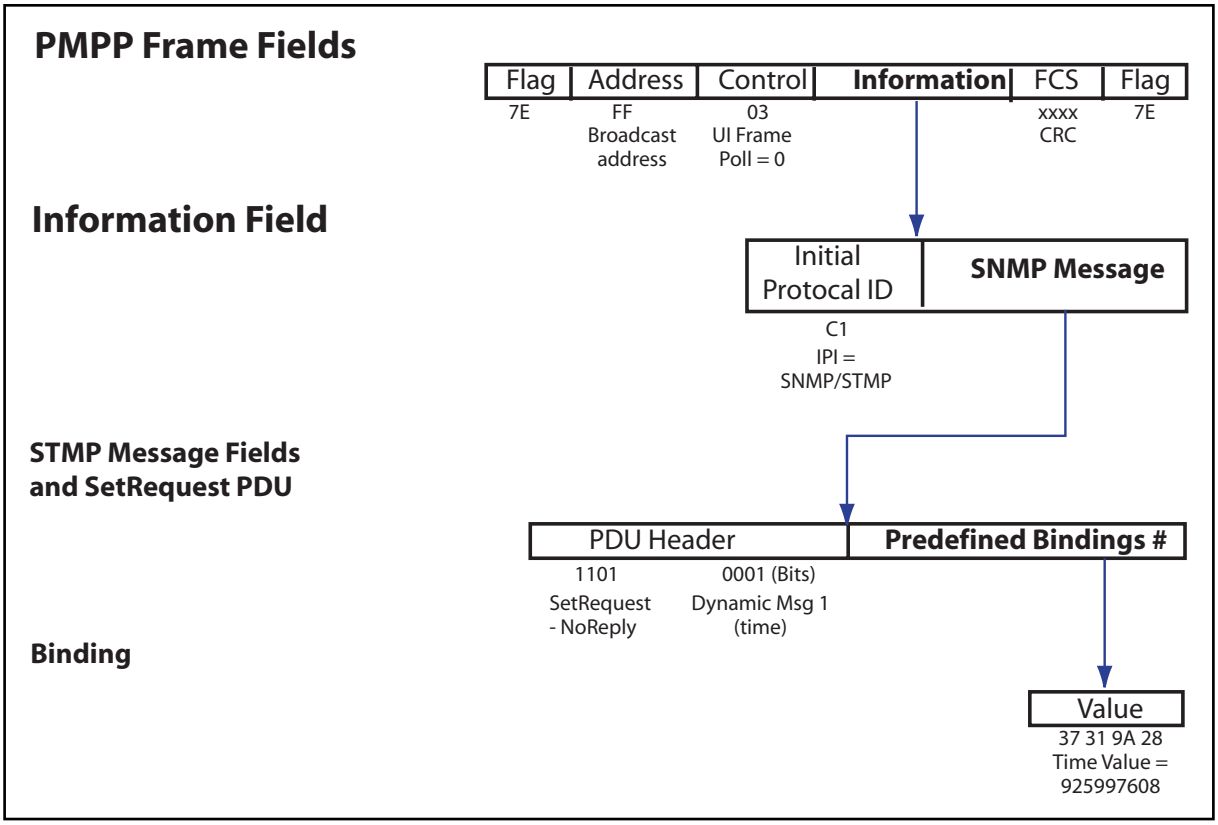


Exhibit 5.3: Set Time operation using STMP over PMPP

Estimate Application Message Exchanges

In any exchange of messages, one has to consider the size of both the command and response. In SNMP, the size of the command and response are approximately the same. In STMP, the size of the command and response are very different. The following two sections discuss the details.

SNMP Application Message Exchange Sizes

Using the SNMP rule of thumb, one can estimate the size of an SNMP message and exchanges by the number of data elements that are contained in them. Exhibit 5.4 summarizes the messages in the example, how many data elements are in the message, the command size in bytes and the size of an exchange.

Exhibit 5.4: Message Size Example

SNMP Message Overhead	Data Elements	Command/ Response Size	Exchange Size
Date and Time	1		98
Intersection Map Data	10		512

Exhibit 5.4: Message Size Example (Continued)

SNMP Message Overhead	Data Elements	Command/ Response Size	Exchange Size
Pattern Command	3		190
Detector Data	5		282
Detailed Status	2		144
Upload Download	1 + bytes	59 - 177	118 - 254
Tuning	5		282

In SNMP, typical commands and the responses have about the same number of bytes. A `getRequest` command will contain placeholders for values that would be contained in a response to it. In a `setRequest`, the values of data elements that are to be set are contained in the set command. In the corresponding `setResponse`, the same values would also be included to indicate what the data elements were actually set to. Therefore, in an SNMP exchange, the number of bytes is equal to two times the message size.

STMP Application Message Exchange Sizes

The rule of thumb for estimating STMP message size is 1 byte + 1 byte per data element. To estimate message exchanges, however, one has to understand that only a command or response contains the value(s) of any associated data element(s). To eliminate as much overhead as possible, a management application can also send a command where no reply is necessary. An STMP `getRequest`, `getNext` and `setResponse` do not contain any data element values. An STMP `setRquestNoReply` does not return any response. Exhibit 5.5 summarizes the typical command and responses.

Exhibit 5.5: Typical Command and Responses

Command	Response
getRequest	GetResponse + value
getNext	GetResponse + value
setRequest + value	SetRespone
setRequestNoReply + value	[no response]

Exhibit 5.6 shows what commands will be used to set or get the data elements. It also lists the size for each command and response. By summing the size of the command and response, the size of the message exchange can be derived.

Exhibit 5.6: Derivation of STMP Message Exchange Sizes

Dynamic Message	Command	# of Data Elements	Size		
			Command	Response	Exchange
Date and Time	setRequestNoReply	1	2	-	2*
Date and Time	getRequest	1	1	2	3*
Intersection Map Data	getRequest	10	1	11	12
Pattern Command	setRequestNoReply	3	4	-	4
Detector Data	getRequest	9	1	10	10
Detailed Status	getRequest	2	1	3	3
Upload Download	N/A	-	-	-	-
Tuning	N/A	-	-	-	-

* As with any rule of thumb, it does not always apply. The actual sizes are 5 and 6, respectively.

The setting of Date and Time and Pattern Command will be handled with the `setRequestNoReply` commands. Retrieving of Date and Time will be handled with a `getRequest` command and `getResponse` reply. The Intersection Map Data, Detector Data and Detailed Status will be handled with the `getRequest` command and `getResponse` response. Several Upload Download messages could, in theory, be defined as Dynamic Objects. However, the limited number of definable Dynamic Objects (13) would tend to preclude this. Some implementations may specifically prohibit this, as well. The Tuning message while easily defined in SNMP cannot be predefined in STMP because various phases and patterns would have to be indexed.

Estimate Transport and Subnetwork Protocol Size

The Point-to-MultiPoint (PMPP) and Point-to-Point Protocols (PPP) share a common header structure that has 6 fields associated with it. These fields consist of starting flag, address, control, information, checksum and a closing flag. The address field in PMPP is typically one byte, but could be extended. The address field in PPP is always 0xFF and is one byte. The fields are illustrated in Exhibit 5.2, in the **PMPP Frame Fields** row.

The first field in the **Information Field** indicates the next higher-level protocol to process the information. This field is referred to as the Initial Protocol Identifier (IPI). For non-networked communications, a "null" or no transport or network protocol is used. The IPI in this case is 0xC1 and indicates that the information should be passed directly to SNMP or STMP.

One particular facet of PMPP that may come into play but is not factored into the rules of thumb is byte stuffing. Byte stuffing ensures that the opening and closing flags are unique in any exchange. Any value of 125 (0x7D) or 126 (0x7E) occurring between the two flags will be padded with an additional byte. In this way, reception of a Flag (0x7E) uniquely identifies the beginning or ending of an HDLC frame. PPP also uses the byte stuffing technique but extends it to cover any value between 0x00 and 0x1F. On average, byte stuffing adds 1% overhead or 1 byte for every one hundred transmitted.

It is very likely that, in the future, field devices will support truly networked communications. Messages and exchanges could be routed from workstations on a local area network through a communications server or field processor to a device. In this scenario, the Internet UDP/IP Protocols would be used. Exhibit 5.7 illustrates all the typical fields and values used in sending a set `globalTime` message over a typical office environment, network communications stack. The message is sent via the SNMP Application Profile over a UDP/IP Transport Profile over an Ethernet Subnetwork Profile. The use of UDP/IP has an overhead of 28 bytes. A typical Ethernet Frame has an overhead of 24 bytes.

It is also possible to send STMP over UDP/IP over Ethernet. Exhibit 5.8 illustrates the same globalTime message sent via the STMP Application Profile over the same transport and subnetwork. Note that the only difference in transport and subnetwork layers is the value of the Destination Port in the UDP Header. SNMP uses the value 161 (0x00 A1) and STMP uses the value 501 (0x01 F5).

The term UDP/IP may be unfamiliar to transportation personnel. However, if a computer supports TCP/IP or the Internet Protocol Suite, it supports UDP/IP, as well. What this means, for example, is that a message that is meant to set the time-of-day in a variable message sign can be generated by and routed through the computers involved in C2C communications. The use of UDP/IP over Ethernet also typifies a real implementation. A traffic signal controller and dynamic message sign system in Toronto, Canada uses SNMP over UDP/IP over a mix of Subnetwork technologies. The current Advanced Transportation Controller – Model 2070 type field controller may use a 10 Mbps Fiber Optic Ethernet Subnetwork, as an example.

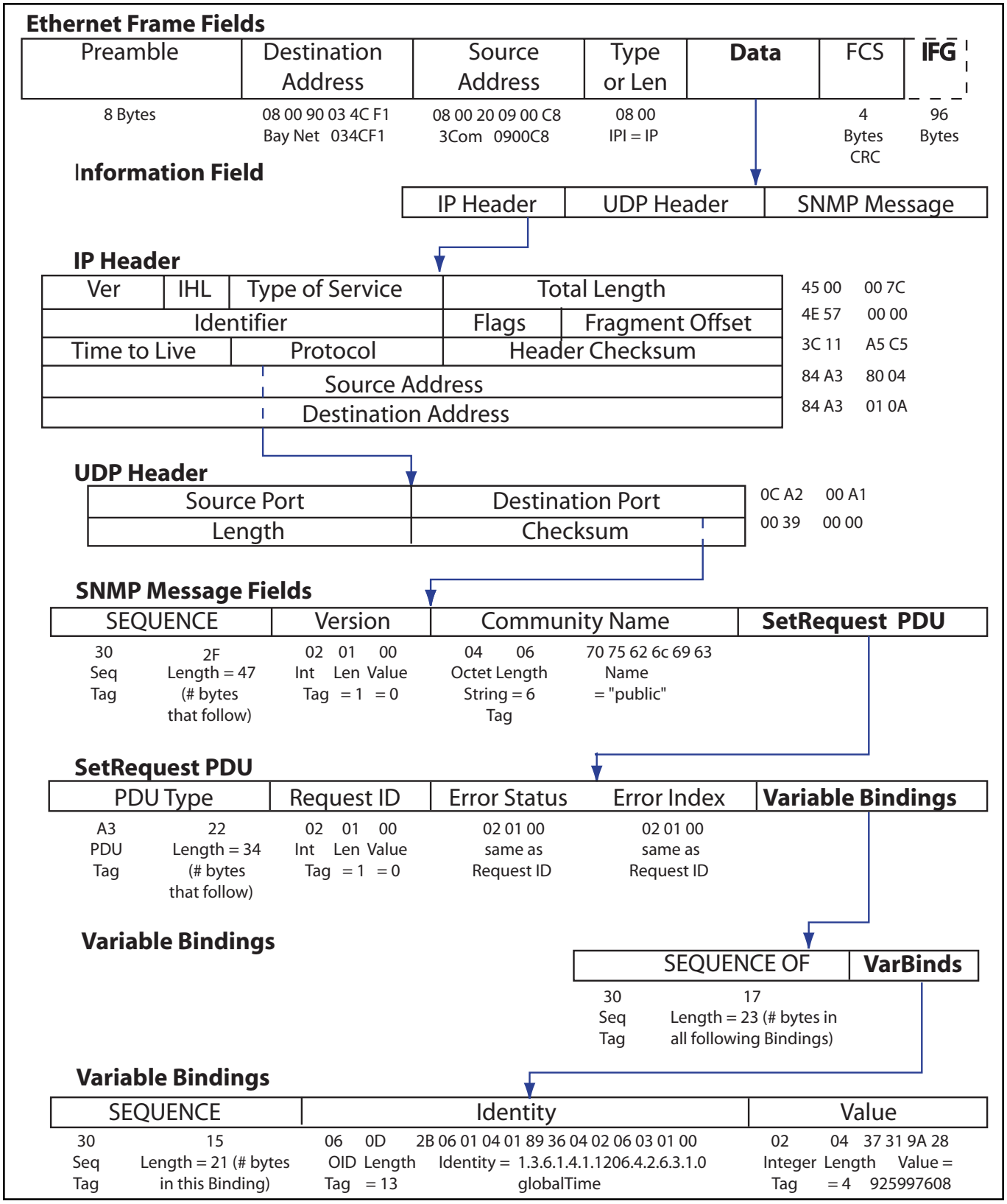


Exhibit 5.7: Set Time operation using SNMP over UDP/IP/Ethernet

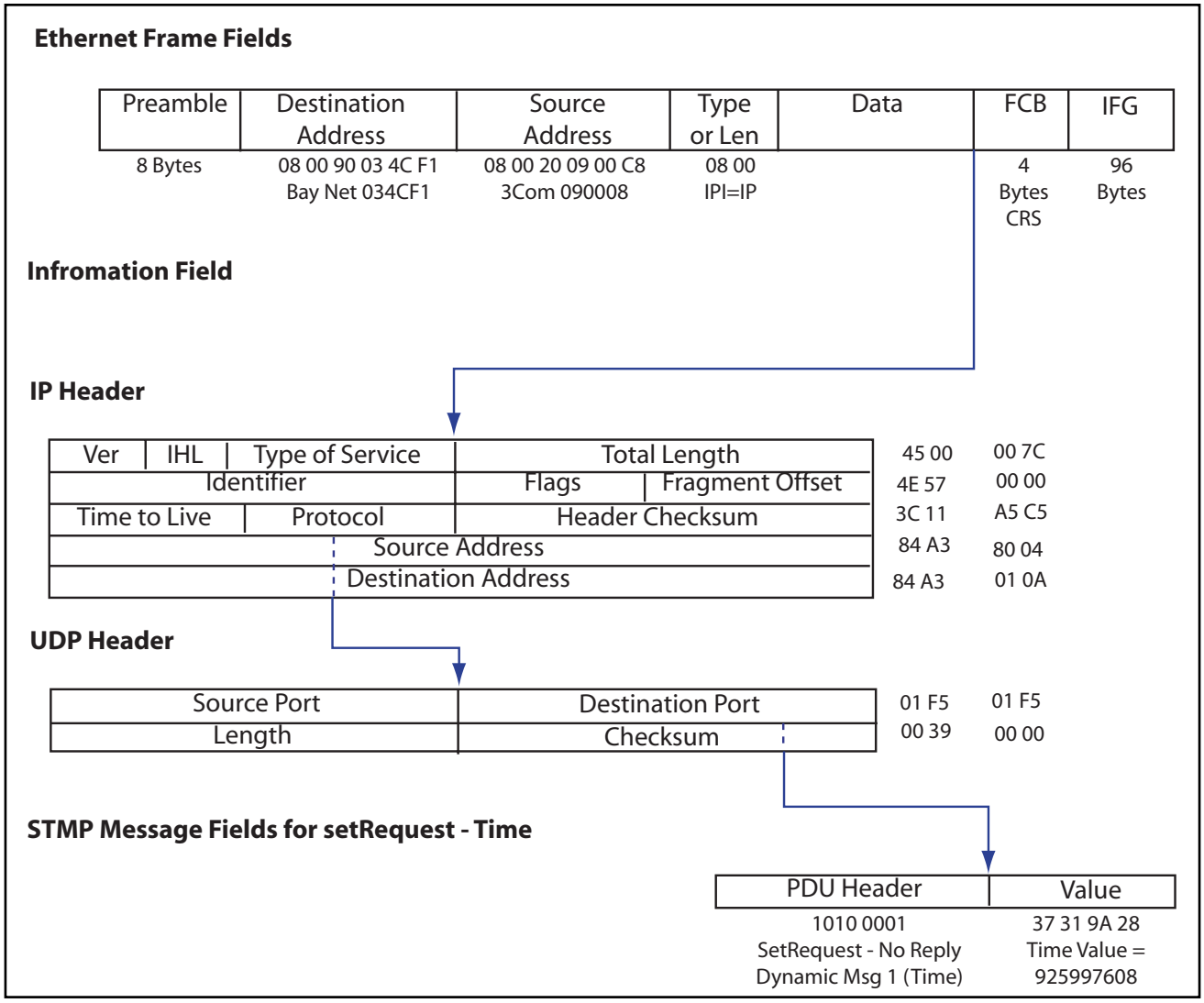


Exhibit 5.8: Set Time operation using STMP over UDP/IP/Ethernet

Exhibit 5.9 summarizes the overhead for the various transport and subnetwork protocols.

Exhibit 5.9: Overhead Estimates

Transport and Subnetwork Protocol	Overhead per Message	Overhead per Exchange
Null over PMPP	7	14
Null over PPP*	7	14
UDP/IP over PMPP	35	70
UDP/IP over Ethernet	54	108
*afterthedial-upsessionshasbeenestablished.Otherwise,thesevalueswouldbehigher.		

Estimate Timing Factors

In performing a bandwidth analysis, there are numerous timing factors that come into play. Processing delays, modem response and duplexing mode may need to be considered. One can intuitively understand that the response to a command asking for 100 data elements will take longer to process than one that only asks for 1 data element. Once a message is received, the device will need to parse it in order to understand what is being asked for or what is being sent. Once it understands what, it must then either gather the data or store away each data. It is very important to understand that processing delays will vary according to message content and implementation. For the sake of this analysis, a processing delay value of 50ms is used. Exhibit 5.10 shows a graphical representation of the various timing factors to be considered.

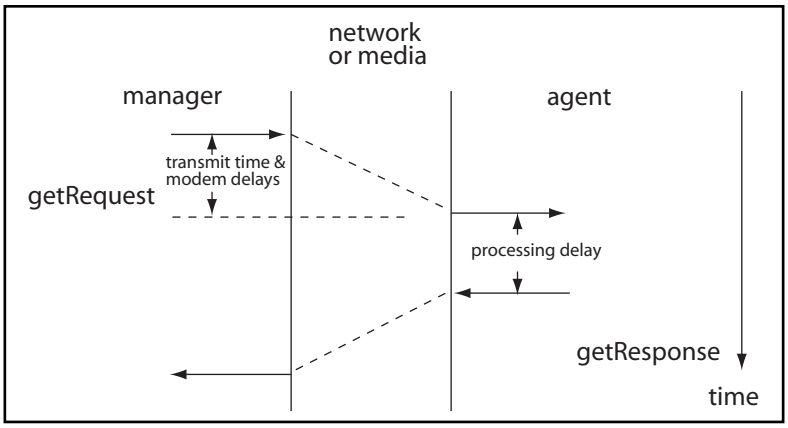


Exhibit 5.10: Timing Factors

Modem detect and turnoff delays can be as high as 2 or 3 seconds. The typical 56Kbps modem that one might use to log into the Internet takes several seconds to "train" or adjust to the wireline characteristics. These may be suitable for Point-to-Point operation, but in a multi-drop environment, a "fast" turn-on/turn-off type modem is the only practical choice. For the sake of this analysis, it is assumed that a "fast" modem will be used and that the turn-on and turn-off delays are on the order of 10 milliseconds each.

The duplexing mode of operation can have a significant impact on timing. In full-duplex mode, commands and responses can overlap, as shown in Exhibit 5.11. A second command can be sent while the response to a previous one is being received. In half-duplex mode, a second command cannot be sent until the response to the first is received. Full-duplexing can effectively cut the data rate requirements significantly. Exhibit 5.12 summarizes the delays that will be used in what follows.

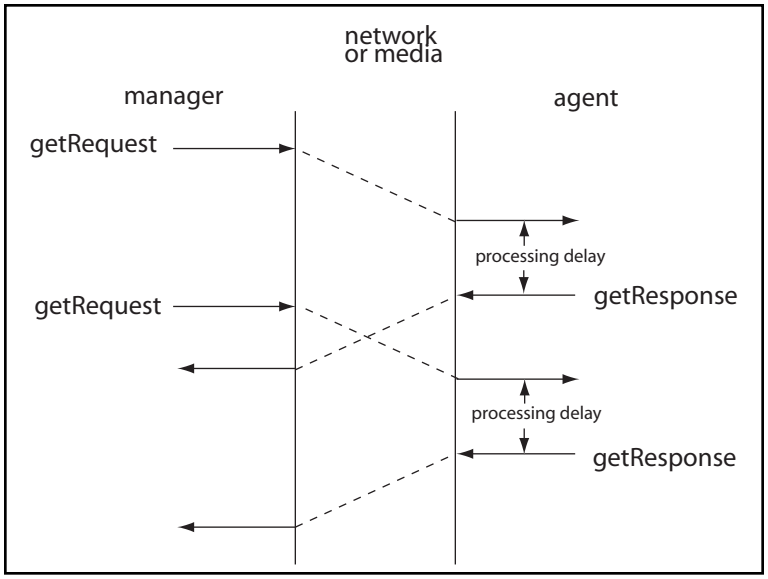


Exhibit 5.11: Full Duplexing

Exhibit 5.12: Delay Estimates

Delays	Time (ms)
Modem Carrier Turn-on	10
Modem Carrier Turn-off	10
Processing Delay	10
Total	**30**

Modems

C2F communications have traditionally used 1200 bps Frequency Shift Keying (FSK) modems for wireline communications. These modems come in different versions for different applications, such as half or full duplex, leased telephone lines (Bell 3002 voice circuit) or agency-owned twisted pair cable, internal or external to the device, support EIA/

TIA-232 flow control or not. In analyzing bandwidth requirements for copper communications plant and attempting to increase modem bit rate, it is important to remember that not all modems and bit rates may be practical for a given implementation environment. In particular, the following issues need to be considered:

1. Consumer modems used for general-purpose computer communications, for example, V.90 56kbps, cannot be used in multi-drop field implementations because they are too slow to reach ready state prior to each transmission (they require "training" time).
2. Consumer modems and modems designed for indoor use may not operate reliably in the temperature and humidity extremes encountered in field applications.
3. The fastest modems currently available for agency-owned twisted pair multi-drop applications operate at up to 28,800 bps.
4. Currently, modems suitable for multi-drop operation over leased telephone lines (Bell 3002 analog voice circuits) cannot support 9600 bps unless "a metallic circuit" is provided.
5. There is a limit to the distance that a modem can operate on agency-owned twisted pair cable. The maximum distance reduces as the bit rate increases and as the number of devices on the channel increases.
6. There is no distance limit on leased telephone lines.
7. Modems from different manufacturers can vary greatly in their features and operational characteristics. A thorough test of the actual modem planned for use (in a real-world long distance multi-drop environment) should be made before committing to its use. Note that many manufacturers provide a list of modems that have been tested to work with their equipment, but this does not ensure that different modems can be mixed on the same channel.
8. Some field devices do not yet have a 9600 bps internal modem option
9. Modems that are external to the field device (connected by a serial cable) require a dedicated suitable EIA/TIA-232 port on the field device, in addition to any serial port(s) used for other purposes, for example, laptop computer connection.
10. Asynchronous modems add a start and at least one stop bit for every byte (8 bits) transmitted; synchronous modems do not. This equates to a 25% increase in overhead.
11. Some processing devices have a limited capability to process the data handed it from the modem. Some legacy equipment isn't powerful enough to process at 9600 bps.

There are similar but different lists of constraints and considerations for modems or transceivers for other types of plant such as fiber and radio.

Electrical Limitations

The maximum number of modems on a wireline channel due to electrical limitations is an issue of modem sensitivity, the desired signal-to-noise ratio for a given bit-error-rate and the characteristics of the wire and interface. The *Communications Handbook for Traffic Control Systems*[1] provides an example of the characteristics and calculations for a 1200 bps FSK multi-drop system. The handbook goes into more detail than what is presented here and covers other technologies such as wireless and fiber optic.

Following the example in the handbook, the calculations for any modem technology that uses a wireline (twisted pair) medium would apply. The formula for determining maximum number of drops is:

Number of Drops = (Sensitivity - Cable Loss - S/N Ratio)/Insertion Loss per Drop

Exhibit 5.13 shows hypothetical characteristics of a 9600 bps modem and wiring that is to be used in a multi-drop configuration.

Exhibit 5.13: Modem Parameters

Parameter	Value
Modulation Technique	Some type of Phase and Amplitude Modulation
Operation Mode/Line	Full Duplex/4 wire (metallic or user owned)
Modem Frequencies	Center Frequency ~ 9600 Hz
Receiver Sensitivity	0 dBM to -39 dBM
Signal-to-Noise Ratio	15 dB for a Bit-Error-Rate of 1×10^{-5}
Cable Loss	3.3 dB/mile at 9600 Hz for 19 AWG
Insertion Loss	.5 dB per drop
Distance	8 miles

The modulation technique used by a modem may not always be FSK. Phase Shift Keying (PSK) and Quadrature Amplitude Modulation (QAM) are typically employed to increase throughput without necessarily increasing the signaling frequency. The operating mode of the 9600 bps modem is assumed to be full duplex using two wire pairs (four wires). This configuration minimizes distortion from line reflections and the turnaround times associated with switching from transmit to receive. The signaling frequencies are assumed to be 9600 Hz. The signaling frequencies will vary with modulation techniques but must be quantified because they will determine the cable losses. Receiver sensitivity is an indication

1. Communication Handbook for Traffic Control Systems, Federal Highway Administration Report FHWA-SA-93-052, April 1993

of how well a modem is at picking up weak signals and signal-to-noise ratio is the ability of a modem to pick out a signal with back ground noise (static). Insertion loss comes from a manufacturer's data sheet. There is always some type of loss associated with the connection to the wire. Usually this is due to slight impedance mismatches and physically routing the signal through a connector to the modem electronics. For a given signaling frequency, the size of the interconnect wire will define how much signal is lost over some distance. The cable loss is derived from Figure 6-2 in the handbook. The distance from the primary to the farthest secondary is assumed to be 8 miles.

Using the formula given above, we can calculate that:

Number of Drops = (Sensitivity - Cable Loss - S/N Ratio)/Insertion Loss per Drop

Number of Drops = (39 dBM - (8 miles x 3.3 dB per mile) - 15 dB)/.5 dB

Number of Drops = (39 dBM - 19.8 dB - 15 dB)/.5 dB

Number of Drops = 8.2

Rounding down the value, we find that the maximum number of drops for this example is 8, from a purely electrical point of view.

Communications Limitations

The above discussion shows how to calculate the electrical limitations using modem and wireline techniques. It does not address the logical aspects of organizing a system into communications channels, defining what information is sent on each channel, or ensuring each channel can carry the desired information. What follows are the procedures and calculations to define the number of channels and drops per channel based on the message exchange requirements.

What we defined so far is:

1. Size of the message exchanges and how often they will occur are shown in Exhibit 5.14.

Exhibit 5.14: Message Frequency and Size

Message Exchange	Frequency	SNMP Exchange (bytes)	STMP Exchange (bytes)
Date and Time	1 per day - all	98	2
Intersection Map Data	1 per second X 24 intersections	512	12
Pattern Command	1 per minute - all	190	4
Detector Data	1 per minute X 8 intersections	282	7
Detailed Status	1 per hour X 8 intersections	144	4
Upload Download	1 per day X 24 intersections	118 - 254	N/A

Exhibit 5.14: Message Frequency and Size

Message Exchange	Frequency	SNMP Exchange (bytes)	STMP Exchange (bytes)
Tuning	2 per day X 24 intersections	282	N/A

2. Transport and Subnetwork Protocol Overhead estimates are shown in Exhibit 5.15.

Exhibit 5.15: Protocol Overhead Estimates

Transport and Subnetwork Protocol	Exchange Overhead (bytes)
Null over PMPP	14
Null over PPP	14
UDP/IP over PMPP	70

3. Processing and Modem Delay estimates are shown in Exhibit 5.16.

Exhibit 5.16: Delay Estimates 5.10 Delay

Delays	Time
Modem Carrier Turn-on	10ms
Modem Carrier Turn-off	10ms
Processing Delay	10ms
Total	**30ms**

The processing delay of traffic signal controllers is highly variable, with actual response times varying from 10ms to 50ms. Achieving response times at the lower end of this range, as shown in Exhibit 5.16, may require the use of techniques such as asynchronous messaging whereby the response to a request is placed in a buffer for immediate transmission at the next poll.

SNMP Timing

At this point, we need to choose specific protocols to analyze and then normalize the data exchanges and delays to some common time interval. For SNMP over Null over PMPP we have the values shown in Exhibit 5.17.

Exhibit 5.17: Normalized Data using SNMP over NULL over PMPP for 24 drops per channel

Message Exchange	Frequency	Message Exchange Size Bytes	Messages per day	Bytes per day
Date and Time	1 per day - all	112	24	2688
Intersection Map Data	1 per second X 24 intersections	526	2073600	1090713600
Pattern Command	1 per minute - all	204	1440	293760
Detector Data	1 per minute X 8 intersections	296	11520	3409920
Detailed Status	1 per hour X 8 intersections	158	192	30336
Upload Download	1 per day X 24 intersections	268	24	6432
Tuning	2 per day X 24 intersections	296	48	14208
Totals per day				

Normalizing the bytes per day to bits per second, we calculate the total system bandwidth required as:

1094470944 bytes per day x 10 bits per byte/86400 seconds per day = 12667.49 bits in one second

The value 126675 is the average number of bits that are required to transmit all message exchanges to and from the 24 intersection controllers in one second.

Given a specific modem speed, we can calculate a first order approximation of the number of drops per channel and channels. For a 9600 bps modem, this is calculated as:

126670 bits overall/9600 desired bits per channel = 13.19 channels

And

24 intersections/13.19 channels = 1.82 drops per channel

Rounding both of these figures downward, the use of 9600 bps modems would only work if there was a single modem and drop dedicated to each intersection. There are some systems that use a dedicated modem and cabling arrangement. If this is feasible, a second order approximation should be performed. A second order approximation accounts for the changes in the number of drops and the need to send broadcast messages on each channel.

The impact of any delays must also be considered. Since the steps are same for any protocol combination, only the reiterations for STMP over NULL over PMPP using 1200 bps modems will be illustrated. Additionally, no errors resulting in a need for retransmission is assumed.

Clearly, SNMP is not a feasible protocol choice unless each signal has a dedicated channel. In practice, such signal systems will use STMP.

STMP Timing

The STMP and PMPP Protocols were designed to be open to address diverse communications need yet be very efficient to meet the limited bandwidth capability of current systems. A typical traffic control system of today that controls 24 intersections uses a proprietary communications scheme, is usually configured as two groups of 12 intersections or three groups of eight intersections and uses internal 1200 bps FSK modems. Conversion of these systems to NTCIP may impact the existing configuration and require the use of higher speed modems. The following calculations for STMP over Null over PMPP should help understand what the potential impact may be.

For this NTCIP Stack, Exhibit 5.18 summarizes the messages, frequency and sizes of the message exchanges. As before, we begin by looking at the system as 24 intersections on a single drop and normalize the total exchanges to a per day basis.

Exhibit 5.18: Normalized Data using STMP over NULL over PMPP for 24 drops per channel

Message Exchange	Frequency	Message Exchange Size Bytes	Messages per day	Bytes per day
Date and Time (set)	1 per day - all	16	1	16
Date and Time (get)	1 per day X 24intersections	17	24	408
Intersection Map Data	1 per second X 24 intersections	26	2073600	53913600
Pattern Command	1 per minute - all	18	1440	25920
Detector Data	1 per minute X 8 intersections	21	11520	241920
Detailed Status	1 per hour X 8 intersections	18	192	3456
Upload Download	1 per day X 24 intersections	N/A	N/A	N/A
Tuning	2 per day X 24 intersections	N/A	N/A	N/A
Totals per day				

Normalizing the bytes per day to bits per second,

54185320 bytes per day x 10 bits per byte/86400 seconds per day = 6271.45 bps

The value 6271.45 bps is the average data rate required to transmit all message exchanges to and from the 24 intersection controllers

For this protocol configuration, let's try a 1200 bps modem. As before, we can calculate a first order approximation of the number of drops per channel and channels by dividing the number of averaged data rate value by the modem speed. For a 1200 bps modem, this would work out to drops per channel using channels.

These seem to be a reasonable values, so we need to perform a second order approximation. For this iteration shown in Exhibit 5.19, a configuration of 6 channels of 4 drops per channels will be used. The frequency of some of the messages will be adjusted accordingly.

Exhibit 5.19: Normalized Data using STMP over NULL over PMPP for 4 Drops per Channel

Message Exchange	Frequency	Message Exchange Size Bytes	Messages per day	Bytes per day
Date and Time	1 per day - all	16	1	16
Date and Time	1 per day - X 4 intersections	17	4	68
Intersection Map Data	1 per second X 4 intersections	26	345600	8985600
Pattern Command	1 per minute - all	18	1440	25920
Detector Data	1 per minute X 2 intersections	21	2880	60480
Detailed Status	1 per hour X 1 intersections	18	24	432
Upload Download	1 per day X 1intersections	N/A	N/A	N/A
Tuning	2 per day X 24 intersections	N/A	N/A	N/A
Totals per day				

Normalizing the bytes per day to bits per second,

9072516 bytes per day x 10 bits per byte/86400 seconds per day = 1050.06 bps

The value 1050.06 bps is the average data rate required to transmit all message exchanges to and from the 4 intersection controllers

This appears to be a reasonable value, but delays must be taken into account. Any delays will take away from the time that is available to be actually transmitting data. Total delay per second is calculated as:

349949 messages per day X .03 seconds delay per message/86400 seconds per day = 0.122 sec.

The value 0.122 seconds is the average delay per second. We calculate the modem speed to transmit 1050 bits in the remaining time as:

1050 bits/(1 sec. - 0.122 delay time) = 1195.90 bps

Therefore, 4 drops per channel at 1200 bps is a suitable configuration. If more drops per channel are desired, the data rate can be increased to possibly 4800 or 9600 bits per second, by using faster modems.

5.2.3 Center-to-Field Bandwidth Alternate Analysis

In the previous scenario, the emphasis was on acquiring once-per-second data from all intersections. This may not necessarily apply to all situations. In applications other than traffic signal control, this would certainly not be the case. The following scenario addresses the same requirements as before except for map display. In this case, the map display is only for one intersection at a time. In general, this scenario might apply to cases where there is a requirement for real-time (once-per-second) data from a single device but system data can be exchanged on a once-per-minute or longer basis. The communications requirements are summarized as:

1. Synchronize the time and date in all field devices.
2. Provide a map display of the status of **one** intersection.
3. Control the overall timing pattern to be put into effect.
4. Control the operation of 2 lane-closed signs.
5. Monitor all intersections for any abnormal conditions.
6. Accumulate volume and occupancy data for 16 detectors to perform off-line optimization.
7. Provide full upload and download of the complete database or programming data in each field device.
8. Support 24 intersections.

Estimate Message Exchanges and Frequency

In this scenario, all the previous messages will be used but a new one will be added. Since the map display information will only be gathered from one intersection, the status of the other intersections will be monitored by an "Intersection Status" set of data elements.

To provide indications of what coordination timing pattern is in effect and any abnormal condition at an intersection, the following data elements defined in NTCIP 1202 will be used:

systemPatternStatus - Section 2.5.10

shortAlarmStatus - Section 2.4.9

These are the same data elements used in the map display. However, the intersection map display is to be gathered from only one intersection at a time. These data elements would be used to monitor the other intersections in the system. For the purposes of monitoring, these would be read from each intersection approximately once-per-minute.

Exhibit 5.20 summarizes the new set of messages and the how often they occur.

Exhibit 5.20: Message Frequency Alternate Scenario

Message Exchange	Frequency
Date and Time	1 per day - all
Intersection Map Data	1 per second X 1 intersections
Intersection Status	1 per second X 23 intersections
Pattern Command	1 per minute - all
Detector Data	1 per minute X 8 intersections
Detailed Status	1 per hour X 8 intersections
Upload Download	1 per day X 24 intersections
Tuning	2 per day X 24 intersections

SNMP Application Message Exchange Sizes

Exhibit 5.21 summarizes the messages in the new scenario.

Exhibit 5.21: SNMP Message Sizes (Alternate Scenario)

SNMP Message Overhead	Data Elements	Command/ Response Size	Exchange Size
Date and Time	1		98
Intersection Map Data	10		512
Intersection Status	2	72	144
Pattern Command	3		190
Detector Data	5		282
Detailed Status	2		144
Upload Download	1 + bytes	59 - 177	118 - 254
Tuning	5		282

The only addition is the intersection status message.

STMP Application Message Exchange Sizes

Exhibit 5.22 is an update to Exhibit 5.6. The only difference is the addition of the Intersection Status exchange.

Exhibit 5.22: Derivation of STMP Message Exchange Sizes (Alternate Scenario)

Dynamic Message	Command	# of Data Elements	Size		
			Command	Response	Exchange
Date and Time	setRequestNoReply	1	2	-	2
Date and Time	getRequest	1	1	2	3
Intersection Map Data	getRequest	10	1	11	12
Intersection Status	getRequest	2	1	3	4
Pattern Command	setRequestNoReply	3	4	-	4
Detector Data	getRequest	9	1	10	10
Detailed Status	getRequest	2	1	3	3
Upload Download	N/A	-	-	-	-
Tuning	N/A	-	-	-	-

Other Estimates

In this example, the estimates for transport and subnetwork protocols remain the same. The timing factors and delays apply, as well.

Number and Size of Slots per Channel

The only new topic to be considered in the alternate example is the concept of communications slots. The number of communications slots per channel can best be thought of as the number of opportunities to communicate in any time period. It is not necessarily equal to the number of drops per channel. For example, assume that there are 8 drops per channel. If one needed to communicate with each drop once every minute, there could be 8 slots. The width of each slot in this case would be 7.5 second. An arrangement of 60 slots, each 1 second wide, would be just as suitable if all exchanges took less than 1 second. If this were the case, 52 slots would be available for other uses.

In the alternate example, only one message exchange needs to take place on a once-per-second basis. All other exchanges take place on a once-per-minute, once-per-hour, or one-per-day basis.

If the once-per-second exchange could be completed in less than one-half second, and all of the other exchanges could each be completed in less than one-half second, the concept slotting arrangement could be used. There could be two slots one-half second wide. The first slot would be reserved for the once per second exchange. The second slot would be used to perform all the other exchanges but on a rotating basis.

Communications Drops (Drops per Channel)

At this point, we are ready to perform the timing analysis. As before, it is necessary to pick a specific NTCIP Communications Stack. In the following examples, the transport and subnetwork protocols are assumed to be T2/Null and PMPP. Exhibit 5.23 summarizes the frequency and all overhead associated with the message exchanges.

Exhibit 5.23: Message Frequency And Size

Message Exchange	Frequency	SNMP Message Exchange Bytes	STMP Exchange Bytes
Date and Time	1 per day - all	112	15
Intersection Map Data	1 per second X 1 intersections	526	26
Intersection Status	1 per second X 23 intersections	158	17
Pattern Command	1 per minute - all	204	18
Detector Data	1 per minute X 8 intersections	296	21
Detailed Status	1 per hour X 8 intersections	158	18
Upload Download	1 per day X 24 intersections	268	N/A
Tuning	2 per day X 24 intersections	526	N/A

Since the "system requirements" require communications to 24 intersection controllers, the use of the PMPP and "fast" modems would allow multiple secondary devices to share a communication link. However, the characteristics of wire and the distances between intersections may place an upper limit on how many devices can share a communications link. For the sake of this analysis, the maximum number of drops is assumed to be 9. This would allow a management application and 8 intersections to share a channel. An assumption is made that the network of 24 intersections is to be organized into 3 drops of 8. The revised message frequency and size per channel would then be as shown in Exhibit 5.24.

Exhibit 5.24: Message Frequency and Size

Message Exchange	Frequency	SNMP Message Exchange Bytes	STMP Exchange Bytes
Date and Time	1 per day - all	112	15
Intersection Map Data	1 per second X 1 intersections	526	26
Intersection Status	1 per second X 7 intersections	158	17
Pattern Command	1 per minute - all	204	18

Exhibit 5.24: Message Frequency and Size

Message Exchange	Frequency	SNMP Message Exchange Bytes	STMP Exchange Bytes
Detector Data	1 per minute X 2 intersections	296	21
Detailed Status	1 per hour X 1 intersections	158	18
Upload Download	1 per day X 8 intersections	268	N/A
Tuning	2 per day X 8 intersections	526	N/A

SNMP Timing

Next, we analyze the exchanges to gauge the impact of multiple secondary devices and the frequency of the exchanges. In this example, the assumption is that the user wants to see the Intersection Map Data with some accuracy. Two back-to-back samples of the signal display would not be the same as two spaced exactly one second apart.

Considering this, the Intersection Map Data exchange should take place once every second on the second. Since all other exchanges take place on a minute, hour or day basis, the Intersection Map Data could be requested every second and all other exchanges requested on a rotating basis. To do this would require that the Intersection Map Data and the largest other exchange take place within one second. The largest exchange other than Intersection Map Data is the Tuning exchange. After summing up the size of the exchanges and processing delays, we can then compute the required data rate as:

*Data Rate = bytes * 10/(1 - delay)*

[The numbers of bytes is multiplied by 10 because in asynchronous communications, a start and stop bit is added to each byte.]

Exhibit 5.25 summarizes the overhead and delays associated with the Intersection Map Data and the Tuning message exchanges.

Exhibit 5.25: SNMP Overhead and Delay Estimate Example

Slot	Exchange	Size (bytes)	Delays and Processing (ms)
1	Intersection Map Data	526	70
2	Tuning	526	70
Totals			**140**

This results in a requirement to transmit 1052 bytes in one second with 140ms of delays. The required data rate is computed as:

*Data Rate = (1024 +28) *10/(1 - 0.140) = 1232.558 bps*

This number is too high for readily available "fast" multi-drop modems, so a new approach will be considered. Since the Tuning exchanges are meant to change the timing characteristics of the system and need to be performed manually, we can make the assumption that it does not have to run concurrently with the Intersection Map Data exchange. If we consider the next largest exchange, Detector Data, we come up with the values shown in Exhibit 5.26.

Exhibit 5.26: SNMP Overhead and Delay Estimate Second Example

Slot	Exchange	Exchange Overhead (bytes)	Delays and Processing (ms)
1	Intersection Map Data	526	70
2	Detector Data	296	70
Totals			**140**

*Data Rate = (794+28) *10/(1 - 0.180) = 10024.39 bps*

This value is still too high to consider 9600 bps modems. It is always a good engineering rule of thumb have some margin for error. To gain some margin one could consider the use of fiber optic modems. The carrier turn-on and turn-off delays could be significantly less than 20ms. If an intersection did not have pedestrian movements, dropping them from the Intersection Map Data Exchange could reduce the data rate to 8341bps. Minimizing carrier turn-on and turn-off delays could be also be accomplished by use of a simple full-duplex operation. The primary's carrier is always on and any secondary turns on it carrier as soon as it recognizes that it needs to send a response. Exhibit 5.27 summarizes the overhead and delays for a simple full-duplex operation arrangement.

Exhibit 5.27: SNMP Overhead and Delay Estimate Second Example

Slot	Exchange	Exchange Overhead (bytes)	Delays and Processing (ms)
1	Intersection Map Data	526	60
2	Detector Data	296	60
Totals			**120**

*Data Rate = 822 *10/(1 - 0.120) = 9340.909 bps*

Looking at the other exchanges, they could be mapped in to the second slot on a rotating basis as shown in Exhibit 5.28.

Exhibit 5.28: SNMP Command And Response Mapping To Third Slot

Interval	Command and Response
1	Date and Time
2	Detector Data - Pair 1
3	Detector Data - Pair 2
4	Detector Data - Pair 3
5	Detector Data - Pair 4
6	Detector Data - Pair 5
7	Detector Data - Pair 6
8	Detector Data - Pair 7
9	Detector Data - Pair 8
10	Status - Intersection 1
11	Status - Intersection 2
12	Status - Intersection 3
13	Status - Intersection 4
14	Status - Intersection 5
15	Status - Intersection 6
16	Status - Intersection 7
17	Status - Intersection 8
18	Pattern Command - Intersection 1
19	Pattern Command - Intersection 2
20	Pattern Command - Intersection 3
21	Pattern Command - Intersection 4
22	Pattern Command - Intersection 5
23	Pattern Command - Intersection 6
24	Pattern Command - Intersection 7
25	Pattern Command - Intersection 8
26	Spare
…	…
30	Spare

Assuming a total of 30 slots, each of these exchanges would have a resolution of once every 30 seconds. The only concern in this arrangement is that a new pattern command might not be transmitted until 29 seconds after it was selected. Since there are spare time slots, one approach could be to send any new Pattern Command as it occurs. In this case, however, it would be sent to all intersections using a group address.

STMP Timing

The above example shows that while SNMP could be used for some real-time applications, it may require higher data rates than traditional 1200 bps, FSK modems support. For these applications, STMP is more suited. The following illustrates how to calculate the bandwidth requirements for an STMP over Null over PMPP stack.

In this example, the messages are defined as dynamic objects. The OIDs of the data elements that comprise the messages are downloaded to Dynamic Objects 1 - 6 as follows:

Dynamic Object 1 = Time and Date

Dynamic Object 2 = Intersection Map Data

Dynamic Object 3 = Intersection Status

Dynamic Object 4 = Pattern Command

Dynamic Object 5 = Detector Data

Dynamic Object 6 = Detailed Status

Following the same strategy as in the alternate SNMP timing example, the Intersection Map Data and one of the other exchanges could be sent every second. Assuming Detector Data is the largest exchange to be handled in one second, we have the values shown in Exhibit 5.29.

Exhibit 5.29: STMP Overhead And Delay Estimate Example

Slot	Exchange	Exchange Overhead (bytes)	Delays and Processing (ms)
1	Intersection Map Data	26	60
2	Detector Data	21	60
Totals			**120**

*Data Rate = 47 *10/(1 - 0.120) = 534.091 bps*

Since this is well under the 1200 bps data rate that is typically available, we might want to consider sending a Pattern Command every second, as well. This would result in overhead and delays as shown in Exhibit 5.30.

Exhibit 5.30: STMP Overhead and Delay Estimate Second Example

Slot	Exchange	Exchange Overhead (bytes)	Delays and Processing (ms)
1	Intersection Map Data	26	70
2	Pattern Command	18	20
3	Detector Data	21	70
Totals			**160**

*Data Rate = 65 *10/(1 - 0.160) = 773.81 bps*

[Note that the Delay and Processing for a Pattern Command is only 20ms. Since this is sent as a `setRequestNoReply`, there should not be any internal processing required.]

Since 774 bps provides plenty of margin, one could increase the amount of information being brought back in the Intersection Map Data. For example, if the intersection had a preemption sequence, the `preemptState` - Section 2.7.2.16 could be added. This data element could be used to indicate the state or interval of a preemption sequence. Another data element that could be added is `phaseStatusGroupPhaseNexts` - Section 2.2.4.11. This would indicate the next vehicle phase that is to be serviced at the end of any currently timing phase.

As in the SNMP example, the other exchanges could be mapped in to the third slot on a rotating basis as shown in Exhibit 5.28.

5.2.4 Center-to-Center Bandwidth Requirements

C2C communications typically involve communications networks connecting many computers in a peer-to-peer arrangement. These networks typically involve both local area networks, for example, within a building or adjacent buildings) and wide area networks, for example, across town or across the nation. The bandwidth requirements will vary for each link in each network, depending on the amount of C2C messaging traffic using that link, and whether or not the network is shared with other applications. Multiplexers, routers, switches, hubs and other devices are commonly used to manage, segment and optimize computer networks.

The typical subnetwork consists of a local area network adapter that operates at 10 Mbits-per-second (Mbps). In an office environment, even 100 Mbps is readily available (most newly installed office networks use 100 Mbps). Point-to-Point dialup and dedicated external links run at a maximum of 56 Kbits-per-second (Kbps). Most important to a

planner or implementer is that there are plenty of information resources available. In today's business environment, there is usually a person with strong computer skills or network administrator that can help understand and quantify bandwidth and allocations issues.

In a C2C environment, the computers that run the transportation applications are typically just users of the "network" or communication links. Other applications such as e-mail, database management, graphics design and word processing may also be users of the network. This has a big advantage when it comes to design and implementation. A network specialist usually handles its design and implementation. However, they expect the transportation system designer or implementer to be able to quantify what demands will be placed on the network.

NTCIP has adopted two application level protocols for C2C communications. These protocols include, **DAT**a **EX**change in **ASN**.1 (DATEX-ASN, commonly referred to as simply DATEX) and **C**ommon **O**bject **R**equest **B**roker **A**rchitecture (CORBA). Both of these approaches provide the same basic functionality, but they differ in the method of implementation and each has some unique features, refer to Chapter 3. The Internet Protocol (IP) and both UDP and TCP are used at the transport level for both of these C2C communication solutions. Regardless of the application level protocol, C2C communications requires participating systems to exchange standard messages at the information level.

The NTCIP C2C protocols are used for two basic types of message exchange. The first type involves a human operator at a center requesting information on a one-time basis from another center. Since a human is in the loop, the volume of such messages is small, and they are unlikely to be critical in any network design. The other type of messaging occurs when an operator at a center sets up a permanent subscription for data to be sent from another center automatically. There is no human in the loop and messaging is often repeated. Such subscriptions may request the data to be sent every x seconds, or only when it changes. In most cases, network traffic is minimized if subscriptions specify change-based triggers rather than time based. However, the network designer must consider peak loading conditions of the network. Thus, even if change-based triggers are used, the designer should consider the network loading when most or all of the triggers are activated near-simultaneously.

It may be difficult for a system designer to anticipate all the different types of data that may be subscribed for between each pair of centers. It is recommended that designers gather actual operating experience from existing C2C networks to help make such estimates. One important consideration is the frequency of change in status or other data at each center since changes are what other centers will be interested in monitoring. For example, a center that manages only incidents and related information is not likely to generate as much message traffic on the network as one that manages 200 traffic signals each of which changes status every few seconds.

It is possible to perform a worst-case analysis by considering the frequency, or quantity per second, of useful information generation at each center, estimate that other centers will have an interest in receiving that information, and assign the message loads to network links accordingly. Some messages will not require a confirmation or other response message, but many will. These need to be allowed for as well. CORBA also uses various administrative and exchange initiation messages that can add more traffic on the channel. Further allowance needs to be made for retries when a message is not delivered successfully on the first attempt.

For DATEX, each IP packet containing data (a publication message – the most common type) will contain at least 70 bytes of overhead information (including the IP header), plus the actual encoded data. Most messages will contain only a relatively small quantity of actual data – say 20 to 100 bytes. An average DATEX-generated IP packet might contain 150 bytes. At this rate, a full duplex 56 Kbps wide area network link could support in the order of 30 messages per second in each direction. This will be sufficient for some centers, such as the incident management center, but may not be sufficient for others such as the large traffic signal system, or a center that wants to obtain a lot of data from other centers.

THIS PAGE LEFT INTENTIONALLY BLANK

Chapter 6

Implementing NTCIP

6.1 Introduction

This chapter describes the various issues related to implementing the NTCIP in a device or central system. The primary audiences for this chapter are the system/device developers and system implementers. Readers should already be familiar with the concepts presented in Chapters 1-4, especially the concepts related to system design and specification as presented in Chapters 3 and 4.

This chapter is intended to be germane to all of the NTCIP standards. As such, the concepts are presented at a high level. However, one detailed example is given at the end of the chapter in order to explain the concepts more fully.

The reader is warned not to rely on this interpretation of the NTCIP for development purposes. A system or device developer will need to review the relevant NTCIP standards and all available amendments in order to implement them properly. Any questions or interpretation problems should be directed to the NTCIP Working Group that is responsible for developing and maintaining that standard, since only this approach will ensure interchangeability in the long run.

This publication is updated from time to time to reflect changes in NTCIP. To check whether this is the current version of this publication, access the NTCIP home page on the World Wide Web at on www.ntcip.org/.

6.2 Implementation Roadmap

There are certain steps that should be taken in any systems development project. It is especially critical to follow these steps when developing systems that are intended to meet standards. Exhibit 6.1 summarizes some of the more important steps that should be followed by any organization considering the development of NTCIP software.

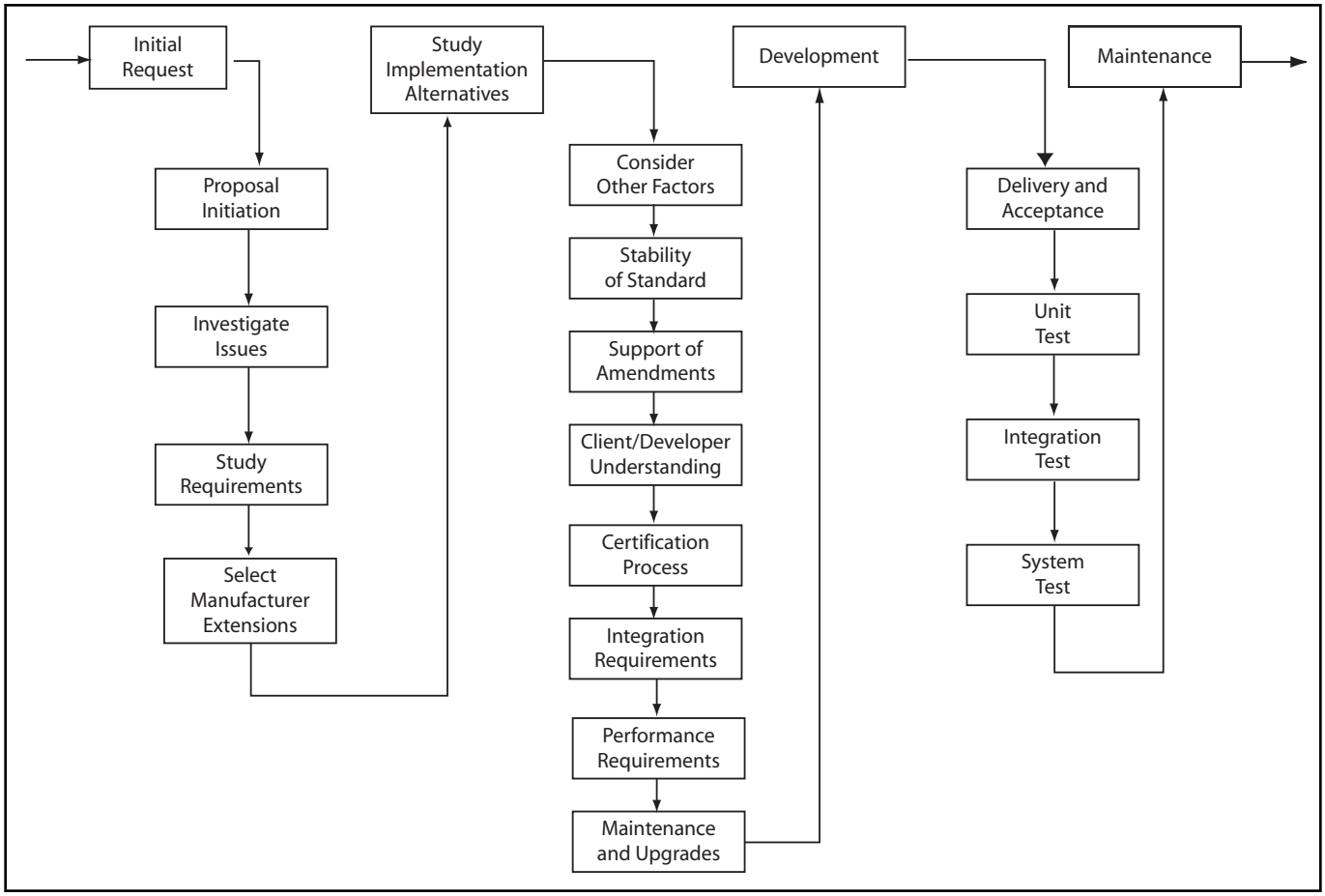


Exhibit 6.1: Roadmap for Implementing NTCIP

6.2.1 Initial Request

An individual or organization (client) initiates software projects by requesting a certain functional capability from a developer. The client and developer may be a part of the same organization or might represent two distinct organizations. For example, a manager may wish to develop an NTCIP device using internal resources in order to be the first NTCIP-conformant device on the market. Alternatively, the request may come from an agency wishing to procure such a device, even though the device is not currently available on the market. In either case, it is wise to perform a full investigation of the issues surrounding the request prior to submitting the proposal.

6.2.2 Investigate Issues

The developer must ensure that there is an adequate understanding of the request. Some requests may be very ambiguous, that is, "The device shall be NTCIP conformant." Others may be very detailed and precise, and some may have precise statements that conflict with each other. The developer must first perform an investigation to ensure a proper understanding of the client's needs. This is then followed by an investigation of how the system may be implemented while recognizing the development risks that may be encountered.

It should be realized that this process works best in an iterative fashion. This allows the client and the developer to work together in developing a list of requirements and a proposal that best matches everyone's needs. However, this is not always possible due to the procurement regulations of some organizations.

Device and/or System Requirements

The first aspect of the investigation should be to determine the exact operational and functional requirements for the system. This will often require expanding the original request. For example, if the request is simply for an "NTCIP-conformant device," the developer must determine what functionality the device is supposed to support, the communications infrastructure that this device is being connected to, and then determine what NTCIP options might be appropriate.

The developer may also need to modify or limit the original request in order to meet safety, schedule, budget, market, or other concerns. For example, the request may be for a signal controller and require "support for the full range of all data elements." However, for safety and liability reasons, the developer may want to develop his software to limit the valid values for the yellow clearance interval to 3.0 to 5.0 seconds. Identifying these variances from the request as early as possible will help keep expectations matching the resulting products capabilities.

The result of this effort should be a detailed requirements document with which both the client and developer are satisfied. Additional details of this investigation are given below. As a minimum, the document should address those issues identified in Chapter 4.

How NTCIP Standards Fit Together

Ideally, there would only be one NTCIP standard that met everyone's needs. However, reality requires a large number of options to meet the unique needs of specific sites. For example, some agencies have a large amount of twisted-pair copper that they want to continue to use. Other agencies are installing new systems and want to take advantage of fiber optic cable and other technologies. Likewise, some agencies have fairly simple data exchange needs with field devices, whereas other centers need to exchange large amounts of information with other centers. The NTCIP accommodates these various needs by providing a suite of standards, each providing unique features.

NTCIP standards are based on a layered approach that is similar to those used by the International Organization for Standardization (ISO) and the Internet community. There are four primary levels of the NTCIP stack:

1. ***Information*** **–** Information Standards define the data to be exchanged and the format of that data.
2. ***Application*** **–** Application Standards (also known as Profiles) 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 equivalent to the Session, Presentation and Application Layers of the ISO seven-layer stack.
3. ***Transport*** **–** Transport Standards (also known as Profiles) define the rules and procedures for exchanging the Application data between point 'A' and point 'X' on a network. This includes any necessary routing, message disassembly/re-assembly and network management functions. This is similar to the rules and procedures used by the telephone company to connect two remotely located phones.
4. ***Subnetwork*** **–** Subnetwork Standards (also known as Profiles) 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.

Any data exchange requires the use of at least one standard taken from each of the four levels. In theory, a profile from one level should be designed such that it can be combined with any profile from another level; however, in practice, profiles will often require certain services from other levels. Thus, only certain combinations are desirable and recognized by the NTCIP effort—other choices are atypical or bad practice, and are therefore mutually exclusive. These combinations are depicted in Exhibit 6.2.

Selecting Standards for an Implementation

The client may inform the developer which standards to use in the request; however, even in this case, the developer must be familiar enough with the standards to ensure that the request is consistent with the intended purpose of the standard. For example, the CORBA standard is not intended for field device communications using the "object definition standards." Another example would be a request for a particular function for which none of the standards have a corresponding data element(s). If a developer receives such a request, he should contact the client to ensure that there is an appropriate understanding of what is required.

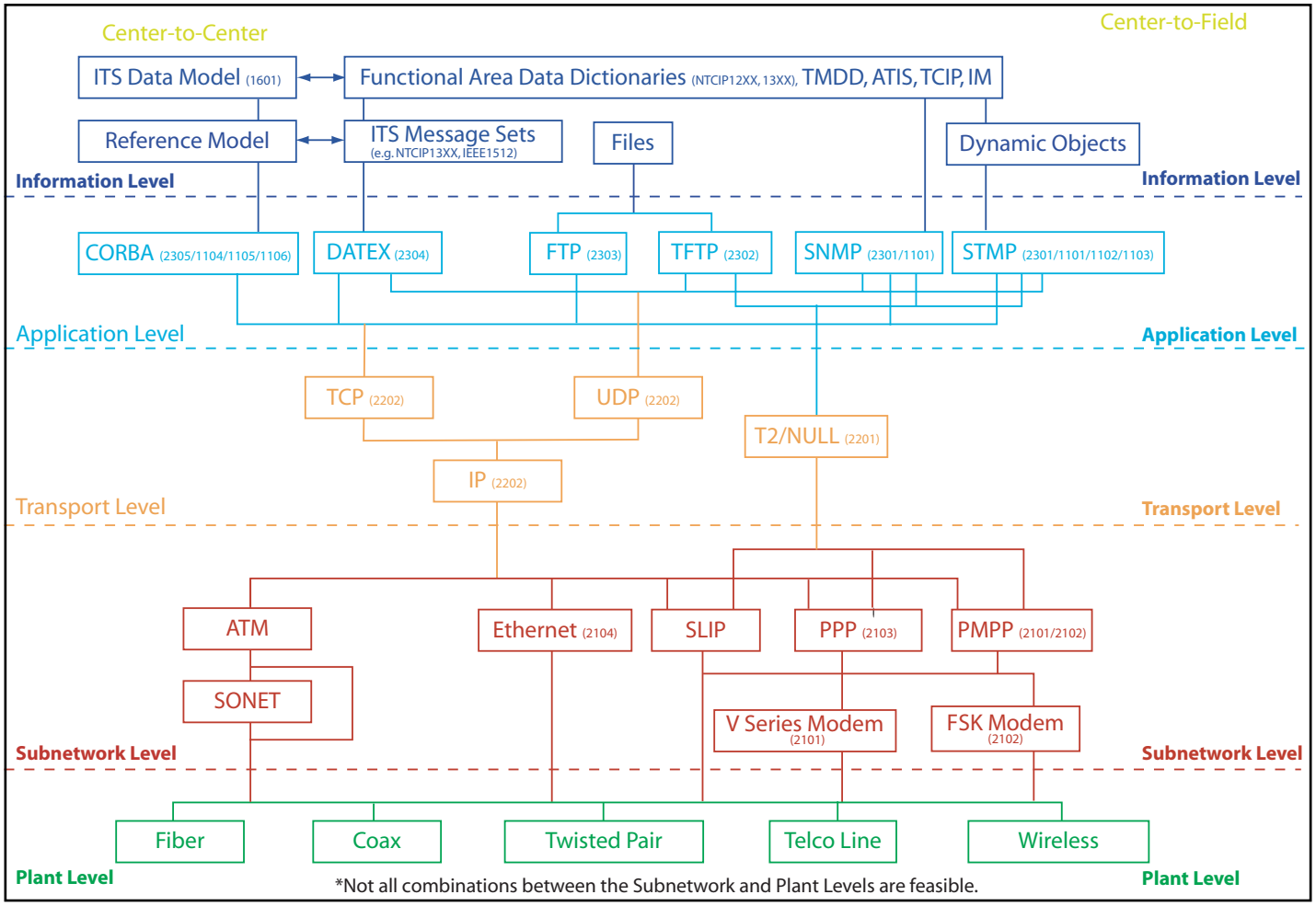


Exhibit 6.2: NTCIP Standards Framework

During this phase of the investigation, the developer should also consider the general market applicability of the selected standards. For example, if the developer believes that the marketplace will seldom request the selected combination, the bulk of the implementation costs will have to be borne by the one client. Thus, it may be appropriate to suggest a more common combination of standards in order to spread the development costs over multiple clients.

Selecting Manufacturer Extensions—Benign or Malignant

Finally, the developer must determine whether the features of the standard support all of the functional features supported by the manufacturer's device. The NTCIP standards and framework have been explicitly designed to allow for innovations to keep pace with advances in technology; it is recognized that the NTCIP standards do not currently define standardized data elements for every technology or functional feature of every device and every technology. The developer must determine if there are special features of the subject device that are not yet standardized by the NTCIP. If such features are present, then the

developer will need to determine precisely how these features will be supported without conflicting with the standardized implementations. (It should be noted that the use of manufacturer specific extensions might tie the agency to a single source of software for all similar devices in the system.)

Usually, this adaptation is accomplished by simply extending the capabilities of existing features of the standard, or by defining additional data elements or features under a developer-specific or agency-specific node for these specific MIB extensions. It is important that the agency be aware of the use of these benign extensions and request that the systems developers or integrators clearly identify these in their proposal.

Another style of extending the standard might be based on complete replacement of a partially incomplete feature with a complete custom feature—this would be considered a malignant extension as it defeats the purpose and goals of any open standardization effort—interoperability and interchangeability. An ITS implementation that uses benign extensions is likely to achieve a level of conformity with known exceptions, for example, the specific extensions are listed. While an ITS implementation that embodies malignant extensions, for example, replacement of the standard's features with custom features, should not achieve conformity as this would mislead customers, and would negatively impact the ability to achieve interoperable and interchangeable ITS.

In any case, if specific benign or malignant extensions have been introduced and the user wants to have the associated functions available in future purchases of the same device type, it is imperative that these extensions are made part of the agency's specifications and documentation deliverables. This necessity also requires that the user agency obtain re-distribution and/or re-use rights to these (MIB) extensions, even if the original manufacturers/vendors/integrators developed and implemented them. Additionally, the agency should obtain both electronic and paper copies of the entire MIB, including the manufacturer-specific extensions. Negotiating the rights for re-distribution and/or re-use, along with documenting the requirements for MIB delivery, is much easier accomplished up front in the procurement process rather than after the fact.

Implementation Alternatives

Once there is a clear understanding of the project requirements, the developer can investigate ways to implement the desired features. For example, the developer may be able to acquire off-the-shelf software to minimize the effort required to implement the features. If this needs to be platform (computer) or operating system, or database specific to be compatible with an existing site infrastructure or support staff capabilities—that needs to be specified in the contract requirements for the implementation. A layered hardware or software system design will minimize the effort required to maintain the code and to implement and introduce different standards in the future. However, these benefits may impose other constraints on the system. A related phenomenon is that over-specification can significantly limit or preclude the expected competitive response environment; thus, agencies should use caution in what they ask for—as they might get exactly that.

The NTCIP has used widely recognized standards whenever possible. For example, the NTCIP standards reference the Transmission Control Protocol (TCP), Internet Protocol (IP), Simple Network Management Protocol (SNMP), Common Object Request Broker Architecture (CORBA) and High Level Data Link Control Protocol (HDLC) standards to name just a few.

In many cases, the private industry has developed off-the-shelf tools to aid system developers in implementing these protocols. Being aware of what products are available off-the-shelf, inherent in an operating system or browser, and their associated cost will allow the agency to set a reasonable expectation, and the developer to provide a more realistic estimate of development costs. For example, most developers use an off-the-shelf implementation of TCP/IP rather than creating their own. Standards for which there are known products include:

- File Transfer Protocol (FTP);
- Trivial File Transfer Protocol (TFTP);
- SNMP;
- CORBA;
- XML
- TCP/IP and UDP/IP;
- Point-to-Point Protocol (PPP); and
- Ethernet;

While off-the-shelf software can save a considerable amount of development time and greatly simplify maintenance of the software, it may not always provide the most efficient implementation. Off-the-shelf software has generally been designed in a very layered fashion for easy maintenance and fully generic use; however, real-time system performance can frequently be improved by violating the strict rules of a truly layered design and by embedding customized optimization code for a specific purpose. The system developer should consider the benefits and detriments of each approach before approving such a development approach and cost estimate.

It should also be recognized that the availability of off-the-shelf tools might affect the selection of features to be included in the requirements document.

Other Factors

There may be a variety of other factors that need to be considered in order to finalize a proposal. Each of these issues may impact the proposed budget, schedule and/or scope. Therefore, they should be explicitly addressed in the proposal in order to manage expectations. Without the management of expectations early in the process, a product, which the developer believes is conformant, may be perceived to be lacking by the client. A sample of these issues is provided below.

Stability of the Standard

The NTCIP standards are still relatively new and all standards are subject to amendments. Amendments typically result from developers attempting to implement the subject standard and recognize either a technical inconsistency or completeness problem, with the specification or ambiguous wording. Thus, new standards are frequently amended to solve these problems and the standards become more stable over time. Thus, from a developer's perspective, there is greater risk in implementing new standards. Typically, the first manufacturers to implement are the manufacturers who establish the greatest market share. Thus, these trade-offs must be considered in any implementation.

Support of Amendments

Because the standards are relatively new, the developer must consider what will happen if an amendment to the standard is approved during the development period of the product. As a general rule, it may be difficult to support amendments that are made after the product design is finalized and coding has begun. However, many times, a draft amendment may be present during design and the issues identified in the draft can be incorporated. In any case, the proposal should explicitly state whether or not amendments will be included for the proposed price and whether or not there is a cut-off date for such amendments. However, it is anticipated that once there are successful faithful implementations of the complete standard that few amendments will be needed.

Interpretation Resolution

When implementing relatively new standards, a developer should ensure that there is a clear understanding of how interpretation problems will be addressed. For example, one could propose that any interpretation conformant with the wording is valid for acceptance. This would minimize the risk undertaken by the developer, but may not result in a product that is interoperable with other "standard" devices. Another approach would be to have the respective NTCIP Working Group provide an interpretation of the standard; this would increase the risk assumed by the developer, but would also increase the probability for interoperability.

Client/Developer Understanding

Another factor to consider is whether the client has realistic expectations. While the NTCIP provides a standardized interface that is flexible enough to meet various needs, it will most likely be more bandwidth intensive than the client's existing systems and/or it may use a slightly different database design. It is important to make sure that the client has realistic expectations at the start of the project in order to ensure that the project will be perceived as a success. A thorough understanding of the expectations on the part of both the client and developer is important to the success of any project.

Conformance and Certification Process

The developer must also consider the certification process for the product. While a rigid certification process will undoubtedly provide a greater assurance to the client, it will also increase costs. These costs are especially important to consider if the developer is responsible for any testing costs, for example, through hiring an independent lab. Additionally, both the client and the developer need to understand that the certification of a product is typically valid for a particular communications stack (such as, SNMP over T2/NULL over PMPP). This means that the certification is not valid for another communications stack (such as, if the requirement is to provide routable dial-up, which would require SNMP over TCP/UDP/IP over PPP).

Currently, the overall ITS Standards Development effort is determining the spectrum of user testing needs, then what support is needed for testing, testing tools, conformity assessment, certification, and user testing. It is likely that the standards, especially the NTCIP standards, will be amended to include suggested test cases and procedures in a normative annex to the standard, for example, helpful but not required. These anticipated test cases will be independent of the implementations that eventually embody the standard, for example, independent of the keystrokes, mouse clicks that operators will use; but, they will be easily reusable in constructing the project-specific test procedures for implementations that eventually use the standard.

Integration with Other Components

The developer may also be required to ensure that his device works with other components within a larger system. Such integration may reveal problems that do not appear during product certification and thus may also affect the project costs.

Performance Issues

The developer should also realize that the flexibility of NTCIP also comes at the price of a more complex system than what the industry has traditionally used. Therefore, the system may require more sophisticated processors or better communication facilities than traditional systems in order to achieve the same performance level, for example, response times. If the developer overlooks these issues at the design time, there could be significant costs imposed at the end of the project in order to provide the necessary performance. The client should also be informed of performance trade-offs.

Maintenance/Future Upgrades

A final issue to consider is whether the client desires extended maintenance or future upgrades. Such services may be appropriate given that the standards may change based on other deployment projects; but clearly such a service will increase the costs associated with the project.

6.2.3 Development

If the proposal is accepted, the development phase will begin. This will include finalizing the development approach, building the prototypes and internally testing the units.

6.2.4 Delivery/Acceptance Testing

Once the developer is satisfied with the quality of the implementation, it is ready for delivery to the client. At this point, the client will perform an acceptance test. The type of acceptance test should be specified in the proposal process as this may affect the cost of the delivered product. It should be realized that the NTCIP is a very complex set of standards and it is impractical to perform completely comprehensive testing. However, well-designed test plans can be produced to provide a high level of confidence for a reasonable cost. Examples of test procedures that provide detailed steps to perform testing have been prepared for the ENTERPRISE Program (on www.enterprise.prog.org/) and are available free-of-charge on the Internet. Test procedures are available for the following NTCIP standards (and their amendments up to November 2001):

- NTCIP 1201 Global Object Definitions
- NTCIP 1203 Dynamic Message Sign (DMS)
- NTCIP 1204 Environmental Sensor Stations (ESS)
- NTCIP 2301 Simple Transportation Management Framework (STMF)
- NTCIP 2102 Point-to-Multi-Point Protocol over EIA/TIA-232
- NTCIP 2103 Point-to-Point Protocol (referred to as dial-up)
- NTCIP 2001 Class B Profile (which is being replaced; however, the test procedures does not address all the new features defined in NTCIP 2201, which is the reason why 2201 is not listed).

In general, there are three levels of testing: (1) unit testing, (2) integration testing and (3) system testing. Agencies might also require and specify "Burn-In" testing to identify and reduce the risk of infant-mortality failures, and/or "Stress Testing" to operate the system at capacity to identify any peculiarities or affects on operational performance or functional capability. If needed, burn-in test can be associated as a subset of (2) integration test, and stress test can be associated as a subset of (3) system test.

Unit Testing

The focus of unit testing is on a comparison of an implementation against the standard. This may be performed by inspecting the code or with the use of "proven" software to send test messages to the device. This process should be formalized by documenting a specific test procedure that will be followed. During the test, the result of each step of the procedure

should be recorded. A test should result in a completed PICS statement that confirms the accuracy of the PICS included in the procurement documents. Each NTCIP standard includes, or will include in amendments or newer versions, a PICS statement in Annex A of that standard. For any particular implementation, four (4) PICS statements are required:

- One for the device-specific data dictionary (Information Level),
- One for the selected Application Level protocol,
- One for the selected Transport Level protocol, and
- One for the selected Subnetwork Level protocol.

Unit testing provides a basic level of validation and verification that a product is conformant to a standard. Many times, the test plan will be designed such that the failure of one procedure will provide a clear indication of what problem resides within the implementation, thereby minimizing the cost of finding and fixing the error or "bug." A device that fails such a test plan would almost certainly not be able to interoperate or be interchangeable with other systems. A device that passes such a test has less risk, and a reasonable probability of interoperating and interchanging with others. However, any performance issues encountered during unit testing must also be considered and weighed against overall operational system requirements.

Integration Testing

Integration testing consists of connecting two or more devices together and having them exchange data (typically performed in a laboratory/test environment). Assuming the individual devices have previously passed a sufficiently designed unit test plan and the two devices support the same features and communications protocols, the devices should integrate together fairly easily. Examples include two different interpretations of a specific requirement (typically a problem of newer standards) and problems related to system timing between the two implementations.

In theory, the unit test should be thorough enough to prevent any problems in integration testing. However, the integration testing phase provides a higher level of confidence that the system devices and subsystem components will interoperate and that nothing has been overlooked.

If burn-in testing is desired, it can begin and continue concurrently with integration testing. A general rule-of-thumb for burn-in testing criteria might be that all devices or subsystem components must survive the first 30-60 days of testing and/or operational use. Further, the agency may specify that any failures that occur during that period will be declared as "infant-mortality" and must be repaired/replaced by the provider or manufacturer.

System Testing

A final level of testing is system testing. At this level, each device on the system is integrated together to form the final complete and operational system. This level of testing should identify and global problems with the new systems as well as any issues with legacy systems, site infrastructure, power, and signal.

Agencies should note that there could be great similarity or great diversity in the conditions of integration testing versus system testing. The latter, systems testing, must be done in the actual site operational environment. This introduces nuances of the site's quality of service for power and signal telecommunications, which can have a significant negative affect on the system. This may also be the first time that the real operations staff have been able to have hands-on the system—do they discover system anomalies or training issues? The same would be true for agency maintenance staff—is everything all right with them as far as system problem identification, diagnosis and troubleshooting tools? On the other hand, integration testing is very likely to begin in the factory, then continue and conclude on site. The in-factory phase is appropriate to minimize the introduction of site-specific issues when ironing out that last few remaining "bugs" as the system components are integrated for the first time. It is suggested that agencies should require that final integration testing must be completed on site prior to the start of system testing.

Once again, in theory, devices that successfully pass unit testing and integration testing should pass this system level testing as well, given that the system was properly designed. However, the final check is only provided when this system test is performed and any problems that arise at this stage are corrected.

It may also be desirable to include a stress test as part of system testing. A stress test attempts to operate the ITS devices and/or component subsystems at their maximum capacities to determine if there are any remaining insidious interactions that affect operational performance or functionality. It may, or may not be possible to operate the system at maximum capacity, for example, will the drivers cooperate? An alternative may be available through simulated stimulation of the system, for example, insertion of maximum traffic counts from the field. While it may be suspect, a well-designed simulation for stress testing can reduce risks and provide assurances that there are no remaining performance "bugs" in the system.

6.2.5 Maintenance

Both the developer and the agency should also be aware of any requirements for maintenance and upgrades, as these will affect the overall costs of the project. In general, it should be recognized that the NTCIP standards are still relatively new and thus changes may occur to the standards. Further, as there are relatively few implementations available,

ambiguities may still be discovered in the standard and the standards may be modified in order to correct these problems. Any such change may require a modification to deployed equipment if the equipment is to maintain compatibility with the new version of the standard.

6.3 Example Implementation Process

This section provides an example of the various decisions that must be made during an implementation project. The following example represents a procedure that a manufacturer or developer might use to develop an NTCIP-conformant device. In this case, the device is a dynamic message sign.

6.3.1 The Request

For the purposes of this example, we will assume that the client has issued a Procurement Invitation for a dynamic message sign and controller (DMS) containing the following statements:

A. The DMS shall be a full matrix capable of displaying three lines of text with 20 characters per line when 18-inch characters are utilized. The full matrix display shall be capable of displaying other size characters and other number of lines depending on the height of characters utilized. The sign shall be designed to provide 2 pixels of spacing between lines of text when displaying the characters and lines of text as indicated herein.

B. The DMS shall be provided with a temperature sensor to monitor the interior temperature of the sign.

C. The DMS shall be capable of the following types of displays.

1. Signs shall be able to display each line as either static or flashing, as described below.

   a. **Static Message** - The line shall be displayed constantly on the sign face until the sign controller is instructed to do otherwise.

   b. **Flashing Message** - A selected line shall be displayed and blanked alternately at durations separately controllable in 0.5-second increments.

2. The DMS shall be capable of displaying up to three different pages (each page consisting of up to three lines of text) alternately at duration's separately controllable in 0.5-second increments.

3. The sign shall be able to display text as centered, right justified, or left justified.

4. The sign shall be able to display a message in a specific font, for example, single-stroke or double stroke.

5. In the event of communication errors or controller lock-ups, the sign shall retain the current message. In the event of a power failure, sign shall display the current message upon restoration of power.

D. The DMS shall display a message composed of any combination of the following characters and shapes:

1. "A" through "Z"- All upper case letters.

2. "0" through "9"- All decimal digits.

3. A blank or space.

4. Punctuation marks shown in brackets [.,!? -:; " '/( )]

5. Special characters shown in brackets [# & * + < >]

6. Graphic displays

E. All communications between the DMS and central computer shall be NTCIP-conformant in one of the following modes, which shall be user selectable:

1. *Polled Operation* in which the sign controller informs the central computer of its current status in response to a query from the central computer; or;

2. *Event-Driven Operation* in which the sign controller not only responds to queries from the central computer but also calls the central computer by telephone whenever it detects: restoration of AC power at the sign controller and/or internal DMS temperature exceeds programmed safety limit. If the line is busy, it shall retry the call at an interval that can be selected by the operator until it connects with the central computer.

F. The DMS shall contain a computer-readable time-of-year clock with a lithium battery backup. The battery shall keep the clock operating properly for at least 10 years without external power. The clock shall automatically adjust for daylight saving time and leap year through hardware or software or a combination of both. It shall be set by the sign controller's microprocessor. The clock shall be accurate to within 1 minute per month.

G. The DMS shall be provided with an eight-character (minimum) password, for access to sign controller.

H. In the absence of instructions to the contrary from the remote control port, the DMS shall implement a display selected from those stored in its memory based upon date and time as specified in the schedule.

I. The DMS shall incorporate fail-safe procedures to check messages received and shall not change a message stored in memory, the display currently on the sign,

the schedule stored in memory, or the current time unless the message is received correctly.

J. The DMS shall associate a priority level with each message. Only if the priority status is higher than the status of the message that it is to replace, the new message shall be posted.

K. The DMS shall include a system that senses the background ambient light level and provide a minimum of sixteen field adjustable intensities (dimming).

L. An 8-byte ID code shall be assignable to each DMS.

The agency should also provide completed PICS(s).

6.3.2 The Investigation

While the above request provides a fair amount of detail as to the required functionality of the sign, the information is not presented in a format that directly relates to NTCIP requirements and there are several issues on which the request is silent. The first task of the investigation is to determine exactly what the requirements are and to then investigate the other related issues. The discussion presented here only focuses on the NTCIP issues; however, a real investigation would clearly have to investigate hardware issues as well.

Requirements

The first task is to provide an interpretation of each requirement of the request. In this case, there is a fair description of the desired functionality, thus, this task is a matter of mapping the functions to specific NTCIP features. In other cases, the developer may have to work more closely with the client to develop the functional requirements. Once the initial interpretation is performed, the developer may have a list of questions for the client.

Interpretation

The list below interprets the above requirements into specific NTCIP requirements. Normal text indicates the original statement. Text in italics indicates the NTCIP interpretation. Text in bold indicates significant statements that may impact costs and/or may impact the user's expectations.

A. The DMS shall be a full matrix capable of displaying three lines of text with 20 characters per line when 18-inch characters are utilized. The full matrix display shall be capable of displaying other size characters and other number of lines depending on the height of characters utilized. The sign shall be designed to provide 2 pixels of spacing between lines of text when displaying the characters and lines of text as indicated herein. *The DMS shall be a full matrix display consisting of 120 pixels wide by 27 pixels high. Pixels shall be evenly spaced both vertically and horizontally. A 5 x 7 pixel matrix shall form a standard fixed width 18" high character.* **The DMS shall support at least two fonts (single-stroke**

and double-stroke as required in Clause C-4), as defined by the NTCIP Font Conformance Group.

B. The DMS shall be provided with a temperature sensor to monitor the interior temperature of the sign. *The Temperature Status Conformance Group shall be supported to monitor the interior temperature of the sign.* ***This shall be achieved by two additional sensors: one to monitor the ambient temperature and the other to monitor controller cabinet temperature.***

C. The DMS shall be capable of the following types of displays.

1. Signs shall be able to display each line as either static or flashing, as described below. *The flashing of a displayed line shall be achieved through the use of the'*fl*' MULTI Tag.*

   a. **Static Message** - The line shall be displayed constantly on the sign face until the sign controller is instructed to do otherwise.

   b. **Flashing Message** - A selected line shall be displayed and blanked alternately at durations separately controllable in 0.5-second increments.

2. The DMS shall be capable of displaying up to three different pages (each page consisting of up to three lines of text) alternately at duration's separately controllable in 0.5-second increments. *The display of up to 3 different pages shall be achieved through the use of the'*np*' MULTI tag, the page display duration shall be achieved through the use of the'*pt*' MULTI Tags.*

3. The sign shall be able to display text as centered, right justified, or left justified. *The capability to position the text shall be achieved through the use of the'*jl*' MULTI Tag; the following values shall be supported as a minimum: 2, 3, and 4.*

4. The sign shall be able to display a message in a specific font, for example, single-stroke or double stroke. *This shall be achieved through the use of the'*fo*' MULTI Tag.*

5. In the event of communication errors or controller lock-ups, the sign shall retain the current message. In the event of a power failure, sign shall display the current message upon restoration of power. *This shall be achieved by storing the currentBuffer row of the message table in non-volatile memory and configuring the appropriate Default Message data elements (dmsCommunicationsLossMessage, dmsPowerLossMessage) to point to the currentBuffer. Displaying a particular message after a 'controller lock-up' is not covered in the NTCIP 1203 standard.*

D. The DMS shall display a message composed of any combination of the following characters and shapes: *These shall be stored in the default fonts as their respective ASCII character codes. Other character codes can be used for graphics. There shall also be one font reserved for graphics* ***(however, graphics are not currently standardized by the NTCIP 1203 standard).*** *Alternatively, a manufacturer specific graphic capability can be provided.*

1. "A" through "Z"- All upper case letters.
2. "0" through "9"- All decimal digits.
3. A blank or space.
4. Punctuation marks shown in brackets [.,!? -:; " '/( )]
5. Special characters shown in brackets [# & * + < >]
6. Graphic displays

E. The DMS shall permit the communication with an NTCIP-conformant central computer in either of the following modes which shall be user selectable:

1. *Polled Operation* in which the sign controller informs the central computer of its current status in response to a query from the central computer; or;
2. *Event-Driven Operation* in which the sign controller not only responds to queries from the central computer but also calls the central computer by telephone whenever it detects: restoration of AC power at the sign controller and/or internal DMS temperature exceeds programmed safety limit. If the line is busy, it shall retry the call at an interval that can be selected by the operator until it connects with the central computer.

Note: *Since the provided requirements do not unambiguously identify the type of communications between the central computer and the DMS sign controller, the developer has to work with the client to determine the appropriate communications plant. The Event-Drive Operation' description points, however, to dial-up communications. Let's assume that dial-up is the selected type of communications. Next, the developer needs to determine whether a routable Transport Level protocol is to be used. Let's also assume that this is the desired setup. Lastly, the developer needs to determine whether both SNMP and STMP need to be supported as the Applications Level protocols. Let's assume that only SNMP is desired. We would then end up with the following NTCIP wording: The DMS shall provide, as a minimum, support for the PPP Subnetwork Profile (i.e., Dial-up Modem, PPP), the Internet Transport Profile (i.e., UDP/IP), Conformance Level 1 of the STMF Application Profile (i.e., SNMP), and the DMS Information Profile (as defined in Sections 4 and 5 of NTCIP 1203 and Section 3 of NTCIP 1201). The Event-Driven Operations shall be achieved via the following operation: the DMS controller calls the central computer and, once the dial-up connection is established, the DMS controller shall 'hand over' control of the communications line to the central computer. The notification of alarm conditions*

(here, the excess of temperature thresholds and the restoration of AC power) shall be achieved via manufacturer-specific traps. Both, temperature safety limit notification and the AC power restoration notification are not standardized in NTCIP standards and the developer shall propose appropriate data elements. These data elements shall be fully documented for approval by the ENGINEER. Additionally, the developer shall make these new data elements available to the AGENCY without restrictions for future use—(this is an important point that should be reviewed with the agency prior to contract signing).

F. The DMS shall contain a computer-readable time-of-year clock with a lithium battery backup. The battery shall keep the clock operating properly for at least 10 years without external power. The clock shall automatically adjust for daylight saving time and leap year through hardware or software or a combination of both. It shall be set by the sign controller's microprocessor. The clock shall be accurate to within 1 minute per month. *The sign shall support the globalTime, globalTimeDifferential, and globalDaylightSavings parameters. Future modifications to this setup shall be provided free of charge within 4 months of publication of these modifications within an amendment or new version.*

G. The DMS shall be provided with an eight-character (minimum) password, for access to sign controller. *The DMS shall support the security (community name) data elements as defined originally in the amendment to NTCIP 1201 (which have since been moved to NTCIP 1103). This password will also be required when accessing the controller locally.*

H. In the absence of instructions to the contrary from the remote control port, the DMS shall implement a display selected from those stored in its memory based upon date and time as specified in the schedule. *The DMS shall support the Timebase Event Schedule conformance group from NTCIP 1201 and the Scheduling conformance group from NTCIP 1203.*

I. The DMS shall incorporate fail-safe procedures to check messages received and shall not change a message stored in memory, the display currently on the sign, the schedule stored in memory, or the current time unless the message is received correctly. *The DMS shall provide this feature by using the CRC-16 algorithm of PPP.*

J. The DMS shall associate a priority level with each message. Only if the priority status is higher than the status of the message that it is to replace, the new message shall be posted. *The DMS shall use the run-time and activation priorities as identified in NTCIP 1203.*

K. The DMS shall include a system that senses the background ambient light level and provide a minimum of sixteen field adjustable intensities (dimming). *The DMS shall support the Illumination and Brightness control conformance group.*

L. An 8-byte ID code shall be assignable to each DMS. *Each DMS will be associated with an IPv6 address in addition to the IPv4 address and physical address that it must support in order to be conformant to the selected NTCIP communications protocol standards (NTCIP 2202 [Transport Profile] and NTCIP 2103 [Subnetwork Profile]).*

The developer should also verify the agency PICS(s) from the procurement documents.

Questions Arising from Requirements Review

During the above analysis, there were three significant issues that should ideally be clarified prior to providing a bid estimate. However, in some cases it may not be possible to ask such questions. In these cases, the developer may wish to prepare a bid that documents other options.

The three questions that arose from this analysis are:

1. How many fonts must the sign support?
2. Should graphics be handled as a font or as a manufacturer specific feature?
3. Is support for subnetworks other than PPP required?

A second iteration through this process would include questions arising from the text below, namely:

1. How will the sign be tested to ensure conformance?
2. Who is going to supply the central software?
3. Are there any other devices in the system?
4. What are the performance requirements of the system?
5. Is the developer expected to provide maintenance of the software and/or upgrade the software if the standards change? If so, until what date?
6. How many messages must the sign support and of what type?

Implementation Alternatives

Once the initial requirements are known, the developer can determine the best approach to developing the system. This approach will then allow the developer to start estimating the costs associated with the project.

Products are readily available from multiple manufacturers for a standard implementation of SNMP, UDP/IP and PPP. In this case, the developer would likely choose to use a great deal of off-the-shelf software. This would allow the developer to focus on the actual functionality of the data elements rather than spending a large amount of time on the protocols.

Other Factors

As mentioned above, there are a variety of other factors to consider as well. The following text describes how these factors might affect the example project.

Stability of the Standard

In this case, the developer will have to implement the following standards:

- ***PPP Subnetwork Profile***, which includes
  - ❖ AT Command Set
  - ❖ HDLC-like framing
  - ❖ PPP
  - ❖ LCP
  - ❖ CHAP
- ***Internet Transport Profile***, which includes

UDP (however, most off-the-shelf software would also provide TCP)

  - ❖ IP
- ***STMF Application Profile***, which includes
  - ❖ SNMP
  - ❖ BER
- ***Global Object Definitions*** plus amendment(s) or new version
- ***Object Definitions for Dynamic Message Signs*** plus amendment(s) or new version

These standards are somewhat stable, but could change to some degree. The communications standards referenced by these protocols are widely deployed and are very stable.

Support of Amendments

Given this design, the developer would probably want to state that the project will use off-the-shelf software for the protocols and will be conformant with the current version of the Profiles. Given the stability of these base standards, this design should be fully compatible with the final version of the Profile documents. If, however, amendments are made to the profiles that are not compatible to the traditional use of the base standards, additional costs may be incurred.

The developer would need to develop the software for the data elements internally. As such, the developer would probably indicate that he will support all defined features and all approved amendments up to a certain date (perhaps six months after award). If an amendment is approved after this date, additional costs may be incurred.

Interpretation Resolution

In this case, the developer would probably want protocol issues to be resolved by the Internet community and data element definitions to be resolved by the NTCIP community. Thus, the proposal should include a statement indicating that the relevant working group shall be contacted to provide any necessary clarification of the standard. If the resolution is simply a clarification and does not require a normative change to the standard, the decision of the working group should be implemented. If the decision results in an effort to amend the standard and the amendment is not approved by the indicated date; the client and developer will negotiate what the appropriate solution might be and how that solution might impact the schedule and budget of the project.

Client/Developer Understanding

Given the initial set of requirements provided by the client, it is likely that the client is only aware of the NTCIP and is unfamiliar with the details. Thus, the developer should budget resources during the project to ensure that he is able to properly manage expectations. This may include a meeting during the initial stages of the project to clearly present the features of the end product and how this may be different than what the client expects.

The client on the other hand should include statements in the procurement documents requiring the developer to provide detailed and meaningful descriptions for any new data elements and protocol deviations. Additionally, the client needs to include statements to the effect that they can use these new data elements and descriptions and other deviations as seen appropriate including, but not limited to, passing these on to other developers for integration purposes and subsequent bids (update of procurement documentation).

Conformity Assessment and Certification Process

The initial requirements did not indicate any conformity assessment or certification process requirements. However, it is likely in the developer's best interest to indicate what sort of conformance testing would be appropriate and how it is intended that certification will be achieved, for example, 1st, 2nd, or 3rd-Party, if that is desirable. Refer to the discussion in Chapter 2 for additional information. In the case of this project, the proposal might suggest that the developer also prepare a 1st or 2nd-Party conformity assessment test plan, to be approved by the client, and that these tests will be performed in front of the client. The completed conformity assessment test will result in, at least, four completed PICS statements using copies of the PICS statements as provided in the updated NTCIP standards.

Integration with Other Components

The initial requirements did not indicate whether this sign would be integrated with other components, but one would assume that a management station would be used. Thus, the developer may wish to suggest that the procurement will include a central system to control the sign and maintenance software to perform diagnostics on the sign.

Performance Issues

The original specification did not include any requirement for performance. The developer may want to provide a statement in the proposal that the sign will produce a response to a '`GET globalTime`' request within one second and a '`SET dmsActiveMessage`' request within two seconds (measured from last byte in to first byte out). However, ideally, the client should specify the performance requirements [this can be an important issue for traffic signal systems]. When a system cannot meet the stated performance requirements, the developer must highlight the issue and seek to resolve it with the client.

Maintenance/Upgrades

The initial requirements are silent as to maintenance and upgrades. The developer may decide to minimize risks and not include any such features in the proposal, or may decide that the product will have to be maintained for other clients anyway and thus include the estimate in the proposal. In the latter case, the developer would likely want to encourage the client to include maintenance and upgrades in the requirements for the bid by asking a question to that effect.

6.3.3 Proposal

Once all of these issues are resolved, the developer is able to prepare a proposal. For this example, the following text may be included in the proposal.

Display Requirements

The DMS display will be full matrix and contain 120 pixels wide by 27 pixels high. The pixels will be evenly spaced both horizontally and vertically.

The display will be configurable to support different size fonts and the number of lines supported will be determined based on the selected font. When displaying a 5x7 font, a character shall be 18" high and the sign will display 3 lines, each separated by two pixels, with 20 characters per line, each separated by one pixel.

The sign will be equipped with three temperature sensors: one for the interior of the sign, one for the interior of the cabinet and one for the ambient air temperature.

An internal clock will be provided to support the globalTime data element. It shall have a lithium battery backup, which will last a minimum of ten years. The controller shall adjust for daylight savings (according to the NTCIP mechanisms) and leap years. The clock will be accurate to within one minute per month.

The sign will include a system of light sensors and adjust the illumination/brightness according to the mechanisms defined in NTCIP 1203.

NTCIP Functional Requirements

The DMS will support the following NTCIP conformance groups.

- Configuration, as defined in NTCIP 1203 and Amendment 1
- Time Management, as defined in NTCIP 1201 and Amendment 1
- Timebase Event Schedule, as defined in NTCIP 1201 and Amendment 1
- Security, as defined in NTCIP 1201 Amendment 1 (or NTCIP 1103)
- Sign Configuration, as defined in NTCIP 1203 and Amendment 1
- Font Configuration, as defined in NTCIP 1203 and Amendment 1
- Message Table, as defined in NTCIP 1203and Amendment 1
- Sign Control, as defined in NTCIP 1203 and Amendment 1
- Default Message Control, as defined in NTCIP 1203 and Amendment 1
- MULTI Error Control, as defined in NTCIP 1203
- Illumination/Brightness Control, as defined in NTCIP 1203 and Amendment 1
- Scheduling, as defined in NTCIP 1203 and Amendment 1
- Status Error, as defined in NTCIP 1203and Amendment 1
- Temperature Status, as defined in NTCIP 1203 and Amendment 1

In addition, the sign will support the following data elements, as defined in NTCIP 1203 and Amendment 1:

- *defaultFlashOn*
- *defaultFlashOff*
- *defaultFont*
- *defaultJustificationLine*
- *defaultPageOnTime*
- *defaultPageOffTime*

The full range of each data element will be supported, except as noted in Exhibit 6.3.

Exhibit 6.3: Range Values Supported

Data Element	Values Supported
NTCIP 1203 and Amendment 1	
Max Time Base Schedule Entries	7
Max Day Plans	7
Max Day Plan Events	7
NTCIP 1203 and Amendment 1	
Number Fonts	5
Max Font Characters	127
Default Background Color	0
Default Foreground Color	9
Default Justification Line	2, 3, 4
DMS Num. Permanent Msg	0
DMS Max. Changeable Msg	21
DMS Max. Volatile Msg	0
Non-Volatile Memory	5 KB
DMS Control Mode	2, 4 and 5
Number Action Table Entries	15

The current buffer of the message table will be stored in non-volatile memory. This will enable the controller to redisplay the last message after a power outage, if so selected by the dmsShortPowerRecoveryMessage and/or dmsLongPowerRecoveryMessage.

In addition, the sign shall support the following manufacturer-specific data elements:

- Maximum Allowed Sign Housing Temperature
- Sign Housing Temperature Exceeded Trap
- AC Power Recovery Trap
- IP v6 Address

The software shall implement the following tags (opening and closing where defined) of MULTI as defined in NTCIP 1203 and Amendment 1.

- Flash ('fl')
- Font ('fo')
- Justification Line ('jl')
- New Line ('nl')

- New Page ('np')
- Page Time ('pt')

NTCIP Protocol Requirements

The sign will comply with the minimum requirements of the PPP Subnetwork Profile (NTCIP 2103). The sign will also comply with the minimum requirements of the Internet Transport Profile (NTCIP 2202). Finally, the sign will comply with the Conformance Level 1 and other minimum requirements of the STMF Application Profile (NTCIP 2301). Exhibit 6.4 depicts the protocols that will be supported.

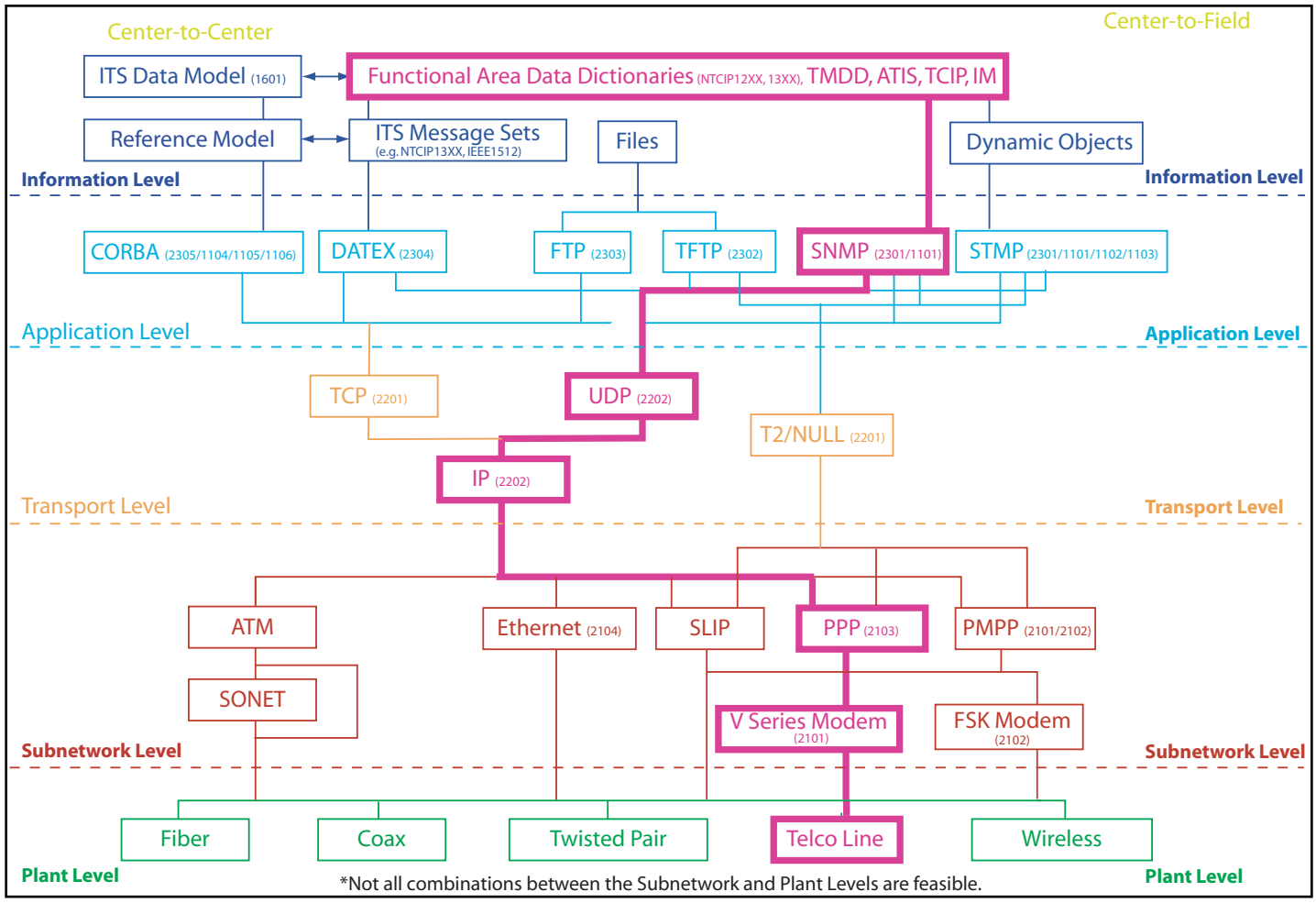


Exhibit 6.4: Example Center-to-Field Stack

Initial Configuration

The controller will be shipped with a four standard font sets: an 18" (5x7) single stroke, an 18" double stroke as required, and a 13" (3 or 4 x5) single stroke, and a 36" double stroke. The stored characters will include all of the upper case letters (A-Z), digits (0-9), a blank, and the following marks: [.,!? -:;“ '/( ) # & * + < > $]. All characters will be stored according to their ASCII character codes. The character entries for all other ASCII character codes will be left empty for the user to define. A fifth font provided will contain a sampling of common graphics.

Acceptance

A test plan will be provided to the client for approval. Upon delivery of the sign, the test plan will be performed in the presence of the client to demonstrate conformance to the standard. Four completed PICS statements will be provided that demonstrate the sign has passed conformance testing for:

- Global Object Definitions and DMS Object Definitions (Information Profile)
- SNMP (Application Profile)
- UDP/IP (Transport Profile)
- PPP (Subnetwork Profile)

Maintenance/Upgrades

This contract does not include maintenance or upgrade support.

6.4 Example Byte Streams

This section will provide the reader with a basic understanding of how the NTCIP works in a C2F environment.

6.4.1 The NTCIP Database

Transportation devices need to store and communicate constants, parameters and collected data. Examples include minimum cycle time for a traffic signal, text for a dynamic message sign, vehicles per hour for a count station and current wind speed from a weather station.

NTCIP is intended for many types of transportation devices, each with different database requirements. NTCIP relies on the SNMP approach to database management. SNMP uses an industry-standard GET/SET paradigm to read and write data into a database. Data elements in the database are called “managed objects” or just “objects” for short. The database is a group of related data elements and is called a “management information base” or MIB. The entity that manages the MIB within a device is called an agent. The concept is that a management application sends messages to the agent to fetch or modify the values of

data elements stored within the MIB. When MIB values change, the transportation device responds as defined in its programming. The agent works at the application layer in the protocol, but is itself not the application. The agent does not care whether the MIB represents a traffic controller or dynamic message sign or any other device.

STMP works in the same way as SNMP and uses the same data elements. STMP simply provides a more bandwidth efficient, but more processor intensive, solution to the same problem.

A data element is a type of data. Within an agent, one or more instances of the data element may exist. Different instances are identified by their index, as discussed below. A data element instance must be transported as a whole. As an example, a data element may define the current time, say 12:15:30. Since this data element is defined as hours, minutes and seconds, it cannot be used to transport just seconds. Alternatively, time could be defined as three separate data elements, one each for hours, minutes and seconds; in this case, a request could deal with any one of the three data elements or simultaneously access all three. A third alternative would be to define both of these representations of time (for a total of four data elements). It may be convenient to have access to different forms of the same data in the same MIB but it is not very efficient, since extra data elements require more computer memory. Thus, when designing data elements, the designer must consider the trade-offs of each approach. Additionally, one needs to consider that NTCIP only addresses the transport of this data not its presentation to the user; that is, while time could be sent in 3 data elements, it could be presented to the user in the 12:15:30 format.

To standardize some of the commonly needed data elements, the NTCIP defines a global data element's MIB module. The global MIB module contains definitions of commonly needed data elements that are basic to the NTCIP, such as the name and versions of the MIBs supported by an agent, the representation of time, logging of events, or the definition of a scheduler.

A MIB and its data elements are defined using Abstract Syntax Notation One (ASN.1). "Abstract syntax" means that the manner used to define the data is independent of the procedure for encoding the data into binary form. The MIB is a text document that can be read by a human and compiled by computer. A management application must have a copy of the MIB employed by the managed agent. The MIB is transferred to a management application via a text file on a floppy disk. This is usually performed when the device is first installed. However, other methods could be used for MIB transfer. However, it is possible that the management application does not have a complete copy of the MIB employed by the managed agent. This scenario would limit the possible data exchange between management application and the agent to the data elements supported within the management application, which is sometimes desired when the field device includes many features not (currently) used by the management application and when expensive software modifications to the management application are to be avoided.

Example 6.1:

Consider the example above where the device includes a clock. The management application will need to set the clock periodically to ensure that all devices are synchronized. The MIB defined in Global Object Definitions (NTCIP 1201 and Amendment 1), includes a data element called "globalTime." Below is the ASN.1 definition of this data element.

```
globalTime OBJECT-TYPE
SYNTAX  Counter
ACCESS  read-write
STATUS  mandatory
DESCRIPTION "The current time in seconds since the epoch 00:00:00
(midnight) January 1, 1970 UTC (a.k.a. Zulu)."
::={globalTimeManagement 1}
```

The first line is the name of the data element, followed by the formal invocation of the OBJECT-TYPE macro.

The SYNTAX line defines the variable type. In this example, the type is a Counter. The SNMP standards define a Counter to be an `INTEGER` with a range of 0 to 4294967295 that performs a counting operation. Upon reaching the maximum value, the Counter rolls over and starts at zero.

The STATUS line is provided to simplify conformance statements. At the end of each data element standard, conformance groups are defined. For a device to claim conformance to a conformance group, it must support all "mandatory" data elements within that group. It may also support "optional" data elements within the group. For a device to claim conformance to a standard, it must support all "mandatory" conformance groups defined by the standard, and may optionally support "optional" conformance groups. Note: Version 2 of the NTCIP 1201 standard will revise this scheme for global data elements (only) in that the definition of conformance groups and contained mandatory data elements are left up to the device-specific standards, such as NTCIP 1202 (actuated signal controllers).

The Description line provides a human readable description of the data element. This data element represents the current time as represented in seconds since midnight January 1, 1970 in Greenwich, England. Many data elements specify some sort of functionality; in this case, this data element requires the device to increment the value of this data element by one at a rate of exactly once a second.

The last line indicates the location of this data element on the ISO Global Naming tree. In this case, the data element is the first node under the globalTimeManagement node. Earlier within the standard, the globalTimeManagement node was defined to be underneath the global node. This referencing continues within the standard all the way back to the ISO root node.

Exhibit 6.5 lists some common ASN.1 terms used for data element definitions. Since this is an incomplete list, refer to ISO 8824 and the NTCIP publications for more information. The NTCIP also defines additional limitations to ASN.1. These limitations are defined in a section called the NEMA Structure and Identification of Management Information (NEMA_SMI). The NEMA_SMI is not a MIB but is added to all NTCIP MIBs.

The ASN.1 macro language is very powerful, even with the restrictions imposed by SNMP. A MIB may define a new syntax by combining basic (primitive) data types. Likewise, a MIB can define a one or multi-dimensional table using the `SEQUENCE` operator. Default values and ranges for data elements can also be defined in the MIB. The robustness of the ASN.1 language allows for the modeling of virtually any database likely to be encountered in ITS field devices.

The MIB data elements are related by device type, for example, a traffic controller MIB or a message sign MIB. These device MIBs are called modules. NTCIP has MIB modules for actuated traffic controllers (ASC), dynamic message signs (DMS), closed circuit television control (CCTV) and environmental sensor stations (ESS), to name but a few. It is desirable to use a standard MIB wherever possible, but as new device features require additional data elements, new versions of a MIB can be created. NTCIP also supports proprietary and experimental MIBs. Experimental MIBs are kept under a separate node and users know that the MIB is subject to change. Proprietary MIBs can exist under nodes registered to either private firms or public agencies.

Exhibit 6.5: Some Common ASN.1/NTCIP Terms for Data Element Definitions

ASN.1 Tag	Description	Some Options
OBJECT-TYPE	Alphanumeric string that names the data element	
SYNTAX	Object data type	**INTEGER (-128...127)** **INTEGER (0...255)** **INTEGER (0...4294967295)** **OCTET STRING** - a string of bytes, such as ASCII text
ACCESS	Determines read/write capabilities	**read-only** **read-write** **not-accessible**
STATUS	Determines whether this data element is required.	**mandatory** - must be supported **if** a conformance group containing this data element is supported. **optional** - not mandatory. **deprecated -** use of the data element is discouraged, however, management stations should support the data element as it may be encountered in a deployed device; future releases of the standard may mark the data element obsolete. **obsolete** - the data element has been deleted or replaced; management stations and agents are not required to implement it.
DESCRIPTION	Explanation of what the data element represents and how to interpret it	Anything you want to write to unambiguously describe the purpose of the data element including any limitations, the units, that is, seconds or tenths of seconds.

Data elements in the MIB are arranged in a tree structure, and data elements are named by the path along the branches of the tree to the data element. The path starts at the trunk of the tree, and a node identifier is added at each branch until the data element is reached. The node identifiers are unsigned integers and are frequently documented in text as dot separated, for example, "1.3.6.1.4.1.1206". The tree structure is formally defined by ISO and CCITT. An entire MIB module will hang off this global name tree. Below is a diagram showing the tree structure from its root to the NEMA node. All standardized NTCIP MIB modules will be attached to the NEMA node.

All data elements in the NEMA NTCIP MIB modules will start with 1.3.6.1.4.1.1206 or (*iso.org.dod.internet.private.enterprises.nema*). NEMA has further divided the 1206 node into four subgroups: mgmt(1), experimental(2), private(3) and devices(4).

Everything below the transportation node constitutes the Transportation MIB (TMIB). Within the TMIB there are protocol, devices and tcip data element groups. The devices group has subtrees for each of the supported devices: asc, ramp meter, dms, cctv, ess, and global. Branches are added as new devices are included in the NTCIP family of standards.

Example 6.2:

Consider our globalTime data element in example 6.1. The object identifier for globalTime is defined as globalTimeManagement 1. GlobalTimeManagement is previously defined as global 3. Finally, the header of the MIB contains the following:

```
nema OBJECT IDENTIFIER::= {iso(1) org(3) dod(6) internet(1)
private(4) enterprises(1) 1206}
              transportation OBJECT IDENTIFIER::= {nema 4}
              devices OBJECT IDENTIFIER::= {transportation 2}
              global OBJECT IDENTIFIER::= {devices 6}
```

Thus, the Object Identifier (OID) for global is 1.3.6.1.4.1.1206.4.2.6 or (iso.org.dod.internet.private.enterprises. nema.transportation.devices 6). The OID for globalTimeManagement is 1.3.6.1.4.1.1206.4.2.6.3 and the OID for globalTime is 1.3.6.1.4.1.1206.4.2.6.3.1. As mentioned above, each data element is instantiated by the agent. In the case of globalTime, there is only one instance, that is, the data element is not contained in a table, and thus, its instance number is zero (0). Thus, the full OID for the instance of globalTime within our DMS would be 1.3.6.1.4.1.1206.4.2.6.3.1.0.

When using STMP, this 13-node identifier (OID) can be pre-configured to minimize bandwidth consumption on frequently transmitted messages.

The databases for NTCIP devices are defined using ASN.1, which provides a standard method for data element definition, organization and identification. We have examined how to define a data element and identify the path to the data element using this standard. Next, we examine how the object identifier or path and the value of the data element are encoded into binary data for transmission.

6.4.2 Encoding the NTCIP Database for Transmission

To transmit a data element we first need to select the protocols that we will use for transmission. In the DMS example, we indicated that we would support the minimal requirements of the STMF, Internet and PPP profiles; these protocols were identified in Exhibit 6.4. Thus, in this example, we use an application layer of SNMP.

Encoding a data element with Its Value

SNMP uses a standard set of rules for encoding called, Basic Encoding Rules (BER) (ISO 8825-1). BER defines that each data element is encoded in variable binding list. A variable binding list consists of a separate encoding for the OID of the data element and the encoding for the value of the data element. The encoding for both types (OID and value) follows the same setup: data type, length and value.

Example 6.3:

Using the data element from example 6.1, we need to encode the object identifier and value:

Identifier

```
Type    OBJECT IDENTIFIER
Length  The number of octets (i.e., bytes) used to encode the value
of the identifier
Value   1.3.6.1.4.1.1206.4.2.6.3.1.0
```

Value

```
Type    Counter
Length  The number of octets used to encode the value of the
identifier
Value   915148800 (i.e., 00:00:00, 1 January 1999 UTC)
```

SNMP defines the values for allowed types. The hexadecimal values for the most common types are:

- INTEGER 0x02
- OCTET STRING 0x04
- NULL (Placeholder) 0x05
- OBJECT IDENTIFIER 0x06
- SEQUENCE 0x30
- Counter 0x41
- Gauge 0x4x
- Opaque 0x4x

According to the rules of BER, the first two components of an OBJECT IDENTIFIER are combined using the formula (40X)+Y to form the first subidentifier. Each subsequent component forms the next subidentifier. Each subidentifier is encoded as a non-negative integer using as few seven bit blocks as possible. The blocks are packed into octets, with the first bit of each octet set to a 1 except for the last octet of each subidentifier. Thus, the object identifier (OID), {1.3.6.1.4.1.1206.4.2.6.3.1.0} is encoded as follows:

Exhibit 6.6: Data Element Component, Subidentifier and Octet Sequence Hex

Component	Subidentifier	Octet Sequence Hex
1.3 (iso org)	43	[2B]
6 (dod)	6	[06]
1 (internet)	1	[01]
4 (private)	4	[04]
1 (enterprises)	1	[01]
1206 (nema)	1206	10010110110 bin [89][36]
4 (transportation)	4	[04]
2 (devices)	2	[02]
6 (global)	6	[06]
3(globalTimeManagement)	3	[03]
1 (globalTime)	1	[01]
0 (instance 0)	0	[00]

Note that [xx] represents a number in hexadecimal format.

Adding the OBJECT IDENTIFIER type of [06] and a length of [0D] or (13 decimal) yields the following byte sequence:

```
[06][0D][2B][06][01][04][01][89][36][04][02][06][03][01][00]
```

Next, we encode the data value, which is 915148800. BER encodes Counters in the same way as it encodes INTEGERs, with a two's complement representation using the minimum number of octets (note - this means the value 255 would be encoded in two bytes, [00][FF], so that the high order bit is set to zero indicating a positive number). Thus, the byte sequence of would be:

```
[36][8C][10][00]
```

A Counter has a type code of [41].

Thus, our data element value with a type of [41] and a length of [04] would become:

```
[41][04][36][8C][10][00]
```

The combined byte SEQUENCE (Type [30]) for the OID and value has a length of 21 ([15]). Thus, the entire encoding for this data element is:

```
[30][15][06][0D][2B][06][01][04][01][89][36][04][02][06][03][01][
00][41][04][36][8C][10][00]
```

If STMP was used, a dynamic object could be configured to include this data element. In this case, only the object identifier would not be transmitted (because each end of the link would already be aware of what data to expect next). Further, the data value would be encoded using Octet Encoding Rules (OER) as defined in NTCIP 1102, which is more efficient than BER. Thus, an STMP dynamic object would encode the above information in 4 bytes instead of the 23 bytes shown, that is, 21 plus type and length of the sequence. Some occasional messages must still be sent via SNMP, including the message used to tell the field device of a change in a dynamic message definition.

Example 6.3 examined only two data types that can be encoded with BER. BER contains encoding rules for all ASN.1 types.

Encoding the SNMP Data Packet

We have created a data element using ASN.1, placed it in a tree structure, gave it a real value, and finally encoded the data element and its value using BER. Now this information must be given in a context. For example, is this a request to set the time, or is it a response to a get request? The context is given by the surrounding structure of the data packet, as defined by the rules of SNMP.

SNMP uses a get/set/trap paradigm. The table below lists the SNMP message types, purposes and originators.

Exhibit 6.7: SNMP Message Type, Purpose, and Originator

Message Type	Purpose	Originator
Get Request	Contains a list of data elements, the agent is to return the values	Management Application
Get Next Request	Contains a list of data elements, the agent is to return the values of the next sequential data element from those indicated.	Management Application
Set Request	Contains a list of data elements and values, the agent is to set the values in its MIB per this message	Management Application
'Get' Response	Agent response to either a Get or a Set request	Agent Application
Trap	An Agent initiated transmission to indicate that a defined event has occurred.	Agent Application

The SNMP Message structure is given by the following ASN.1 structure:

```
Message::= SEQUENCE {
              version            INTEGER { version-1(0)},
              communityOCTET STRING,
              data               CHOICE {
get-request GetRequest-PDU (with a data type value of 0xA0),
              get-next-request GetNextRequest-PDU (data type value
= 0xA1),
              get-response GetResponse-PDU (data type value =
```

```
0xAx),
                set-request         SetRequest-PDU (data type value
= 0xA2),
                trap                                Trap-PDU
                }
}
```

All of the PDU structures have essentially the same structure, as follows, with a different Tag.

```
GetRequest-PDU::= [0] IMPLICIT SEQUENCE {
                request-id          RequestID,
                error-status ErrorStatus,
                error-index         ErrorIndex,
                variable-bindings SEQUENCE OF SEQUENCE {
                                name   OBJECT IDENTIFIER,
                                value  ObjectSyntax -- i.e., the SYNTAX
of the selected data element
                                }
                }
```

The 23 byte data stream produced above forms the following sub-structure in the above structure.

```
SEQUENCE {
                                name                OBJECT IDENTIFIER,
                                value               ObjectSyntax --
i.e., the SYNTAX of the selected data element
                                }
```

Thus, we now have to add the rest of the components of the data packet. In this case, we will assume the data packet is a get response for a get request of both the globalTime data element as well as the globalDaylightSavings data element, as follows:

Exhibit 6.8: Example of Get Response

Field	Byte Stream
SEQUENCE - Type and Length (Value is below)	[30][45]
version - INTEGER of 1 byte, value 0	[02][01][00]
community - OCTET STRING of 6 bytes (“Public”)	[04][06][50][75][62][6C][69][63]
data - Type and Length (Value below)	[A2] [38]
request-id - In this case we use 1	[02][01][01]
error-status	[02][01][00]
error-index	[02][01][00]
variable-bindings SEQUENCE OF	[30] [2D]
SEQUENCE	[30][2B]
name	[06][0D][2B][06][01][04][01] [89][36][04][02][06][03][01][00]
value	[41][04][36][8C][10][00]

Exhibit 6.8: Example of Get Response

Field	Byte Stream
SEQUENCE	[30][12]
name	[06][0D][2B][06][01][04][01] [89][36][04][02][06][03][02][00]
value	[02][01][03]

The Get Request would be nearly identical. The data type would be [A0] rather than [A2] and the value fields would be NULL, that is, Type 5 and zero length, [05][00].

The Transport Profile

The above structure defines the encoding of the Application Layer. This data must now be prepared for transmission through the network. In general, this consists of transmitting the data from one device (IP Address) to another device (IP Address). The data stream defined above is then packaged into the network datagram required for transmission across this network. Based on the decision to use the Internet Transport Profile, this will entail placing the above data stream into an UDP datagram and then placing the UDP datagram into an IP packet.

The Subnetwork Profile

Once the IP packet is ready for transmission, it must be prepared for transmission across the next link, that is, the subnetwork. Based on the decision to use the PPP Subnetwork Profile, this entails encapsulating the IP packet into a PPP frame and ensuring that the PPP session is properly established before the frame is transmitted. Likewise, at some point after transmission, the link should be closed.

CRC Algorithm for AB3418 and NTCIP

AB 3418 is a 1995 California Department of Transportation (Caltrans) communications standard that ensures interconnectivity of traffic signal control devices, and does so by utilizing existing communication standards and models. AB 3418 specifies parts of the NTCIP and ISO/IEC specifications for the data link layer but specifies a fixed set of messages related to traffic signal controllers. Additional messages were defined in 1999 and this new version is called AB 3418E. See on http://www.dot.ca.gov/hq/traffops/elecsys/ab3418/ab3418a.htm for more information on AB 3418.

Cyclical Redundancy Check (CRC) is 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. The CRC Algorithm applies to NTCIP 2001, NTCIP 2101, NTCIP 2102, and NTCIP 2103. (It is also used in IEEE 1570.)

The following C Source Code is an implementation of a table lookup algorithm for calculating and verifying the FCS value used in the HDLC and PPP Protocols (NTCIP 2103):

```
#include <stdio.h>
typedef unsigned short int u16;

u16 fcstab[256] = {
0x0000, 0x1189, 0x2312, 0x329b, 0x4624, 0x57ad, 0x6536, 0x74bf,
0x8c48, 0x9dc1, 0xaf5a, 0xbed3, 0xca6c, 0xdbe5, 0xe97e, 0xf8f7,
0x1081, 0x0108, 0x3393, 0x221a, 0x56a5, 0x472c, 0x75b7, 0x643e,
0x9cc9, 0x8d40, 0xbfdb, 0xae52, 0xdaed, 0xcb64, 0xf9ff, 0xe876,
0x2102, 0x308b, 0x0210, 0x1399, 0x6726, 0x76af, 0x4434, 0x55bd,
0xad4a, 0xbcc3, 0x8e58, 0x9fd1, 0xeb6e, 0xfae7, 0xc87c, 0xd9f5,
0x3183, 0x200a, 0x1291, 0x0318, 0x77a7, 0x662e, 0x54b5, 0x453c,
0xbdcb, 0xac42, 0x9ed9, 0x8f50, 0xfbef, 0xea66, 0xd8fd, 0xc974,
0x4204, 0x538d, 0x6116, 0x709f, 0x0420, 0x15a9, 0x2732, 0x36bb,
0xce4c, 0xdfc5, 0xed5e, 0xfcd7, 0x8868, 0x99e1, 0xab7a, 0xbaf3,
0x5285, 0x430c, 0x7197, 0x601e, 0x14a1, 0x0528, 0x37b3, 0x263a,
0xdecd, 0xcf44, 0xfddf, 0xec56, 0x98e9, 0x8960, 0xbbfb, 0xaa72,
0x6306, 0x728f, 0x4014, 0x519d, 0x2522, 0x34ab, 0x0630, 0x17b9,
0xef4e, 0xfec7, 0xcc5c, 0xddd5, 0xa96a, 0xb8e3, 0x8a78, 0x9bf1,
0x7387, 0x620e, 0x5095, 0x411c, 0x35a3, 0x242a, 0x16b1, 0x0738,
0xffcf, 0xee46, 0xdcdd, 0xcd54, 0xb9eb, 0xa862, 0x9af9, 0x8b70,
0x8408, 0x9581, 0xa71a, 0xb693, 0xc22c, 0xd3a5, 0xe13e, 0xf0b7,
0x0840, 0x19c9, 0x2b52, 0x3adb, 0x4e64, 0x5fed, 0x6d76, 0x7cff,
0x9489, 0x8500, 0xb79b, 0xa612, 0xd2ad, 0xc324, 0xf1bf, 0xe036,
0x18c1, 0x0948, 0x3bd3, 0x2a5a, 0x5ee5, 0x4f6c, 0x7df7, 0x6c7e,
0xa50a, 0xb483, 0x8618, 0x9791, 0xe32e, 0xf2a7, 0xc03c, 0xd1b5,
0x2942, 0x38cb, 0x0a50, 0x1bd9, 0x6f66, 0x7eef, 0x4c74, 0x5dfd,
0xb58b, 0xa402, 0x9699, 0x8710, 0xf3af, 0xe226, 0xd0bd, 0xc134,
0x39c3, 0x284a, 0x1ad1, 0x0b58, 0x7fe7, 0x6e6e, 0x5cf5, 0x4d7c,
0xc60c, 0xd785, 0xe51e, 0xf497, 0x8028, 0x91a1, 0xa33a, 0xb2b3,
0x4a44, 0x5bcd, 0x6956, 0x78df, 0x0c60, 0x1de9, 0x2f72, 0x3efb,
0xd68d, 0xc704, 0xf59f, 0xe416, 0x90a9, 0x8120, 0xb3bb, 0xa232,
```



```
0x5ac5, 0x4b4c, 0x79d7, 0x685e, 0x1ce1, 0x0d68, 0x3ff3, 0x2e7a,
0xe70e, 0xf687, 0xc41c, 0xd595, 0xa12a, 0xb0a3, 0x8238, 0x93b1,
0x6b46, 0x7acf, 0x4854, 0x59dd, 0x2d62, 0x3ceb, 0x0e70, 0x1ff9,
0xf78f, 0xe606, 0xd49d, 0xc514, 0xb1ab, 0xa022, 0x92b9, 0x8330,
0x7bc7, 0x6a4e, 0x58d5, 0x495c, 0x3de3, 0x2c6a, 0x1ef1, 0x0f78
};

u16 compute_fcs(unsigned char *data, int length)
{   u16 fcs;

    fcs = 0xffff;
    while (length--)
    {   fcs = (fcs >> 8) ^ fcstab[(fcs ^ ((u16)*data)) & 0xff];
        data++;
    }
    return (fcs);
}

unsigned char pattern[8] =
    { 0x03, 0x3f, 0x5b, 0xec, 0x00, 0x00, 0x00, 0x00 };

int main(int argc, char *argv[])
{   int i, j, k;
    u16 fcs;

    fcs = compute_fcs(pattern, 2);     /* generate CRC for
transmission
*/
    fcs = fcs^0xffff;
    printf("%02x %02x %02x %02x\n", pattern[0], pattern[1],
fcs&0xff,
(fcs>>8)&0xff);

    fcs = compute_fcs(pattern, 4);     /* check CR on reception */
    printf("%02x %02x %02x %02x %04x\n", pattern[0], pattern[1],
pattern[2],
pattern[3], fcs);
    if (fcs != 0xf0b8)
        printf("Bad CRC on reception!\n");

#ifdef MSDOS_TEST
    i = *(u16 far *)(0x0040006c);      /* get a random number */
    pattern[0] = (i&0xff);
    pattern[1] = (i>>8)&0xff;

    fcs = compute_fcs(pattern, 2);
    fcs = fcs^0xffff;
    printf("%02x %02x %02x %02x\n", pattern[0], pattern[1],
fcs&0xff,
(fcs>>8)&0xff);

    pattern[2] = fcs&0xff;
    pattern[3] = (fcs>>8)&0xff;
```

```
        fcs = compute_fcs(pattern, 4);
        printf("%02x %02x %02x %02x %04x\n", pattern[0], pattern[1],
    pattern[2],
    pattern[3], fcs);
    #endif
    }
```

The following example shows the proper FCS value for a two-byte HDLC frame consisting of 0x03 and 0x3F for the address and control fields:

The following example shows the proper FCS value for a two-byte frame consisting of 0x03 and 0x3F.

V - first bit transmitted				last bit transmitted - V
0111 1110	1100 0000	1111 1100	1101 1010 0011 0111	0111 1110
flag	address	control	FCS	flag

6.5 Defining New Data Elements

AASHTO, ITE and NEMA have defined an open and expandable suite of protocols. NTCIP permits completely open database definitions without precluding completely proprietary (closed) ones. NTCIP will serve both open and closed databases on the same network. Users are encouraged to review the existing MIB data element definitions before attempting to add new ones to avoid allowing the definition of data elements whose functions are already defined in standard NTCIP data elements.

The creation of a new MIB module can be quite easy. This is especially true if the device to be supported already has a list of defined requirements and database. One should start by defining the necessary data elements for the device using ASN.1 and attempting to organize them in a subtree. Obtain from NEMA, a root node for the subtree under the NEMA private or experimental node. Seek comments from NEMA, manufacturers and users of similar devices. In the early stages of NTCIP development, it may be sufficient to list the needed data elements by name and proposed data types (submit them to the Joint NTCIP Standards Committee for further development). Above all, try to use the existing data element definitions as much as possible; this will further compatibility between devices.

6.6 Examples of Implementation Problems

A number of issues arose during the integration of the various components of the NTCIP demonstration, which was unveiled at TRB in January 1996, and during the subsequent deployment of the NTCIP standards. These issues are documented here to provide future implementers and integrators information for their design consideration.

6.6.1 Protocol-Related Issues

Implementing a standard requires careful examination of a large amount of text within the standards. A number of the problems discovered during the integration work related to invalid interpretation of the specifications, especially relating to those clauses that reference other specifications without providing significant detail. In order to minimize the number of these conflicts in the future, a discussion of some of these issues is provided below.

Bit and Byte Order

Bit and byte order in a computer are not necessarily the same as the bit and byte order on the transmission medium. The transmission order varies in accordance with the guidelines of international standards. Implementations should ensure that the representation of the most and least significant bits and bytes in the computer accurately reflect what is sent and received on the transmission media.

Extended Addresses

There has been some confusion about how large of a high-level data link control (HDLC) address must be supported. For both of the PMPP and PPP Subnetwork Profiles, NTCIP devices are required to fully support one-byte addresses and to accept incoming frames with two-byte addresses to the device address. Production of frames with two-byte addresses is optional as is support for configuring the device to an address greater than 63.

All addresses are odd; if the first byte of an address is even, then the address is multi-byte.

Maximum Duration Between Successive Bytes

Many existing field devices use proprietary protocols that expect incoming messages to be a series of bytes with minimal delay between the bytes. They will time-out as an 'end of message' when a byte is not received in 15ms for 1,200-bps communications. This means that consecutive messages must be separated by about 30ms at 1,200 bps. With the simultaneous use of 'soft carrier turnoff', this gap must be increased by the 'soft carrier turnoff time'. At higher transmission rates, these times are proportionally reduced.

Because of the desire for full-duplex communications, devices conforming to the PMPP Profile should be designed to support much greater durations between successive bytes as suggested in the NTCIP publications. In short, the only distinguishing limit of a message is the 0x7E flag.

Response Time

The public domain code that is available was developed using DOS and Windows; in both cases the serial port interrupt is only checked every 50ms. Thus, these systems do not perform quite as well as desired; however, this was not an issue for the demonstration.

A real product should use a serial port driver to achieve the desired performance. The desired performance is system dependent and is stored in the T2 [the maximum time that a device is allowed to take before starting to send a response] data element. In a multi-drop environment, it is desirable to minimize the duration of the T2 timer. A T2 value of 40ms or less is desirable, but not always achievable. According to NTCIP standards, the secondary is not allowed to respond after its T2 timer expires.

Control Byte

PMPP includes support for three control byte values. A primary can transmit an unnumbered poll (0x33), an unnumbered information command with the poll bit set (0x13), or an unnumbered information command without the poll bit set (0x03). The secondary must respond to every frame received with the poll bit set, that is, either 0x33 or 0x13, and the response frame from the secondary must be an unnumbered information response with the final bit set (0x13). The secondary may not transmit at any other time. (Note that these values are presented according to Internet encoding rules.)

PPP devices are peer devices, that is, either the management station or the field device may communicate at any time, because they are the only devices on the 4-wire link at any given time. In this environment, there is no need to give permission to the other device, nor is there a need to force a data link response. As such, the PPP Profile only uses the unnumbered information command without the poll bit set for both ends of the link. This byte may be omitted, if such operation has previously been negotiated (see the PPP Subnetwork Profile and the PPP RFC).

Frame Handling

In PMPP systems, the primary may constantly poll each device in order to determine whether it has any information to report. If the primary station has information to transmit with this poll, for example, a request, it encapsulates this data in an unnumbered information command with the poll bit set. If there is not any information to send, it sends an "empty" frame of six bytes called an unnumbered poll frame. If the primary station has information to send, but does not want to give the opportunity for the receiving device to respond, for example, a broadcast, it sends the data in an unnumbered information frame without the poll bit set.

When a secondary station receives an unnumbered information frame with the poll bit set or an unnumbered poll, it responds with an unnumbered information frame with the final bit set. If the secondary has any data to send with this frame, it is encapsulated within the frame. If the secondary does not have any data to send, it should send an empty frame.

When a secondary station receives an information command without the poll bit set, for example a broadcast message)\, it does not respond.

It should be further noted that these rules only deal with the data link layer. For example, a central system may send a broadcast message without a poll at the data link layer, while requesting a response at the application layer. The remote device would prepare a response at the application layer that would then be stored in the device's data link layer. This response could only be sent out after the device has received a frame with the poll bit set.

For example, if dynamic object 1 had been defined to be the time data element, the primary (central) station could send the following byte stream:

```
Flag Addr Ctrl IPI STMP   ----SET Time----     CRC     Flag
7E   FF   03   C1   91   31   E6   E7   00   XX   XX   7E
```

The address indicates that everyone receives it and the control byte prevents anyone from responding on the wire; however, the STMP byte is a SET with response. Thus, all of the devices generate responses at the application layer and they are sent to the data link layer to be transmitted. Then, the data link layer waits until permission is granted for the device to speak, for example, an unnumbered poll frame. In this way, a central system can broadcast the time and then go back and ensure that all the devices received the message.

If the secondary has a pending response waiting at the data link layer, it should send the response immediately upon receiving a frame with the poll bit set. If the incoming frame contains information, the information should be processed. This might entail producing a new response that will be sent to the data link layer, where it will reside until the next poll is received.

A device is responsible for storing one response frame at the data link layer. If a second response is generated before the first is sent, the first response should be overwritten.

CRC Algorithm

Examples of how to code the cyclical redundancy check (CRC) algorithm can be found in the AB3418 code and the FHWA code used in the demonstration. Additionally, this code could be retrieved from the Internet. This same algorithm is used in both PMPP and PPP.

Invalid Frame

In both PMPP and PPP, when a device receives an invalid frame it should just discard the frame. Invalid frames include those with invalid CRCs, and invalid initial protocol identifiers, Devices should not provide any response to invalid frames.

STMP Message Type Byte

To see how the STMP Message Type Byte is coded and used, see NEMA Standards Publication NTCIP 1101, National Transportation Communications for ITS Protocol, Simple Transportation Management Framework.

Length Values for Variable Message Fields

The exact meaning of this field, that is, which bytes are included in the count, has led to some confusion. The count value does not include the count byte in the count, that is, the count starts the byte after the count byte.

6.6.2 Systems Integration Issues

In addition to those issues raised about the interpretation of the specifications, there were also issues over how systems should be designed and what should be required in procurement specifications to achieve the goal of systems interoperability. This section provides some guidance on how to approach these issues.

Carriers

It is very important that secondary stations on multi-drop lines turn off their modem carriers when not sending data. After responding to a poll, the carrier must be removed from the line so that other stations may respond.

Number of Devices on a Channel

The input impedance of the transmission output circuit in the field device modems limits the maximum number of field devices that can reliably be supported on a single modem channel. Each of these outputs is a load on the field device transmission line. A practical upper limit is somewhere around 15 field devices for the current technology 202 modems. Advanced 202 modems can be used that will isolate the individual transmission circuits unless the modem is actively transmitting. In a system with only four to seven field devices per channel, this consideration can usually be ignored without detrimental effects, since communications timing is usually the determining factor in the maximum number of devices per channel. Section 5 provides a more detailed explanation for determining the maximum number of devices per channel.

MIB Issues

All NTCIP procurements should specify that the manufacturers/developers must provide the devices' MIB module(s) to the purchasing agency, with rights to distribute to their agents, for example, those persons acting on behalf of the agency. The MIBs should be provided in ASCII format on the medium of the procuring agency's choice. The MIBs should include all Simple Network Management Protocol (SNMP)/Simple Transportation Management Protocol (STMP) data elements that the device(s) support(s).

6.7 Development Resources

There are wide varieties of resources available that relate to the NTCIP. This section lists some of the resource materials that have been used in the development process and early implementations, as well as the location of developed materials.

6.7.1 Websites

A wide range of documentation is available on the World Wide Web NTCIP Home Page located at *www.ntcip.org/*.

The site currently includes such items as these:

- NTCIP Profile publications
- NTCIP data element definitions for a variety of devices
- NTCIP Case Studies
- Various white papers written during the development of the initial standards
- FHWA-sponsored software packages, for example, NTCIP demonstration, NTCIP Exerciser and NTCIP Field Devices Simulator.

Other web sites of interest are shown in Exhibit 6.9.

Exhibit 6.9: NTCIP Related Websites

Website	Address	Description
NTCIP	On www.ntcip.org/	The official web site for NTCIP and related publications and information.
DATEX-ASN	On www.trevilon.com/library.htm	The web site for DATEX-ASN documents and information
DATEX-Net	On www.datex.org/	The official web site of the DATEX-Net Standard currently in use in Europe.
IANA	On www.iana.org/numbers.html	The Internet Assigned Numbers Authority web site.
IEEE	On standards.ieee.org/	Links to all of the IEEE standards efforts, including ATIS, Incident Management, Data Dictionaries and Data Registries.
ISO	On www.iso.ch/	The official ISO home page.
ITE	On www.ite.org/	ITE web site.
ITS America	On www.itsa.org/	The home page for ITS America.
NEMA Standards	On www.nema.org/index_nema.cfm/707/	Site for ordering NTCIP standards.
RFC Index	On www.nexor.com/public/rfc/index/rfc.html	A search engine for all of the Internet RFCs.
SNMP	On www.cmu.edu/	A library of information on SNMP and related topics.
TCIP	On www.tcip.org/	The home page for the Transit Communications Interface Profiles.

6.7.2 Sources of Public Domain Software

There are two basic prototype implementations of NTCIP software. Neither of these packages was designed to operate a real system; rather, they were designed to provide tools to the industry to test equipment submitted as being conformant to a specific protocol. Unfortunately, there is no ongoing program to maintain these packages.

NTCIP Exerciser

This NTCIP Exerciser is able to read in any properly formatted management information base (MIB) from a floppy disk and support the exchange of fully conformant NTCIP messages under the direction of the operator. The package supports the creation of simple macros to enable the user to perform a number of operations sequentially and to record the results. The current version supports the simulation of either a management station (funded by the FHWA) or an agent (funded by Virginia DOT). It currently supports the STMF Application Profile (SNMP only), Null Transport Profile and both the PMPP-232 Subnetwork Profile and the PPP Subnetwork Profile. The most recent version of this software is available for free on the NTCIP Website. It is designed for Windows NT.

Field Device Simulator (FDS)

The FHWA also developed a DOS based program to emulate a field device that supports the data elements contained in the Global Object Definitions. This program supports the STMF Application Profile (SNMP-only), the Null Transport Profile and the PMPP-232 Subnetwork Profile.

6.7.3 Books

During the development of the standards and prototypes, a number of books were consulted; including the following:

Stevens, W. R., *TCP/IP Illustrated, Volume 1, The Protocols*: Reading, Massachusetts: Addison Wesley Publishing Co. 1994

- Wright, G. R. and Stevens, W. R., *TCP/IP Illustrated, Volume 2, The Implementation*, Reading, Massachusetts: Addison Wesley Publishing Co. 1995
- International Technical Support Center Raleigh N. C., *TCP/IP Tutorial and Technical Overview*, Document Number GG24-3376-01, IBM Corp, Armonk, N.Y.: June 5, 1990, 2nd Edition
- Rose, M. T., *The Open Book*, Englewood Cliffs, N.J.: Prentice Hall, 1990
- Stallings, W., *SNMP, SNMPv2, and CMIP The Practical Guide to Network Management Standards,* Reading, Massachusetts: Addison Wesley Publishing Co. 1993

- Perkins, D. and McGinnis, E., *Understanding SNMP MIBS*, 1997, Upper Saddle River, New Jersey: Prentice Hall, Inc., 1997.

6.7.4 Other Resources

In addition, there are articles in the December 1995, January 1996, and April 1996 issues of the *ITE Journal*. There are periodic releases of *NTCIP News*, a newsletter produced by the Joint Committee on the NTCIP. Finally, there are updates of ITS standards in each Journal.

6.8 Summary

Transportation devices, like any other computer device, require databases, processors and interfaces. If the device intends to share its data with other devices, a communication protocol is required. NTCIP fulfills the requirement for a set of communication protocols that are flexible enough to support the variety of fixed-point communications systems within ITS.

THIS PAGE LEFT INTENTIONALLY BLANK

Chapter 7

Glossary

7.1 Useful ITS Acronyms

A

AAR
Association of American Railroads

AASHTO
American Association of State Highway and Transportation Officials

ACC
Adaptive Cruise Control

ACN
Automatic Collision Notification

ADA
Americans with Disabilities Act

ADIS
Advanced Driver Information System

ADUS
Archived Data User Service

AHS
Automated Highway System or Advanced Highway System

ALI
Automatic Location Identification

ANI
Automatic Number Identification

ANSI
American National Standards Institute

AP
Application Profile

API
Application Program Interface

APTA
American Public Transit Association

APTS
Advanced Public Transportation System

AREMA
American Railway Engineering and Maintenance of Way Association

ARSI
Automated Roadside Safety Inspection

ARTS
Advanced Rural Transportation System

ASC
Actuated Signal Control

ASCE
American Society of Civil Engineers

ASCII
American Standard Code for Information Interchange

ASLRRA
American Short Line and Regional Railroad Association

ASN.1
Abstract Syntax Notation – 1

ASTM
American Society for Testing and Materials

ATA
American Trucking Association

ATC
Advanced Transportation Controller

ATCS
Advanced Train Control System

ATIS
Advanced Traveler Information System

ATMS
Advanced Traffic Management System

AVC
Automated Vehicle Classification

AVCS
Advanced Vehicle Control System

AVI
Automatic Vehicle Identification

AVL
Automatic Vehicle Location

AVLS
Automatic Vehicle Location System

AVM
Automatic Vehicle Monitoring

B – C

BA
Business Area

BER
Basic Encoding Rules or Bit Error Rate

bps
bits per second

C2C
Center-to-Center

C2F
Center-to-Field

CAD
Computer-Aided Dispatch

CBTC
Communications-Based Train Control

CC
Control Center

CCITT
International Telegraph and Telephone Consultative Committee, now being referred to as ITU

CCTV
Closed-Circuit Television

CEMA
Consumer Electronics Manufacturers Association

CFR
Code of Federal Regulations

CHAP
Challenge-Handshake Authentication Protocol

CMS
Changeable Message Sign

CORBA
Common Object Request Broker Architecture Protocol

CP
Class Profile

CPT
Common Public Transportation

CRC
Cyclical Redundancy Check

CSA
Canadian Standards Association

CTAA
Community Transit Association of America

CVISN
Commercial Vehicle Information Systems and Networks

CVO
Commercial Vehicle Operations

D

DARC
Data Radio Channel

DATEX
DATa EXchange Protocol

DCM
Data Collection and Monitoring

DD
Data Dictionary

DE
Data Element

DGPS
Differential Global Positioning System

DISA
Data Interchange Standards Association

DMS
Dynamic Message Sign

DMV
Department of Motor Vehicles

DR
Data Registry

DRGS
Dynamic Route Guidance System

DS
Data Set or Dynamic Scheduling

DSRC
Dedicated Short-Range Communications

DTE
Data Terminal Equipment

DTR
Data Terminal Ready

E

EBS
Emergency Broadcasting System

EDI
Electronic Data Interchange

EFT
Electronic Funds Transfer

EIA
Electronics Industry Alliance

EMS
Emergency Management System or Emergency Medical Services

ESS
Environmental Sensor Systems

ETC
Electronic Toll Collection

ETS
Emergency Telephone System

ETMCC
External Traffic Management Center Communication

ETTM
Electronic Toll and Traffic Management

F

FARS
Fatal Accident Reporting System

FC
Fare Collection

FCC
Federal Communications Commission

FCS
Frame Check Sequence (see Cyclic Redundancy Check)

FCW
Front Collision Warning

FHWA
Federal Highway Administration

FMS
Field Management Station

FRA
Federal Railroad Administration

FSK
Frequency Shift Keying

FTA
Federal Transit Administration

FTP
File Transfer Protocol

G – H

GDF
Geographic Data File

GIS
Geographic Information System

GPS
Global Positioning System

HAR
Highway Advisory Radio

HAZMAT
Hazardous Materials

HDLC
High-Level Data Link Control

HHI
Highway-Highway Intersection

HOV
High Occupancy Vehicle

HPMS
Highway Performance Monitoring System

HRI
Highway-Rail Intersection

HSR
High Speed Rail

HUD
Heads-Up display

I

IAB
Internet Activities Board

IANA
Internet Assigned Numbers Authority

ICC
Intelligent Cruise Control

IDB
ITS Data Bus

IEEE
Institute of Electrical and Electronic Engineers

IETF
Internet Engineering Task Force

IM
Incident Management

INCH
Implementing NTCIP-conformant Hardware

IP
Internet Protocol

IPI
Initial Protocol Identifier

ISO
International Organization for Standardization

ISP
Information Service Provider

ISTEA
Intermodal Surface Transportation Efficiency Act of 1991

ITE
Institute of Transportation Engineers

ITS
Intelligent Transportation Systems

ITSA
Intelligent Transportation Society of America

ITU
International Telecommunications Union

IVHS
Intelligent Vehicle Highway Systems

L – M

LAN
Local Area Network

LCP
Link Control Protocol

LMS
Location and Monitoring Service

LOS
Level of Service

LRMS
Location Reference Message Specification

MCMIS
Motor Carrier Management Information System

MIB
Management Information Base

MMI
Man Machine Interface

MPO
Metropolitan Planning Organization

MS
Message Set

MULTI
Mark-Up Language for Transportation Information

MUTCD
Manual on Uniform Traffic Control Devices

N

NAB
National Association of Broadcasters

NEMA
National Electrical Manufacturers Association

NENA
National Emergency Number Association

NHI
National Highway Institute

NIST
National Institute of Standards and Technology

NTI
National Transit Institute

NHTSA
National Highway Traffic Safety Administration

NRC
National Research Council

NRSC
National Radio Systems Committee

NSF
National Science Foundation

NTCIP
National Transportation Communication for ITS Protocol

NTIA
National Telecommunications and Information Administration

NTSB
National Transportation Safety Board

NTSC
National Television System Committee

O – P

OB
On-board systems

OER
Octet Encoding Rules

OET
Outreach, Education and Training

OSI
Open Systems Interconnection

PCS
Personal Communications Service

PDU
Protocol Data Unit

PER
Packed Encoding Rules

PI
Passenger Information

PICS
Protocol Implementation Conformance Statement

PL
Polling

PMPP
Point-to-MultiPoint Protocol

PPP
Point-to-Point Protocol

PSAP
Primary Safety Answering Point

PT
Paratransit

PTC
Positive Train Control

R

RBDS
Radio Broadcast Data System

RDS
Radio Data System

RFC
Request For Comment

RMC
Ramp Metering Control

ROW
Right-of-Way

RSE
Roadside Equipment

RTCM
Radio Technical Commission for Maritime Services

RWIS
Road Weather Information System (see also ESS)

S

SAE
Society of Automotive Engineers

SAFER
Safety and Fitness Electronic Records

SC
Smart Card

SCH
Scheduling and Runcutting

SCP
Signal Control and Prioritization

SDO
Standards Development Organization

SIA
Security Industry Alliance

SLIP
Serial Line Internet Protocol

SNMP
Simple Network Management Protocol

SNMPv2
Simple Network Management Protocol version 2

SP
Spatial Representation

SSM
Signal System Master

SSR
Standard Speed Rail

STIC
Subcarrier Traffic Information Channel

STMF
Simple Transportation Management Framework

STMP
Simple Transportation Management Protocol

T

TCC
Train Control Center

TCIP
Transit Communications Interface Protocol

TCP
Transmission Control Protocol

TCP/IP
Transmission Control Protocol/Internet Protocol

TEA-21
Transportation Equity Act for the 21st Century (successor to ISTEA)

TFTP
Trivial File Transfer Protocol

TG
Transit Garage Management

TIA
Telecommunications Industry Association

TM
Traffic Management

TMC
Transportation Management Center

TMDD
Traffic Management Data Dictionary

TMIB
Transportation Management Information Base

TMS
Transportation Management System or Traffic Management System

TOC
Transportation Operations Center

TS
Transaction Set

TSC
Transit Standards Consortium

TSP
Transit Signal Priority

TSS
Transportation Sensor System

U – W

UDP
User Datagram Protocol

UDP/IP
User Datagram Protocol/Internet Protocol

USPS
United States Postal Service

VERTIS
Vehicle, Road and Traffic Intelligence Society

VIN
Vehicle Identification Number

VMS
Variable Message Sign

VPAS
Vehicle Proximity Alert System

VRC
Vehicle Roadside Communications

WAN
Wide Area Network

WIM
Weigh In Motion

7.2 Useful ITS Definitions

A

Agent
An STMF entity that receives commands and transmits responses to the received commands.

ANSI
American National Standards Institute, a standardization group that develops or adopts standards for the United States.

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.

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.

ASN.1
Abstract Syntax Notation One, a formal language for describing information to be processed by computer, an ISO standard.

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. Compare with Synchronous.

ATC
Advanced Transportation Controller, transportation field control equipment standards. FHWA, NEMA and the ATC Joint Standards Committee are spearheading the development effort.

ATC Joint Committee
A public/private advisory group composed of ITS experts that guide the development of the ATC.

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.

B

Bandwidth
Indicates the transmission-carrying capacity of a channel. The range of frequencies that can be used for transmitting information on a channel, equal to the difference in Hertz (Hz) between the highest and lowest frequencies available on that channel.

Basic Encoding Rules (BER)
A series of procedures for describing transfer syntax of types specified with ASN.1. Transfer syntax is the actual representation of octets to be sent from one network entity to another. Must be used in conjunction with SNMP.

Baud Rate
The number of discrete signal events per second occurring on a communications channel. It is often interchanged with bits per second (bps), which is technically inaccurate but widely accepted for slower bit rates.

bit
Binary digit. A single basic computer signal consisting of a value of 0 or 1, off or on.

Bit Error Rate (BER)
The number of bits transmitted incorrectly. In digital applications it is the ratio of bits received in error to bits sent.

bps
Bits per second, transmission rate (speed) of data

Bridge
A means for connecting two networks at the data link layer.

Broadcast Address
An address referring to all stations on a medium.

BYTE and UBYTE
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. Octet sized (8 bits) integers where BYTE is signed (range -128 to 127) and UBYTE is unsigned (range 0 to 255).

C

(AB3418) California Assembly Bill No. 3418
A legislative bill that requires all new or upgraded traffic signal controllers installed in California after January 1, 1996, to incorporate a standard communications protocol. California Department of Transportation (Caltrans) has published this specification for developers.

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 of the telephone companies.

Certification
An official recognition awarded by an accredited industry forum asserting that the product meets the stated requirements for conformity to the standards.

Changeable Message Sign
Changeable Message Sign (this terms has 2 common definitions: a.) in NTCIP Objects for Dynamic Message Signs (DMS) [Formally known as TS 3.6], it defines Drum signs, and b.) certain public agencies use this term to describe VMS signs (see NTCIP 1203 for a definition)

Checksum
An arithmetic sum used to verify data integrity.

CHOICE
As defined by ITU-T X.680, Abstract Syntax Notation One Specification of Basic Notation, a choice type is defined by referencing a list of distinct types; each value of the choice type is derived from the value of an object or data element.

Compliance
A determination that an implementation or component subsystem is in strict adherence to (1) usage of standards, that is, conformant, and also (2) in strict adherence to local or project unique requirements. Note that (1) and (2) may be in conflict—in such cases, (2) prevails to achieve a determination of compliance.

Component
The closely related functions of a system. A component produces an information product.

Conformance
A determination that an implementation is in strict adherence to the specific requirements for usage of the features of a standard.

Cyclical Redundancy Check (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.

D

Data
Information before it is interpreted.

Data Dictionary
An organized listing of all data elements (and their characteristics) that are essential to the system, with precise, definitions so that both the user and the system developer will have a common understanding of input, output, components of storage and intermediate calculations.

Data Element
An atomic element of information that is defined within a transit business area. As defined by the *IEEE P1489/D0.0.5* (July 14, 1997), a data element is a syntactically formal representation of some information of interest (such as a fact, proposition, and observation.) about some entity of interest, for example, a person, place, process, property, object, concept, association, state, event. May also be referred to as a data object or object.

Data Flow
The description of information movement and the transforms that are applied as the data moves from input to output.

Data Interface
The connection between two or more components through which information, for example, a data element or message is passed.

Data Link Layer
Layer 2 of the OSI Reference Model; it is responsible for transmission, framing and error control over a single communications link.

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

Dialog
An ordered grouping of messages exchanged between at least two components.

DTE
Data Terminal Equipment. The device that is the originator or destination of the data sent by a modem. (An EIA/TIA – 232 – E signal)

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. (An EIA/TIA – 232 – E signal)

E

EIA/TIA-232-E
Electronic Industries Association/ Telecommunications Industries Association specification that defines the serial port on a PC.

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

F – G

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.

FSK modem interface
Typical method of traffic control system communications, phone line, or twisted wire based.

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.

Gateway
A router and translator between protocols; also, (imprecise usage) an entity responsible for complex topology mappings.

H

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 that causes a copy of sent data to be displayed on the sending display.

HDLC
Generalized network approach: high-level data link control

Highway Advisory Radio (HAR)
Low-powered AM or FM stations that broadcast brief messages to standard car radios from small transmitters placed near highways.

Host
(Internet usage) an end system.

I – J

IETF
Internet Engineering Task Force, a group chartered by the IAB to develop certain RFCs for standardization.

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

Infrastructure
This refers to all fixed components to a transportation system such as rights of way, tracks, equipment, stations, parking/park-n-ride lots, signalization equipment and maintenance facilities.

Informative
Non-prescriptive information that provides context to this standard.

Intelligent Transportation Systems (ITS)
A major national initiative to improve information, communication and control technologies in order to improve the efficiency of surface transportation. Technological innovations that apply direct communications and information processing to improve the efficiency and safety of surface transportation systems. These include on-board navigation for vehicles, emergency communications systems, electronic toll/fare collections, and traffic management centers.

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.

Intermodal Surface Transportation Efficiency Act of 1991 (ISTEA)
Federal authorizing legislation for highways, transit and other surface transportation programs. Established intermodal objectives for national transportation system to achieve efficiency, air quality and environmental quality.

Intermodalism
The use and coordination of more than one mode of transportation.

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

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.*

lAB
Internet Activities Board, group in charge of authorizing RFCs for the purpose of standardizing Internet operations.

IANA
Internet Assigned Numbers Authority, group in charge of assigning Internet addresses.

Internet Protocol (IP)
The network protocol offering a connectionless mode network service in the Internet suite of protocols.

IP address
A 32-bit quantity used to represent a point of attachment in an internet. An Internet Protocol Address.

Internet suite of protocols
A collection of computer-communication protocols originally developed under DARPA sponsorship.

Joint Committee on the NTCIP
A public/private advisory group composed of ITS experts that guide the development of the NTCIP.

L – M

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

LONG and ULONG
Four byte (32 bits) integers where LONG is signed (range –2,147,483,648 to 2,147,483,647) and ULONG is unsigned (range 0 to 4,294,967,295).

Management Information Base (MIB)
A collection of data elements or objects defined using Abstract Syntax Notation One (ASN.1) that can be accessed via a network management protocol. (See Structure of Management Information.)

Manager
The entity that sends commands to entries and processes their responses.

Maximum Transmission Unit (MTU)
The largest amount of user data that can be sent in a single frame on a particular medium.

Message
A grouping of data elements that encapsulate an idea, concept or thing, or convey information. A basic message encapsulates an idea, concept or thing, and a compound message embeds one or more basic messages and other data elements to convey information.

Message Set Catalog
A list of messages and the functional requirements needed to support the exchange of information among components within a system, or between systems.

Message Set Template
The format used to transmit messages among components or between systems.

N

Network
A collection of subnetworks connected by intermediate systems and populated by end systems.

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

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 a network. Usually referring to the management of networking specific devices such as routers. In the context of the NTCIP, refers to all devices including end systems that are present on the network or inter network.

Normative
Prescriptive requirements for the use of this standard.

NTCIP
National Transportation Communication for ITS Protocol, communications protocol under development. FHWA, NEMA and the NTCIP Joint Standards Committee are spearheading the development effort.

NTCIP Home Page
Site on the World Wide Web where one may obtain the latest NTCIP information. The address is www.ntcip.org/

O

Object
A representation of a data element that is managed. The definition of a data element or message including its name, object identifier, description and syntax.

`OBJECT IDENTIFIER`
A unique name (identifier) that is associated with each type of data element in a MIB. This is a defined ASN.1 type. "A value (distinguishable from other such values) that is associated with an object identifier type. A simple type whose distinguished values are the set of all object identifiers allocated in accordance with the rules of [ASN.1]." The number or address by which a data element may be located on the NTCIP or TCIP object tree.

OBJECT-TYPE
The macro defined in RFC-1212 that is the format used to define SNMP objects or data elements. In STMF, the OBJECT-TYPE macro consists of five fields:

Object Name
Syntax
Description
Access
Status.

OCTET
An ordered sequence of eight bits.

OER
Octet Encoding Rules, a variation BER developed for use on low bandwith communications links. OER is based on Octet boundaries (in opposite to PER, which is based on bit boundaries).

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

P

Parity
A simple error detection method used in both communications and computer memory checking to determine character validity.

PER
Packed Encoding Rules, a variation of BER developed for use on low bandwidth communications links, specified in ISO 8825. The original version of NTCIP Simple Transportation Management Framework (NTCIP 1101) [Formally known as TS 3.2] used this term for a transportation industry-specific set of encoding rules that has since been renamed to OER (as defined in NTCIP 1102).

Physical Address
The address of a physical interface.

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

Point-to-Point Protocol (PPP)
Transmission of data between two and only two stations on a Point-to-Point link.

Point-to-MultiPoint Protocol (PMPP)
Transmission of data between multiple stations or nodes. That is, one primary and multiple secondaries.

Port Number
Identifies an application-entry to a transport service in the Internet suite of protocols. The concept of ports are often present in OSI literature, however, ports are not Internet 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.

Primary
A node on a link that controls the polling to and from secondary nodes on that link and controls the communications from the secondary nodes on that link.

Profile
The defined protocol at each of the seven OSI layers. A standard that combines one or more base standards and selects appropriate options or functions within them. (A base standard may be a "standard" or another profile that references standards).

Protocol
A formal set of conventions governing the format and relative timing of message exchange between two communicating processes. A system of rules and procedures governing communications between two devices.

Protocol Data Unit (PDU)
A part of transmitted data that contains information used by the protocol at a particular layer in the OSI stack.

Proxy Agent
A device that receives and responds to network management commands on behalf of another entity.

R – S

RFC
Request for Comments, the name given to correspondence and standards by the IAB.

Router
A level 3 (network layer) relay

Secondary
A node on a link that is controlled by the primary node in terms of polling and communications.

`SEQUENCE` and `SEQUENCE OF`
An ordered record or array (respectively) of data elements or objects. "Types defined by referencing an ordered list of types (some of which may be declared to be optional)"

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.

SHORT and USHORT
Double octet sized (16 bits) integers where SHORT is signed (range -32,768 to 32,767) and USHORT is unsigned (range 0 to 65,535).

Simple Transportation Management Framework (STMF)
Simple Transportation Management Framework describes the organization of the information within devices and the methods of retrieving or modifying any information within the device. STMF also explains how to generate and utilize computer readable information organization descriptions.

Simple Transportation Management Protocol (STMP)
Simple Transportation Management Protocol, a variation of SNMP developed by NEMA to address low bandwidth communication links and real time device monitoring.

SMI
Structure of Management Information, a definition of how to create management data element or objects and a hierarchical (tree like) definition of nodes where management objects or data elements will be attached for unique identification.

SNMP
Simple Network Management Protocol, a communications protocol developed by the IETF, used for configuration and monitoring of network devices.

SNMPv2
Simple Network Management Protocol version 2, recent modification of SNMP that is undergoing evaluation by the Internet community.

Socket
A pairing of IP address and a port number

T

TCIP
Transit Communications Interface Protocol – A subset of NTCIP protocols that is specific to the transit community.

TCP/IP
Transmission Control Protocol/Internet Protocol (protocol addressing both the network and transport layers)

TLV
Tag, Length, Value – the form used in SNMP encoding.

Transaction
See Dialog.

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 Level
The combination of protocols, at the transport layer and below, used in a given context.

U – W

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.

User Datagram Protocol (UDP)
The transport protocol offering a connectionless mode transport service in the Internet suite of protocols.

Wide Area Network (WAN)
Any one of a number of technologies that provide geographically distant transfer.

THIS PAGE LEFT INTENTIONALLY BLANK

Chapter 8

Bibliography

8.1 Selected Reading List

Configuration Management

Implementing Configuration Management, Hardware, Software, and Firmware, Buckley, F.J., IEEE Computer Society Press, Los Alamitos, CA, 1996

Configuration Management Plans: The Beginning of Your CM Solution, Dart, S. and N. Bounds, Carnegie Mellon University, Pittsburgh, Pa., 1998

IEEE Standard for Software Configuration Management Plans, Institute of Electrical and Electronic Engineers (IEEE), IEEE 828-1998, Piscataway, N.J., 1998

Practical Software Configuration Management, The Latenight Developer's Handbook, Mikkelsen, T. and S. Pherigo, Prentice-Hall, Upper Saddle River, N.J., 1997

Spectrum of Functionality in Configuration Management Systems, Software Engineering Institute (SEI), CMU/SEI-90-TR11, SEI, Pittsburgh, PA, 1990

CORBA

CORBA for Dummies, J. Schettino, L. O'Hara, R S. Hohman, IDG Books, 1998

Instant CORBA, R. Orfali, D. Harkey and J. Edwards, et al, John Wiley & Sons, 1997, ISBN 0471183334

CORBA Fundamentals & Programming, J. Siegel, Object Management Group, Inc., 1996

Object-Oriented Systems Design: An Integrated Approach, E. Yourdon, Yourdon Press Computing Systems (Prentice Hall), 1994, ISBN 0136363253

Object Lessons: Lessons in Object-Oriented Development Projects, SIGS Books, 1993, ISBN 0962747734

Network Interfaces

The Ethernet Management Guide, 1995, M. Nemzow, McGraw-Hill, Inc., ISBN 0-07-046380-8

The Token-Ring Management Guide, 1995, M. Nemzow, McGraw-Hill, Inc., ISBN 0-07-046321-2

Object Definition

Understanding SNMP MIBS, 1997, D. Perkins and E. McGinnis, Prentice Hall, Inc., ISBN 0-13-437708-7

ASN.1: The Tutorial & Reference, 1993, D. Steedman, Technology Appraisals Ltd., ISBN 1-871802-06-7

ISO/IEC 8824: Abstract Syntax Notation One (ASN.1) (ITU-T X.680-X.690, 1994

IEEE Std 1488- 1999 IEEE Standard for Message Set Template for Intelligent Transportation Systems, 2000

IEEE Std 1489- 1999 IEEE Standard for Data Dictionaries for Intelligent Transportation Systems, 1999

OSI

The Open Book: A Practical Perspective on OSI, 1990, M.T. Rose, Prentice Hall, Inc.

Understanding OSI, 1994, J. Larmouth, on www.isi.salford.ac.uk//books/osi/osi.html,1997

OSI Network Management

Telecommunications Network Management into the 21st Century, 1994, S. Aidarous and T. Plevyak, IEEE Press, New York, NY

Profiles

Guide to Open System Specifications, European Workshop for Open Systems, 1997

US-DOD Internet Related Standardized Profiles, DISA Internet Librarian, on www-library.itsi.disa.mil/, 1997

SNMP Protocol

SNMP, SNMPv2 and CMIP The Practical Guide to Network Management Standards, 1993, W. Stallings, Addison-Wesley Publishing Company, Inc., ISBN 0-201-63331-0

SNMP, SNMPv2 and RMON, 1996, W. Stallings, Addision-Wesley Publishing Company, Inc., ISBN 0-201-63479-1

Managing Internetworks with SNMP, 1995, M. Miller, M&T Books, ISBN 1-5581-304-3

SNMP: A Guide To Network Management, 1995, S. Feit, McGraw Hill, Inc., ISBN 0-07-020359-8

Systems Engineering

Introduction to Systems Engineering, A. P. Sage, J. E. Armstrong, Jr., Wiley, 2000, ISBN 0-471-02766-9

The Engineering and Design of Systems: Models and Methods, D. M. Buede, Wiley, 2000, ISBN 0-471-28225-1

Systems Engineering Guidebook: A Process for Developing Systems and Products, J. N. Martin, A. T. Bahill, Wiley, 1999, ISBN 0849378370

Systems Engineering: coping with complexity, Jackson, Brook, Stevens, Arnold, Prentice Hall, 1998, ISBN 0130950858

Visualizing Project Management, Forsberg, Mooz, Cotterman, Wiley, 2000, ISBN 047135760

INCOSE Website, references, symposium papers, links to SE organizations on incose.org/

SEI Website, on www.sei.cmu.edu/cmmi/products/models.html, CMMI Systems, Software and Integrated Product Team Capability Maturity Model.

EIA/IS 632, Draft Standard: Processes for Engineering a System

ISO/IEC 15288 System Life Cycle Processes

IEEE 1220-1994, IEEE Trial-Use Standard for Application and Management of the Systems Engineering Process.

EIA/IS 731 (SE-CMM): Systems Engineering Capability Maturity Model, Bate, Roger, et. Al.

IEEE 1362-1998, IEEE Guide for Information – System Definition – Concept of Operations Document.

IEEE 830-1993, IEEE Recommended Practice for Software Requirements Specifications

IEEE 1012-1986, IEEE Standard for Software Verification and Validation Plans

IEEE 1233 - IEEE Guide for Developing System Requirements Specifications

TCP,UDP, IP and PPP Protocols

Internetworking with TCP/IP, 1995, D. Comer, Prentice Hall, Inc., ISBN 0-13-216987-8

TCP/IP: Architecture, Protocols and Implementation, 1993, S. Feit, McGraw Hill, Inc., ISBN 0-07-020346-6

TCP/IP Illustrated, Volume 1, The Protocols, W. R. Stevens, 1994, Addison Wesley Publishing Co.

TCP/IP Illustrated, Volume 2, The Implementation, G. R. Wright and W. R. Stevens, 1995, Addison Wesley Publishing Co.

TCP/IP Tutorial and Technical Overview, International Technical Support Center, Raleigh, NC, 1990, Document Number GC24-3376-01, IBM Corp.

Training Courses

Center to Center Communications, ITS Standards Outreach, Education and Training Program, Institute of Transportation Engineers

Intelligent Transportation Systems (ITS) Software Acquisition, National Highway Institute

Intelligent Transportation Systems (ITS) Procurement, National Highway Institute

ITS Standards Overview, ITS Standards Outreach, Education and Training Program, Institute of Transportation Engineers

Management and Operations of Intelligent Transportation Systems

Using the National ITS Architecture for Deployment, National Highway Institute

National ITS Architecture

The National Architecture for ITS, U.S. Department of Transportation Joint Program Office, 1997

THIS PAGE LEFT INTENTIONALLY BLANK

Chapter 9

Example NTICP Implementations

Several potential NTCIP Implementations are presented in this section as examples of how the various Information, Application, Transport, Subnetwork and Plant Levels may be combined.

The following examples will occasionally refer to legacy terminology such as Class Profiles. Rather than developing a different Class Profile for each possible combination of alternative selections at the various NTCIP *stack* levels, the Joint Committee on the NTCIP has chosen to deprecate the use of alphanumeric class profile designations in lieu of individual standards at each level. The user is now able to create an NTCIP *stack* by selecting the appropriate standards at each Level that is applicable for the application and system design. This approach enables the user to better specify choices specific to the system being deployed.

9.1 Center-to-Field

Two examples are provided for C2F communications.

9.1.1 Example Center-to-Field Implementation Without Routing

Example 9.1 *Example of a C2F Implementation Without Routing*

This example shows one possible implementation of NTCIP C2F communications where routing through an intermediate device is not needed.

Exhibit 9.1 depicts a common example of a C2F NTCIP Implementation where routing through an intermediate device is not needed. In this example, the Transport Level is T2/NULL because there is no need for a routing protocol.

The example NTCIP implementation illustrated in Exhibit 9.1 highlights one implementation subset of the NTCIP Framework. The exhibit shows the standard(s) implemented at each NTCIP Framework Level. The example shows the implementation of both STMP and SNMP at the Application Level and T2/NULL at the Transport Level. Together, these standards provide services for an NTCIP system, such as a traffic signal

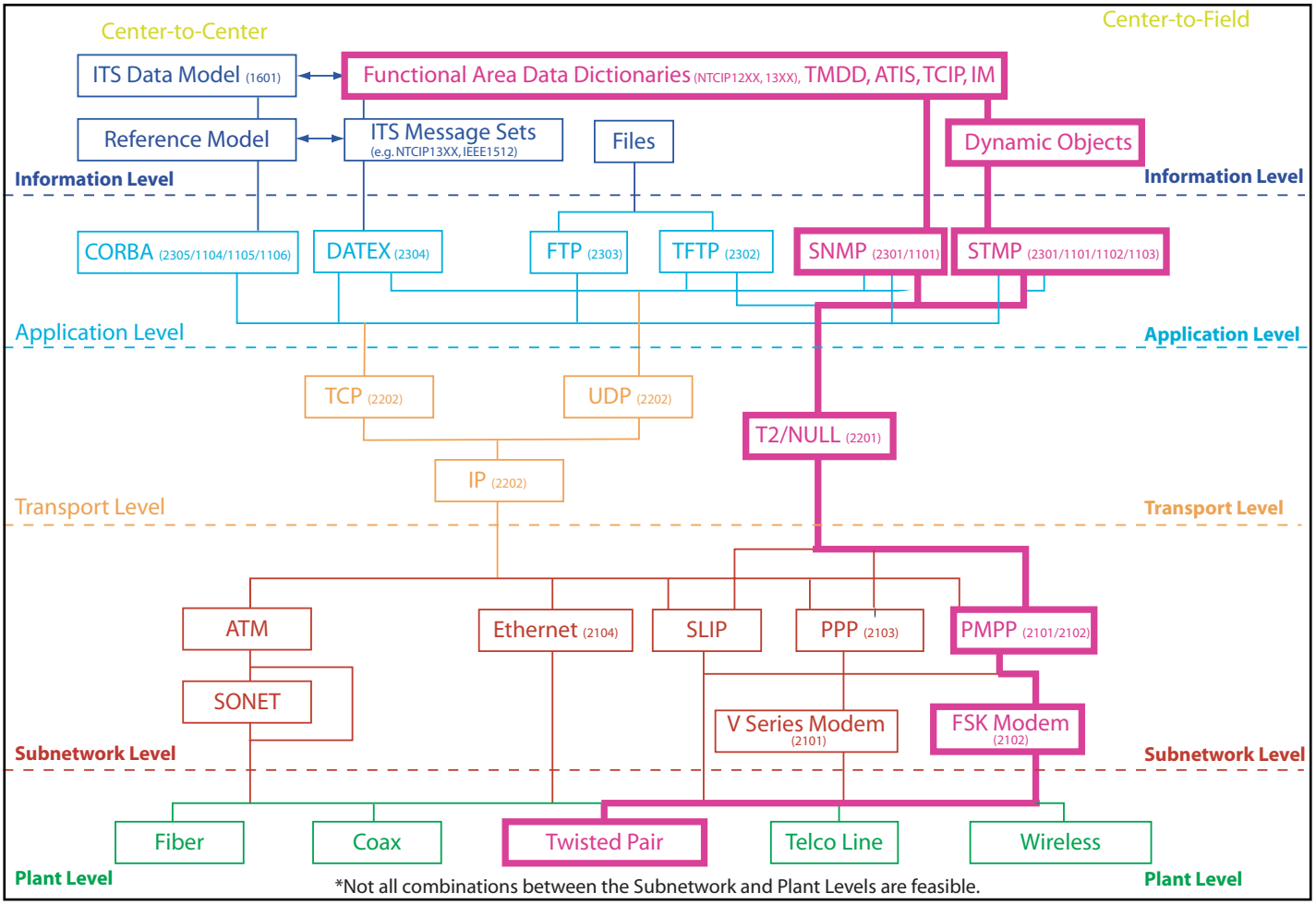


Exhibit 9.1: Example Center-to-Field Implementation with Routing

system, that does not involve routing through intermediate devices. The example shows the selection of both STMP and SNMP at the Application Level within the NTCIP Stack since this will be a common implementation in many systems, such as traffic signal systems, that use dynamic objects.

The implementation subset of the NTCIP Framework shown in this example is similar to that once known as the Class B Profile. It should be noted that the trend is moving away from denoting the various stacks with alphanumeric characters and is moving towards the designation of specific standards at each level within the NTCIP Framework. As a result, Class B should be regarded as a legacy term that will ultimately be abandoned in-lieu of an array of specific NTCIP Framework level standards.

The Subnetwork Level standard selected in this example is Point-to-MultiPoint, FSK modems. The Plant Level in this example NTCIP implementation is shown to be agency owned twisted-pair wire, but any suitable media can be used.

9.1.2 Example Center-to-Field Implementation with Routing

Example 9.2 *Example of a C2F Implementation With Routing*

This example shows one possible implementation of NTCIP C2F communications where routing through one or more intermediate devices is needed.

Exhibit 9.2 depicts a common example of a C2F NTCIP Implementation where routing through an intermediate device is needed. The routing can take either the form of connectionless or connection-oriented transport delivery services depending on the selection at the Transport Level. For connectionless transport delivery services, the selection of User Datagram Protocol over Internet Protocol (UDP/IP) should be made at the Transport Level. For connection-oriented transport delivery services, Transmission Control Protocol over Internet Protocol (TCP/IP) should be selected as the appropriate Transport Level. In other words, TCP establishes a direct connection between the two devices through a handshake arrangement and then proceeds to transmit data with assurance that all messages are received – otherwise the messages are re-transmitted. UDP, on the other hand, uses more of a broadcast approach with no assurance that the message was actually received.

The example NTCIP implementation illustrated in Exhibit 9.2 highlights one implementation subset of the NTCIP Framework. The exhibit shows the standard(s) implemented at each NTCIP Framework Level. The example shows the implementation of both STMP and SNMP at the Application Level and TCP, UDP/IP at the Transport Level. Together, these standards provide services for an NTCIP system, such as a traffic signal system, that involves intermediate routing.

The implementation subset of the NTCIP Framework shown in this example is similar to that once known as the Class C Profile. It should be noted that the trend is moving away from denoting the various stacks with alphanumeric characters and is moving towards the designation of specific standards at each level within the NTCIP Framework. As a result, Class A and Class C should be regarded as a legacy term that will ultimately be abandoned in-lieu of an array of specific NTCIP Framework level standards.

The Subnetwork Level standard selected in this example is Point-to-Point, V-Series modems. The Plant Level in this example NTCIP implementation is shown to be leased line Telco-provided communications.

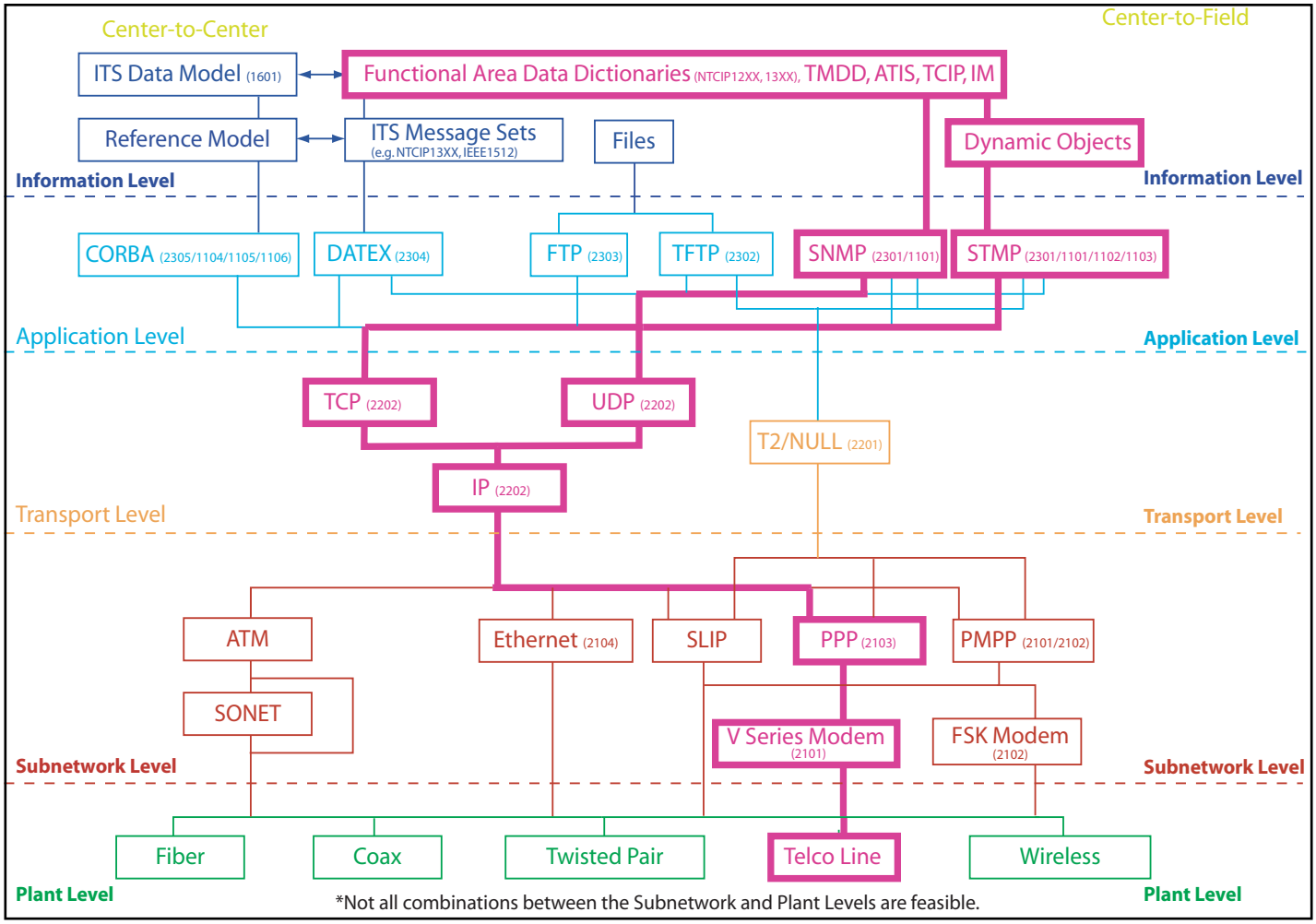


Exhibit 9.2: Example Center-to-Field Implementation without Routing

9.1.3 Example Center-to-Field Implementation With Both Routable and Non-Routable Links

Example 9.3 *Example of a C2F Implementation With Both Routable and Non-Routable Links*

This example shows an implementation of NTCIP C2F communications where both routable and non-routable links are used, such as in the case of a closed-loop traffic signal system.

Exhibit 9.3 depicts a common example of a center-to-field NTCIP Implementation where both routable and non-routable links are needed. This is the classic case of the closed-loop traffic signal system, where the management station (central) dials up the field master and the field master then talks to subordinate controllers using agency owned twisted wire. The routing can take either the form of connectionless or connection-oriented transport delivery services depending on the selection at the Transport Level. For connectionless transport delivery services, the selection of User Datagram Protocol over Internet Protocol

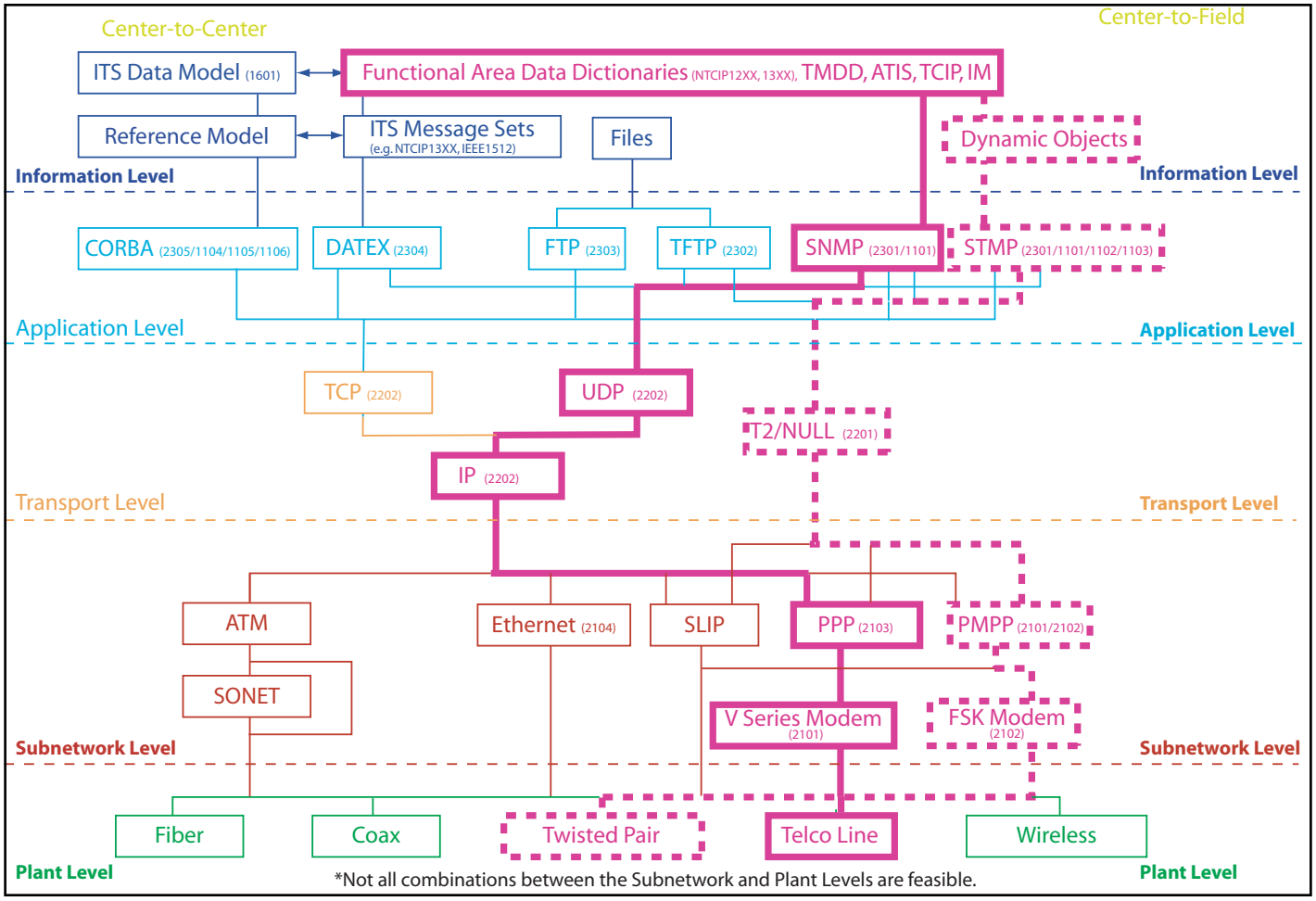


Exhibit 9.3: Example Center-to-Field Implementation with Routable and Non-Routable Links

(UDP/IP) should be made at the Transport Level. For connection-oriented transport delivery services, Transmission Control Protocol over Internet Protocol (TCP/IP) should be selected as the appropriate Transport Level. In other words, TCP establishes a direct connection between the two devices through a handshake arrangement and then proceeds to transmit data with assurance that all messages are received — otherwise the messages are re-transmitted. UDP, on the other hand, uses more of a broadcast approach with no assurance that the message was actually received.

Most closed-loop traffic signal systems use UDP/IP for the dial-up connection from the management station to the field master. Once the dial-up connection is made, the field master will then communicate with subordinate local controllers using a traditional Point-to-MultiPoint and FSK Modem approach.

The example NTCIP implementation illustrated in Exhibit 9.3 highlights an implementation of the NTCIP Framework for a typical closed-loop traffic signal system. The bold lines denote the routable dial-up portion of the communication route. The dashed lines denote the non-routable fixed communications connection. The exhibit shows the standard(s) implemented at each NTCIP Framework Level.

The example shows the implementation of both STMP and SNMP at the Application Level. SNMP is used for the dial-up portion, while STMP is used when dynamic objects are needed for local controllers subordinate to the field master. TCP/IP or UDP/IP is selected for use at the Transport Level for the dial-up connection between the management station and the field master. Together, these standards provide services for an NTCIP system, such as a traffic signal system, that involves intermediate routing. T2/Null is used as the Transport Profile for the non-routable communications portion of the connection between the field master and the subordinate local controllers.

The implementation subset of the NTCIP Framework shown in this example is similar to that once known as the Class C Profile. It should be noted that the trend is moving away from denoting the various stacks with alphanumeric characters and is moving towards the designation of specific standards at each level within the NTCIP Framework. As a result, Class A and Class C should be regarded as a legacy term that will ultimately be abandoned in-lieu of an array of specific NTCIP Framework level standards.

The Subnetwork Level standards selected in this example also depend on whether the routable or non-routable portions are being considered. Point-to-Point and V-Series modems are used when the Plant Level infrastructure is Telco-provided communications, for the dial-up portion of the closed-loop traffic signal system example. Meanwhile, Point-to-MultiPoint and FSK modems are used along with a twisted wire Plant Level for communications between the field master and the local controller.

9.2 Center-to-Center

Two examples are provided for C2C communications.

9.2.1 Example Center-to-Center Implementation using DATEX

Example 9.4 *Example of a Center-to-Center Implementation using DATEX*

This example shows one possible implementation of NTCIP C2C communications using DATEX.

Exhibit 9.4 depicts an example C2C NTCIP implementation and is one variation of an approach using DATEX. This NTCIP implementation example is intended to provide connection-oriented transport delivery services between transportation management centers supporting subordinate field devices.

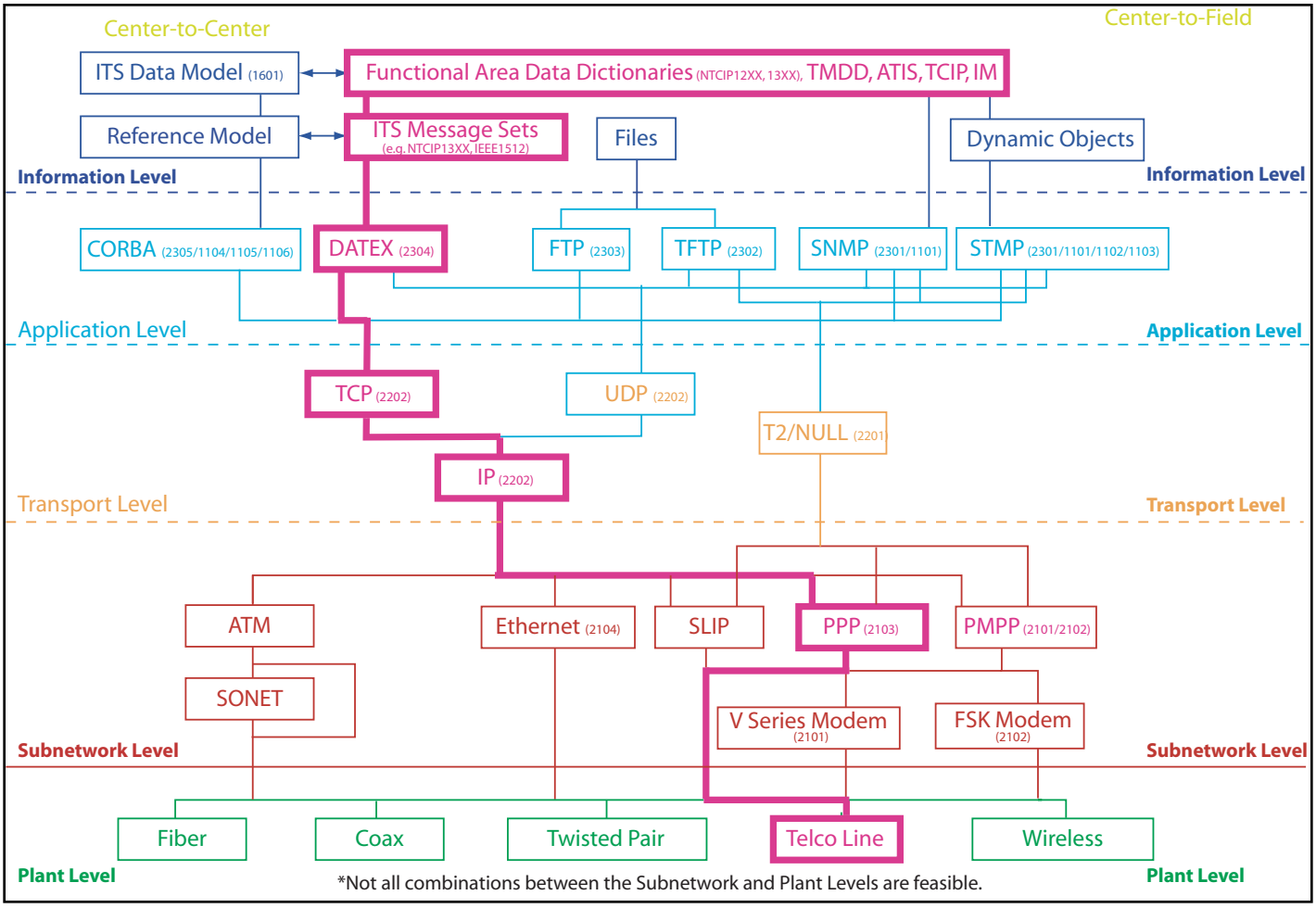


Exhibit 9.4: Example Center-to-Center Implementation with DATEX

The example NTCIP implementation illustrated in Exhibit 9.4 highlights one implementation subset of the NTCIP Framework for C2C communications. The exhibit shows the standard(s) implemented at each NTCIP Framework Level for using DATEX at the Application Level within the NTCIP Framework.

For C2C communications, the choices that are offered at the Application Level include DATEX and CORBA. The choices that are defined for the Transport Level are the User Datagram Protocol over Internet Protocol (UDP/IP) for connectionless transport services and Transmission Control Protocol over Internet Protocol (TCP/IP) for connection-oriented transport delivery services. The Subnetwork Level options include a variety of high bandwidth options, such as ATM, Ethernet and PPP. In this case, an example might be to use Frame Relay with a Point-to-Point Protocol (PPP) at the Subnetwork Level. The Plant Level can include a variety of options such as telco lines, as in this example, or fiber.

9.2.2 Example Center-to-Center Implementation using CORBA

Example 9.5 *Example of a Center-to-Center Implementation using CORBA*

This example shows one possible implementation of NTCIP C2C communications using CORBA.

Exhibit 9.5 depicts an example C2C NTCIP implementation and is one variation of an approach using CORBA. This NTCIP implementation example is intended to provide connection-oriented transport delivery services between transportation management centers supporting subordinate field devices.

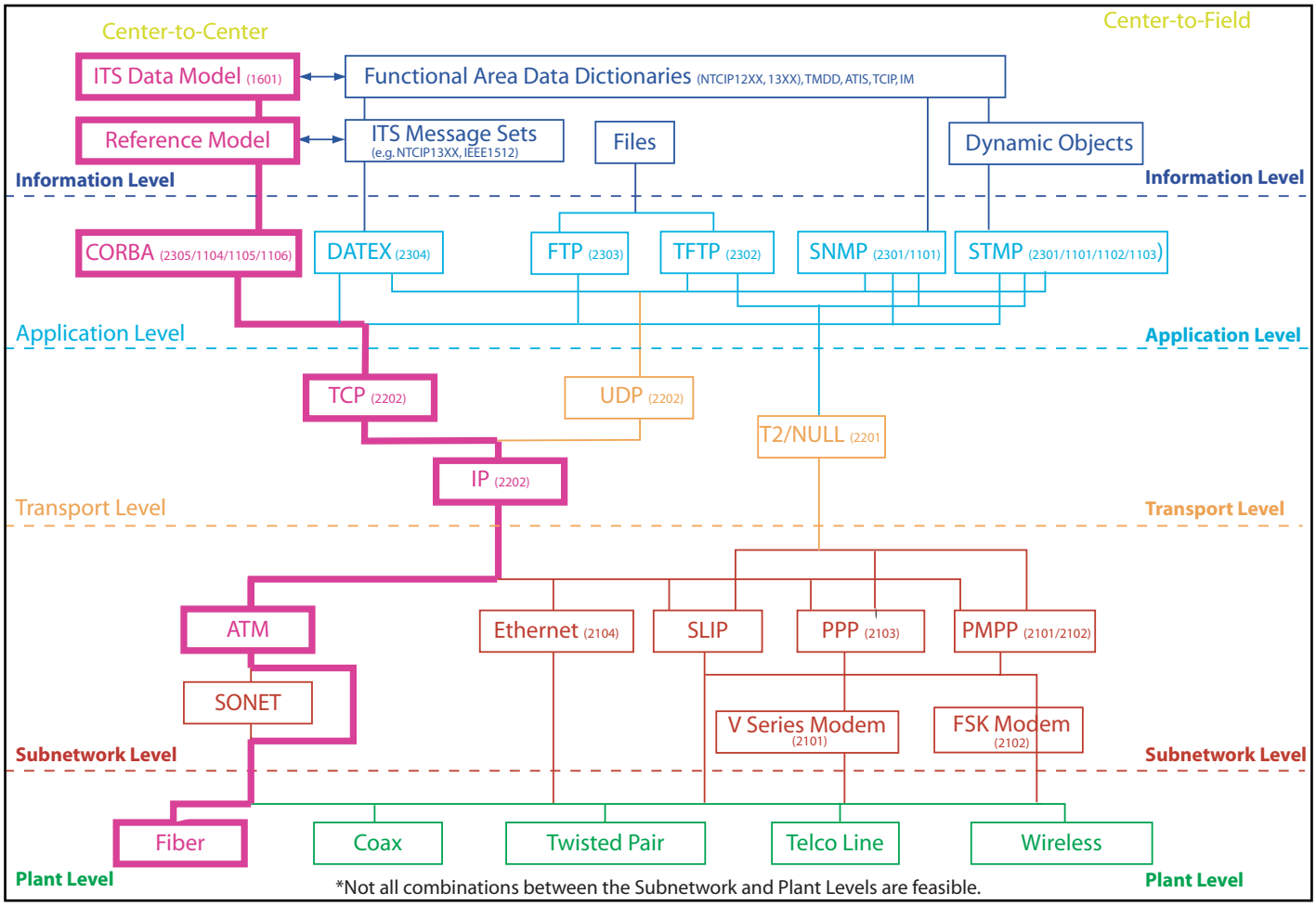


Exhibit 9.5: Example Center-to-Center Implementation with CORBA

The example NTCIP implementation illustrated in Exhibit 9.5 highlights one implementation subset of the NTCIP Framework for C2C communications. The exhibit shows the standard(s) implemented at each NTCIP Framework Level for using CORBA at the Application Level within the NTCIP Framework.

For C2C communications, the choices that are offered at the Application Level include DATEX and CORBA. The choices that are defined for the Transport Level are the User Datagram Protocol over Internet Protocol (UDP/IP) for connectionless transport services and Transmission Control Protocol over Internet Protocol (TCP/IP) for connection-

oriented transport delivery services. The Subnetwork Level options include a variety of high bandwidth options, such as ATM, Ethernet and PPP. In this case, an example might be to use ATM at the Subnetwork Level, although other options might also be appropriate. The Plant Level can include a variety of options such as fiber, as in this example, or telco lines.

THIS PAGE LEFT INTENTIONALLY BLANK

Chapter 10

NTICP Documents

The following list of NTCIP documents is dated March 31, 2002. An updated listing can be obtained by visiting the NTCIP website (www.ntcip.org/library/).

10.1 Listing of NTCIP Documents

Exhibit 10.1: Listing of Current and Planned NTCIP Documents

Number	Old Number	Title	Type	Status
1101	TS 3.2-1996	NTCIP Simple Transportation Mgmt. Framework (STMF)	Base Standard	Published with NEMA cover; Amended
1102	OER	NTCIP Octet Encoding Rules (OER)	Base Standard	Published
1103	STMP	NTCIP Simple Transportation Mgmt. Protocol (STMP)	Base Standard	User Comment Draft
1104	---	NTCIP CORBA Naming Convention Specification	Base Standard	User Comment Draft
1105	---	NTCIP CORBA Security Service Specification	Base Standard	User Comment Draft
1106	---	NTCIP CORBA Near Real-Time Data Service	Base Standard	Proposed Work Item
1201	TS 3.4-1996	NTCIP Global Object (GO) Definitions	Device Data Dictionary	Published with NEMA cover; Amended; version 2 in User Comment Draft
1202	TS 3.5-1996	NTCIP Objects for ASC	Device Data Dictionary	Published with NEMA cover; version 2 in User Comment Draft
1203	TS 3.6-1997	NTCIP Objects for Dynamic Message Signs (DMS)	Device Data Dictionary	Published; Amended; version 2 under development
1204	TS 3.7-1998	NTCIP Objects for Environmental Sensor Systems (ESS)	Device Data Dictionary	Approved by 3 SDOs; Amended; message set (1301) under development
1205	TS 3.CCTV	NTCIP Objects for CCTV Camera Control	Device Data Dictionary	Approved by 3 SDOs
1206	TS 3.DCM	NTCIP Objects for Data Collection and Monitoring. (DCM)	Device Data Dictionary	User Comment Draft
1207	TS 3.RMC	NTCIP Objects for Ramp Meter Control (RMC)	Device Data Dictionary	Recommended Standard; version 2 under development
1208	TS 3.SWITCH	NTCIP Objects for Video Switches	Device Data Dictionary	User Comment Draft
1209	TS 3.TSS	NTCIP Objects for Transportation Sensor Systems (TSS)	Device Data Dictionary	User Comment Draft
1210	---	NTCIP Objects for Signal System Masters (SSM)	Device Data Dictionary	User Comment Draft

Exhibit 10.1: Listing of Current and Planned NTCIP Documents

Number	Old Number	Title	Type	Status
1211	---	NTCIP Objects for Signal Control Priority & HRI (SCP)	Device Data Dictionary	User Comment Draft
1301	---	Weather Report Message Set for ESS	Message Set	Proposed Work Item
1400	TCIP-FRAME	TCIP Framework Standard	Process & Control	Published
1401	TCIP-CPT	TCIP Common Public Transportation (CPT) Objects	Device Data Dictionary	Published
1402	TCIP-IM	TCIP Incident Management (IM) Bus. Area Standard	Device Data Dictionary	Published
1403	TCIP-PI	TCIP Passenger Information (PI) Bus. Area Standard	Device Data Dictionary	Published
1404	TCIP-SCH	TCIP Scheduling/Runcutting (SCH) Bus. Area Standard	Device Data Dictionary	Published
1405	TCIP-SP	TCIP Spatial Representation (SP) Bus. Area Standard	Device Data Dictionary	Published
1406	TCIP-OB	TCIP On-Board (OB) Objects	Device Data Dictionary	Published
1407	TCIP-CC	TCIP Control Center (CC) Objects	Device Data Dictionary	Published
1408	TCIP-FC	TCIP Fare Collection (FC) Objects	Device Data Dictionary	Published
1601	---	CORBA Basic Object Model for TMS	Object Model	Working Group Draft
2001	TS 3.3-1996	NTCIP Class B Profile	Profile - Other	Published with NEMA cover; Amended; to be replaced by NTCIP 2101, 2102, 2201 and 2301
2002	CP-CLA	NTCIP Class A and C Profiles	Profile - Other	Withdrawn
2101	SP-PMPP/RS232	NTCIP SP-PMPP/RS232	Subnet Profile	Approved by 3 SDOs
2102	SP-PMPP/FSK	NTCIP SP-PMPP/FSK	Subnet Profile	Recommended Standard
2103	SP-PPP/RS232	NTCIP SP-PPP/RS232	Subnet Profile	Recommended Standard
2104	SP-Ethernet	NTCIP SP-Ethernet	Subnet Profile	Recommended Standard
2201	TP-Null	NTCIP TP-Null	Transport Profile	Recommended Standard
2202	TP-INTERNET	NTCIP TP-Internet (TCP/IP and UDP/IP)	Transport Profile	Approved by 3 SDOs
2301	AP-STMF	NTCIP AP-STMF	Application Profile	Approved by 3 SDOs
2302	AP-TFTP	NTCIP AP-TFTP	Application Profile	Approved by 3 SDOs
2303	AP-FTP	NTCIP AP-FTP	Application Profile	Approved by 3 SDOs
2304	TS 3.AP-DATEX	NTCIP AP-DATEX-ASN	Application Profile	Recommended Standard
2305	TS 3.AP-CORBA	NTCIP AP-CORBA	Application Profile	Recommended Standard
2500	InP-C2C	NTCIP EP-C2C	Center Information Profile	Withdrawn
2501	InP-DATEX	NTCIP EP-DATEX	Center Information Profile	Proposed Work Item
2502	InP-CORBA	NTCIP EP-CORBA	Center Information Profile	Proposed Work Item
7001	NAN-1	NTCIP Assigned Numbers (NAN) - Part 1	Registry	On-Line Living Document
7002	NAN-2	NTCIP Assigned Numbers (NAN) - Part 2	Registry	Working Group Draft
8001	White Paper	NTCIP Standards Development Process	Process & Control	Recommended Standard

Exhibit 10.1: Listing of Current and Planned NTCIP Documents

Number	Old Number	Title	Type	Status
8002	None	NTCIP Standards Publications Format	Process & Control	Recommended Standard
8003	TS 3.PRO	NTCIP Framework and Classification of Profile	Process & Control	Approved by 3 SDOs
8004	SMI	NTCIP Structure and Ident. of Mgmt. & Info. (SMI)	Process & Control	User Comment Draft
9001	Guide	NTCIP Guide	Information Report	Published; Revision Drafted
9002	None	NTCIP VDOT Case Study on VMS	Information Report	Available; update pending
9003	None	NTCIP WashDOT Case Study on VMS	Information Report	Available; update pending
9004	None	NTCIP Phoenix Case Study on Signal Control	Information Report	Available; update pending
9005	None	NTCIP TxDOT Case Study on DATEX-ASN	Information Report	Project Draft
9006	None	NTCIP Lakewood Case Study on Signal Control	Information Report	Project Draft
9007	None	NTCIP Mesa Case Study on Signal Control	Information Report	Project Draft
9008	None	NTCIP MN DOT Case Study on Environmental Sensor Systems (RWIS)	Information Report	Project Draft
9009	None	NTCIP WA DOT Case Study on Environmental Sensor Systems (RWIS)	Information Report	Project Draft

THIS PAGE LEFT INTENTIONALLY BLANK

Appendix A

Application Areas

Exhibit A.1: Standards Mapped to Application Areas

Document Number	Standard Name	Status March 31, 2002	Center-to-Roadside										Center-to-Center								Vehicle-to-Roadside			Roadside-to-Roadside	
			Traffic Signals	Dyn. Msg. Signs	Video Surveillance	Vehicle Sensors	DataCollection/Monitoring	Weather	Ramp Metering	Incident Mgmt.	Transit	ATIS	ATMS	Maydav	ADMS	HRI	ETC	CVO	ATIS	HRI	CVO (EDI)
NTCIP 1102	BaseStandard:OctetEncoding Rules (OER)	Published	•	•	•	•	•	•	•	•	•	•	•		•	•					
NTCIP 1103	Transportation Management Protocol	User Comment Draft	•	•	•	•	•	•	•		•										
NTCIP 2001	Class B Profile	Approved/Amended/v2 User Comment Draft	•	•	•	•	•	•	•		•										
NTCIP 1101	Simple Transportation Management Framework (STMF)	Approved/Amended	•	•	•	•	•				•										
NTCIP 1104	CORBA Naming Convention	Working Draft								•	•	•	•		•	•					
NTCIP 1105	CORBA Security Service	User Comment Draft								•	•	•	•		•	•					
NTCIP 1106	CORBA Near-Real Time Data Service	Proposed Work Item								•	•	•	•		•	•					
NTCIP 1201	Global Object Definitions	Approved/Amended/v2 User Comment Draft	•	•	•	•	•	•	•												
NTCIP 1202	ObjectDefinitionsforActuated TrafficSignalControllerUnits	Approved/Amended/v2 User Comment Draft	•								•										
NTCIP 1203	ObjectDefinitionsforDynamic Message Signs	Approved/Amended/v2 Working Draft		•																	
NTCIP 1204	Object Definitions for EnvironmentalSensorStations & RWIS	Approved/Amended						•													
NTCIP 1205	Data Dictionary for Closed Circuit Television (CCTV)	Approved			•																
NTCIP 1206	DataCollection&Monitoring Devices	User Comment Draft					•								•						

Exhibit A.1: Standards Mapped to Application Areas

Document Number	Standard Name	Status March 31, 2002	Center-to-Roadside								Center-to-Center								Vehicle-to-Roadside			Roadside-to-Roadside	
			Traffic Signals	Dyn. Msg. Signs	Video Surveillance	Vehicle Sensors	Data Collection/Monitoring	Weather	Ramp Metering		Incident Mgmt.	Transit	ATIS	ATMS	Maydav	ADMS	HRI		ETC	CVO	ATIS	HRI	CVO (EDI)
NTCIP 1207	Ramp Meter Controller Objects	Recommended/v2 Working Draft				•			•														
NTCIP 1208	Object Definitions for Video Switches	User Comment Draft			•																		
NTCIP 1209	Transportation Sensor System Objects	User Comment Draft	•			•	•		•			•											
NTCIP 1210	Objects for Field Management Stations	Working Draft	•	•	•	•	•	•	•			•											
NTCIP 1211	Objects for Signal Control Priority	Working Draft	•									•											
NTCIP 1301	Message Set for Weather Reports	Working Draft						•			•	•	•	•		•					•		
NTCIP 2501	Information Profile for DATEX	Proposed Work Item									•	•	•	•		•	•						
NTCIP 2502	Information Profile for CORBA	Proposed Work Item									•	•	•	•		•	•						
NTCIP 1400	TCIP - Framework Document	Published										•											
NTCIP 1401	TCIP Common Public Transportation (CPT) Business Area Standard	Published										•											
NTCIP 1402	TCIP Incident Management (IM) Business Area Standard	Published									•	•	•	•		•	•				•		
NTCIP 1403	TCIP Passenger Information (PI) Business Area Standard	Published										•											
NTCIP 1404	TCIP-Scheduling/Runcutting (SCH) Business Area Standard	Published										•											
NTCIP 1405	TCIP Spatial Representation (SP) Business Area Standard	Published										•											

Exhibit A.1: Standards Mapped to Application Areas

Document Number	Standard Name	Status March 31, 2002	Center-to-Roadside							Center-to-Center							Vehicle-to-Roadside			Roadside-to-Roadside	
			Traffic Signals	Dyn. Msg. Signs	Video Surveillance	Vehicle Sensors	Data Collection/Monitoring	Weather	Ramp Metering	Incident Mgmt.	Transit	ATIS	ATMS	Mayday	ADMS	HRI	ETC	CVO	ATIS	HRI	CVO (EDI)
NTCIP 1406	TCIP Onboard (OB) Business Area Standard	Published									•										
NTCIP 1407	TCIP Control Center (CC) Business Area Standard	Published								•	•	•	•		•	•					
NTCIP 1408	TCIP Fare Collection (FC) Business Area Standard	Published									•										
NTCIP 2301	Application Profile for Simple Trans Management Framework	Approved	•	•	•	•	•	•	•		•										
NTCIP 2302	Application Profile for Trivial File Transfer Protocol	Approved	•	•	•	•	•	•	•	•	•	•	•		•	•					
NTCIP 2303	Application Profile for File Transfer Protocol (FTP)	Approved	•	•	•	•	•	•	•	•	•	•	•		•	•					
NTCIP 2304	Applications Profile for Data Exchange ASN.1 (DATEX)	Recommended								•	•	•	•		•	•					
NTCIP 2305	Applications Profile for Common Object Request Broker Arch.	Recommended								•	•	•	•		•	•					
NTCIP 2201	TP-Transportation Transport Profile	Recommended	•	•	•	•	•	•	•		•										
NTCIP 2202	Internet (TCP/IP and UDP/IP) Transport Profile	Approved	•	•	•	•	•	•	•	•	•	•	•		•	•					
NTCIP 2101	Point-to-Multi-Point Protocol Using RS-232 Subnetwork Prof.	Approved	•	•	•	•	•				•										
NTCIP 2102	Subnet Profile for PMPP over FSK Modems	Recommended	•	•	•	•	•				•										
NTCIP 2103	Subnet Profile for PPP over RS 232 (Dial-up)	Recommended	•	•	•	•	•	•	•	•	•	•	•		•						
NTCIP 2104	Subnet Profile for Ethernet	Recommended	•	•	•	•	•	•	•	•	•	•	•		•	•					

Exhibit A.1: Standards Mapped to Application Areas

Document Number	Standard Name	Status March 31, 2002	Center-to-Roadside									Center-to-Center								Vehicle-to-Roadside			Roadside-to-Roadside	
			Traffic Signals	Dyn. Msg. Signs	Video Surveillance	Vehicle Sensors	Data Collection/Monitoring	Weather	Ramp Metering	Incident Mgmt.	Transit	ATIS	ATMS	Maryday	ADMS	HRI	ETC	CVO	ATIS	HRI	CVO (EDI)
IEEE 1512.a	Standard for Emergency Management Data Dictionary	Working Draft								•														
IEEE 1512.3	Standard for Hazardous Material IMMS for use by EMCs	Working Draft								•														
IEEE 1512.2	Standard for Public Safety IMMS for use by EMCs	Working Draft								•														
IEEE 1512.1	Standard for Traffic IMMS for use by EMCs	Working Draft								•														
IEEE Std 1512-2000	Standard for Common IMMS for use by EMCs	Published									•													
N/A	Standard Specification for 5.9 GHz Physical Layer	Working Draft															•	•	•					
N/A	Standard Specification for 5.9 GHz Data Link Layer	Working Draft															•	•	•					
ASTM 105-1999	Specification for DSRC Data Link Layer	Published															•	•	•					
ASTM111-200	Specification for DSRC Physical Layer	Published															•	•	•					
ITE 9603-1	ATC Application Program Interface (API)	Recommended									•											•		
ITE 9603-2	ATC Cabinet	Working Draft																				•		
ITE 9603-3	Advanced Transportation Controller (ATC)	Working Draft									•											•		
ITE TM 1.03	Standard for Functional Level TMDD	Working Draft									•					•								
ITE TM 2.01	Message Sets for ETMCC	Approved														•								
SAE J2353	ATIS Data Dictionary	Published										•		•	•				•					

Exhibit A.1: Standards Mapped to Application Areas

Document Number	Standard Name	Status March 31, 2002	Center-to-Roadside								Center-to-Center									Vehicle-to-Roadside			Roadside-to-Roadside	
			Traffic Signals	Dyn. Msg. Signs	Video Surveillance	Vehicle Sensors	DataCollectionMonitoring	Weather	Ramp Metering		Incident Mgmt.	Transit	ATIS	ATMS	Mayday	ADMS	HRI			ETC	CVO	ATIS	HRI	CVO (EDI)
SAE J2354	ATIS Message Set	Published											•		•	•						•		

THIS PAGE LEFT INTENTIONALLY BLANK

Index

B

C

D–E

F–I

L–N

O–P

R–U

THIS PAGE LEFT INTENTIONALLY BLANK