

NTCIP 1210 version v01

National Transportation Communications for ITS Protocol Field Management Stations – Part 1: Object Definitions for Signal System Masters

substitute-RS v01.53 October 2010

This is a pre-standard document, which is distributed for review and ballot purposes only. You may reproduce and distribute this document within your organization, but only for the purposes of and only to the extent necessary to facilitate review and ballot to AASHTO, ITE, or NEMA. Please ensure that all copies include this notice. This pre-standard contains recommended information that is subject to approval. Use this information at your own risk.

Published by

American Association of State Highway and Transportation Officials (AASHTO)

444 North Capitol St., N.W., Suite 249
Washington, D.C. 20001

Institute of Transportation Engineers (ITE)

1627 I ("Eye") Street, NW, Suite 600
Washington, D.C. 20006

National Electrical Manufacturers Association (NEMA)

1300 North 17th Street, Suite 1752
Rosslyn, Virginia 22209-3806

filename 1210v0153.doc

© 2009 AASHTO / ITE / NEMA. All rights reserved.

CONFIGURATION MANAGEMENT of RS
(To be deleted prior to publication)

Reference Status Table

This Document References	Title	Ref Type (Norm, Other)	Dependency Notes	Hold Pending and Status
There are 4 NRs in this document, 1210 v01		Normative		see page 1, Section 1.2.1
NTCIP 1103 v02.14c	TMP	Normative		No Hold. 1103 v02 was Jointly Approved in June 2010. JA version was v02.16b. In Oct 2010, JJ editing 1103 v02.17 for publication.
NTCIP 1201 v03.07d	GO	Normative	last dependent NR in queue; OK for SDO balloting of 1210 in June 2010 or later.	May 2010, 1201 v03.13a sent via B0136 for SDO ballot and approval. NEMA approved; waiting for AASHTO and ITE approval. In Oct 2010, JJ has in pub editing. [no HOLD]
NTCIP 1202 v02.18	ASC	Normative		In Jan 2007, 1202 v02.19 PDF was posted for download. In Apr 2007, 1202 v02.19, Nov 2005 edition, published in hardcopy. [update 1210 ref to v02.19]
IAB STD 17		Normative		No hold

Recent Minor Version Revision History

revision	DATE	NOTE new on top
V01.53	10/1/2010	NEMA staff editing; accepted all changes.
v01.52	3/19/2009	JC approved substitution of v01.52 for previously accepted RS. File edited by ConSysTec.

This Document's Colophon and Metadata

Created and edited with: Microsoft® Office Word 2003 SP3.
32 bit application on OS Windows XP Pro SP3.
File type: Microsoft Word 97-2003 document.

Page Layout:

Different odd and even; odd on right. Header has 2 lines by fore-edge; Footer © next to gutter.
[Pending format conversion to Same odd and even, per NS_1 for primary use with PDF.]

Format >> Styles and Formatting >> inventory: 70 Styles as of 10/01/2010
Heading Styles: Heading 1 (as chapter head), to Heading 4
Heading Annex Styles: Annex A only

Nine Levels of MS Word TOC Styles:

Insert >> Reference >> Index and Tables >> Table of Contents >> mapping: 2

Hyperlink use:

Insert >> Reference >> Cross-references >> used for: TOC page numbers; no figures; no section heading reference.

Text production notes: only keyboard entry or Edit Paste Special; no imports.

Figure production notes: none.

Original figure author(s), application(s), and file type(s): none.

File quality notes:

Open >> Open and Repair >> [date last Repaired, number of errors]: 10/8/2010, one.

(To be deleted prior to publication)

NOTICES

Copyright Notice

Version 01 © 2007 and © 2008 by the American Association of State Highway and Transportation Officials (AASHTO), the Institute of Transportation Engineers (ITE), and the National Electrical Manufacturers Association (NEMA). All intellectual property rights, including, but not limited to, the rights of reproduction, translation and display are reserved under the laws of the United States of America, the Universal Copyright Convention, the Berne Convention, and the International and Pan American Copyright Conventions. Except as licensed or permitted, you may not copy these materials without prior written permission from AASHTO, ITE, or NEMA. Use of these materials does not give you any rights of ownership or claim of copyright in or to these materials.

Visit www.ntcip.org for other copyright information, for instructions to request reprints of excerpts, and to request reproduction that is not granted below.

PDF File License Agreement

To the extent that these materials are distributed by AASHTO / ITE / NEMA in the form of an Adobe® Portable Document Format (PDF) electronic data file (the "PDF File"), AASHTO / ITE / NEMA authorizes each registered PDF File user to view, download, copy, or print the PDF File available from the authorized Web site, subject to the terms and conditions of this license agreement:

- a) you may download one copy of each PDF File for personal, noncommercial, and intraorganizational use only;
- b) ownership of the PDF File is not transferred to you; you are licensed to use the PDF File;
- c) you may make one more electronic copy of the PDF File, such as to a second hard drive or burn to a CD;
- d) you agree not to copy, distribute, or transfer the PDF File from that media to any other electronic media or device;
- e) you may print one paper copy of the PDF File;
- f) you may make one paper reproduction of the printed copy;
- g) any permitted copies of the PDF File must retain the copyright notice, and any other proprietary notices contained in the file;
- h) the PDF File license does not include (1) resale of the PDF File or copies, (2) republishing the content in compendiums or anthologies, (3) publishing excerpts in commercial publications or works for hire, (4) editing or modification of the PDF File except those portions as permitted, (5) posting on network servers or distribution by electronic mail or from electronic storage devices, and (6) translation to other languages or conversion to other electronic formats; and
- i) other use of the PDF File and printed copy requires express, prior written consent.

Data Dictionary and MIB Distribution Permission

To the extent that these materials are distributed by AASHTO / ITE / NEMA in the form of a Data Dictionary ("DD") or Management Information Base ("MIB"), AASHTO / ITE / NEMA extend the following permission:

You may make or distribute unlimited copies, including derivative works, of the DD or MIB, including copies for commercial distribution, provided that:

- i) each copy you make or distribute contains the citation "Derived from NTCIP 0000 [insert the document number]. Used by permission of AASHTO / ITE / NEMA.";
- ii) the copies or derivative works are not made part of the standards publications or works offered by other standards developing organizations or publishers or as works-for-hire not associated with commercial hardware or software products intended for field implementation;
- iii) use of the DD or MIB is restricted in that the syntax fields may be modified only to reflect a more restrictive subrange or enumerated values;

- iv) the description field may be modified but only to the extent that: (a) only those bit values or enumerated values that are supported are listed; and (b) the more restrictive subrange is expressed.

These materials are delivered “AS IS” without any warranties as to their use or performance.

AASHTO / ITE / NEMA and their suppliers do not warrant the performance or results you may obtain by using these materials. AASHTO / ITE / NEMA and their suppliers make no warranties, express or implied, as to noninfringement of third party rights, merchantability, or fitness for any particular purpose. In no event will AASHTO / ITE / NEMA or their suppliers be liable to you or any third party for any claim or for any consequential, incidental or special damages, including any lost profits or lost savings, arising from your reproduction or use of these materials, even if an AASHTO / ITE / NEMA representative has been advised of the possibility of such damages.

Some states or jurisdictions do not allow the exclusion or limitation of incidental, consequential, or special damages, or the exclusion of implied warranties, so the above limitations may not apply to a given user.

Use of these materials does not constitute an endorsement or affiliation by or between AASHTO, ITE, or NEMA and the user, the user's company, or the products and services of the user's company.

If you are unwilling to accept the foregoing restrictions, you should immediately return these materials.

PRL and RTM Distribution Permission

To the extent that these materials are distributed by AASHTO / ITE / NEMA in the form of a Profile Requirements List (“PRL”) or a Requirements Traceability Matrix (“RTM”), AASHTO / ITE / NEMA extend the following permission:

- i) you may make or distribute unlimited copies, including derivative works of the PRL (then known as a Profile Implementation Conformance Statement (“PICS”)) or the RTM, provided that each copy you make or distribute contains the citation “Based on NTCIP 0000 [insert the document number] PRL or RTM. Used by permission. Original text © AASHTO / ITE / NEMA.”;
- ii) you may only modify the PRL or the RTM by adding text in the Project Requirements column, which is the only column that may be modified to show a product's implementation or the project-specific requirements;
- iii) you may only modify the PRL or the RTM by adding additional table columns or table rows that are clearly labeled as ADDITIONAL for project-unique or vendor-unique features; and
- iv) if the PRL or RTM excerpt is made from an unapproved draft, add to the citation “PRL (or RTM) excerpted from a draft document containing preliminary information that is subject to change.”

This limited permission does not include reuse in works offered by other standards developing organizations or publishers, and does not include reuse in works-for-hire, compendiums, or electronic storage devices that are not associated with procurement documents, or commercial hardware, or commercial software products intended for field installation.

A PICS is a Profile Requirements List which is completed to indicate the features that are supported in an implementation. Visit www.ntcip.org for information on electronic copies of the MIBs, PRLs, and RTMs.

Content and Liability Disclaimer

The information in this publication was considered technically sound by the consensus of persons engaged in the development and approval of the document at the time it was developed. Consensus does not necessarily mean that there is unanimous agreement among every person participating in the development of this document.

AASHTO, ITE, and NEMA standards and guideline publications, of which the document contained herein is one, are developed through a voluntary consensus standards development process. This process brings together volunteers and/or seeks out the views of persons who have an interest in the topic covered by this publication. While AASHTO, ITE, and NEMA administer the process and establish rules to promote fairness in the development of consensus, they do not write the document and they do not

independently test, evaluate, or verify the accuracy or completeness of any information or the soundness of any judgments contained in their standards and guideline publications.

AASHTO, ITE, and NEMA disclaim liability for any personal injury, property, or other damages of any nature whatsoever, whether special, indirect, consequential, or compensatory, directly or indirectly resulting from the publication, use of, application, or reliance on this document. AASHTO, ITE, and NEMA disclaim and make no guaranty or warranty, express or implied, as to the accuracy or completeness of any information published herein, and disclaims and makes no warranty that the information in this document will satisfy any of your particular purposes or needs. AASHTO, ITE, and NEMA do not undertake to guarantee the performance of any individual manufacturer or seller's products or services by virtue of this standard or guide.

In publishing and making this document available, AASHTO, ITE, and NEMA are not undertaking to render professional or other services for or on behalf of any person or entity, nor are AASHTO, ITE, and NEMA undertaking to perform any duty owed by any person or entity to someone else. Anyone using this document should rely on his or her own independent judgment or, as appropriate, seek the advice of a competent professional in determining the exercise of reasonable care in any given circumstances. Information and other standards on the topic covered by this publication may be available from other sources, which the user may wish to consult for additional views or information not covered by this publication.

AASHTO, ITE, and NEMA have no power, nor do they undertake to police or enforce compliance with the contents of this document. AASHTO, ITE, and NEMA do not certify, test, or inspect products, designs, or installations for safety or health purposes. Any certification or other statement of compliance with any health or safety-related information in this document shall not be attributable to AASHTO, ITE, or NEMA and is solely the responsibility of the certifier or maker of the statement.

Trademark Notice

NTCIP is a trademark of AASHTO / ITE / NEMA. All other marks mentioned in this document are the trademarks of their respective owners.

ACKNOWLEDGEMENTS

This publication was prepared by the NTCIP Field Master Stations Working Group, which is a subdivision of the Joint Committee on the NTCIP. The Joint Committee is organized under a Memorandum of Understanding among the American Association of State Highway and Transportation Officials (AASHTO), the Institute of Transportation Engineers (ITE), and the National Electrical Manufacturers Association (NEMA). The Joint Committee on the NTCIP consists of six representatives from each of the standards organizations, and provides guidance for NTCIP development.

At the time that this document was prepared, the following individuals were active members of the NTCIP Field Management Stations Working Group:

- Robert Betts
- John Black
- Al Bonificio
- Rick Denney (Chair)
- Robert De Roche
- Bud Kent
- Kai Leung
- Andy Mao
- Greg Mizell
- Ken Montgomery
- Saeed Nowkhasteh
- Peter Ragsdale
- Guillermo Ramos
- Joerg Rosenbohm
- Jo Versavel

Other individuals providing input to the document include:

- Ralph Boaz
- Jack Brown
- Jeff Brummond
- Patrick Chan
- Blake Christie
- Gary Duncan
- Bruce Eisenhart
- Jim Forbes
- Craig Gardner
- Curtis Gobeli
- Curtis Herrick
- David McKinley
- John Michael
- Amrish Raj
- David Richie
- Mike Shea
- Ray Starr
- Warren Tighe
- Ken Vaughn
- Jeris White

In addition to the many volunteer efforts, recognition is also given to those organizations which supported the efforts of the working group by providing comments and funding for the document, including:

- U.S. Department of Transportation, Research and Innovative Technology Administration
- AASHTO
- Caltrans
- Consensus Systems Technologies
- Econolite Control Products
- Florida Department of Transportation
- G.C. Herrick and Associates
- Georgia Department of Transportation
- Harris County
- ITE
- Iteris
- McCain Traffic Supply, Inc.
- Ministry of Transportation, Ontario
- Minnesota Department of Transportation
- Naztec, Inc.
- NEMA
- New York State DOT
- Noblis
- Peek Traffic Systems
- Pillar Consulting
- Robert De Roche Consulting
- Siemens ITS
- Southwest Research Institute
- SRF Consulting Group, Inc.
- Telvent Farradyne
- Texas Department of Transportation
- Washington State Department of Transportation

FOREWORD

This document defines the management information for a Signal System Master (SSM). It defines individual parameters that represent the configuration, status, and control information that is unique to SSMS. It also defines specific groupings of these parameters and others to address the operational configuration, monitoring, and control of the device in a baseline system configuration.

This document is an NTCIP Device Data Dictionary Standard and an Information Profile standards publication. Device Data Dictionaries Standards formally express management information in terms of objects (data elements, data frames, and messages) for use within NTCIP systems. Information Profiles reference one or more object definition, data dictionary, and/or message set standards to fully describe the information level requirements of a device.

For more information about NTCIP standards, visit the NTCIP Web site at <http://www.ntcip.org>.

User Comment Instructions

The term "User Comment" includes any type of written inquiry, comment, question, or proposed revision, from an individual person or organization, about any part of this standard publication's content. A "Request for Interpretation" of this standard publication is also classified as a User Comment. User Comments are solicited at any time. In preparation of this NTCIP standards publication, input of users and other interested parties was sought and evaluated.

All User Comments will be referred to the committee responsible for developing and/or maintaining this standards publication. The committee chairperson, or their designee, may contact the submitter for clarification of the User Comment. When the committee chairperson or designee reports the committee's consensus opinion related to the User Comment, that opinion will be forwarded to the submitter. The committee chairperson may report that action on the User Comment may be deferred to a future committee meeting and/or a future revision of the standards publication. Previous User Comments and their disposition may be available for reference and information at www.ntcip.org.

A User Comment should be submitted to this address:

NTCIP Coordinator
National Electrical Manufacturers Association
1300 North 17th Street, Suite 1752
Rosslyn, Virginia 22209-3801
e-mail: ntcip@nema.org

A User Comment should be submitted in the following form:

Standard Publication number and version:

Page:

Section, Paragraph, or Clause:

Comment:

Editorial or Substantive?:

Suggested Alternative Language:

Please include your name, organization, and address in your correspondence.

Approvals

This standards publication was separately balloted and approved by AASHTO, ITE, and NEMA after recommendation by the Joint Committee on the NTCIP. Each organization has approved this standard as the following standard type, as of the date:

AASHTO – Standard Specification; monthHere 2010
ITE – Software Standard; monthHere 2010
NEMA – Standard; monthHere 2010

History

The following is the development history of NTCIP 1210:

NTCIP 1210 v01 — the UCDs. The FMS WG started drafting the NTCIP 1210 in the year 2000. Two User Comment Drafts were accepted by the NTCIP Joint Committee — the first UCD, version v01.14, was accepted in December 2001, and the second UCD, version v01.46, was accepted in August 2007. Because of the number of user comments on the first UCD, the document was greatly revised by adding Systems Engineering content. The additional content included a Signal System Master Concept of Operations, user needs, and requirements. With the minor version numbering reaching v01.40, the FMS WG added in the dialogs and objects to the draft, which satisfied the ConOps and fulfilled the requirements. Traceability was provided by the PRL and RTM.

NTCIP 1210 v01 — the Recommended Standard. April 2008, v01.47 disposed of the second round of User Comments. In May 2008, the v01.48 proposed Recommended Standard was submitted to the NTCIP Joint Committee for acceptance. In May 2008, the NTCIP Joint Committee accepted v01.48 as the Recommended Standard. However, in August 2008, the JC had extended discussion on the approach to resolve quality issues. Planning for a quality audit ensued.

NTCIP 1210 v01 — the substitute Recommended Standard. In December 2008, a Walkthrough Exercise of NTCIP 1210 v01.49 was conducted for logical consistency and traceability. In January thru March 2009, the decisions from the Walkthrough Exercise were posted, the MIB checked, and tracing quality checked in several minor versions ~v01.51. In March 2009, the 1210 MIB was reported to compile with no errors. Also in March 2009, the NTCIP Joint Committee approved the substitution of v01.52 as the Recommended Standard.

NTCIP 1210 v01 — ballot and Joint Approval. In 2009, the normative reference dependency of “same or higher status” delayed issuance of NTCIP 1210 v01 until after NTCIP 1201 v03, *Global Object Definitions*, was sent for balloting and approval. In May 2010, the normative reference hold was removed, and NTCIP 1210 v01.53 was edited for SDO balloting and approval. NTCIP 1210 v01.54 was edited for publication.

INTRODUCTION

This publication defines the management information related to a Signal System Master (SSM). SSM management information includes individual parameters that represent the configuration, status, and control information of such a device. It also includes predefined message sets of these parameters and others from different standards to address the operational and informational exchanges between the devices in a baseline system configuration. The parameters and message sets are collectively referred to as objects. The objects are defined using several ASN.1 Macros that were initially developed for use with Internet information management. The macros have been modified to include additional information specific to NTCIP and ITS Data Dictionaries and Message Sets.

This standard defines requirements that are applicable to an NTCIP environment that involves the control of traffic signal controllers. While the term Signal System Master implies some type of physical device, many of the data concepts are applicable to any logical implementation. By definition, a SSM operates in the context of a "system" that includes traffic signal controllers and office, computer-based traffic management center software. It, therefore, imposes requirements on both of these "system" components, as well.

This document defines requirements that are applicable to all NTCIP environments and also contains optional and conditional clauses that are applicable to specific environments for which they are intended.

The following keywords apply to this document: AASHTO, ITE, NEMA, NTCIP, FMS, and SSM.

In 1992, the NEMA 3-TS Transportation Management Systems and Associated Control Devices Section began development of the NTCIP. The NEMA Transportation Section's purpose was in response to user needs to include standardized systems communication in the NEMA TS 2 standard, *Traffic Controller Assemblies*. Under the guidance of the Federal Highway Administration's NTCIP Steering Group, the NEMA effort was expanded to include the development of communications standards for all transportation field devices that could be used in an Intelligent Transportation Systems (ITS) network.

In September 1996, an agreement was executed among AASHTO, ITE, and NEMA to jointly develop, approve, and maintain the NTCIP standards. The Joint Committee on the NTCIP formed the Field Master Working Group to define a common set of management information related to roadside devices that act in supervisory capacity. The first meeting of the working group was in February 2000. The WG name was subsequently changed to Field Management Stations WG (FMS WG).

After considering all functionality that could be considered appropriate to a field master, the FMS WG developed a work plan based upon a two-part standard. The initial part, *Object Definitions for Signal System Masters*, addresses the information and operational requirements of traditional "closed-loop" systems. A second part is envisioned to address requirements of an advanced "field management station" that go beyond signal controllers to include such devices as dynamic message signs, environmental system sensors, CCTV camera controllers, and ramp metering controllers.

TABLE OF CONTENTS

	Page
Section 1 GENERAL [INFORMATIVE]	1
1.1 Scope	1
1.2 References.....	1
1.2.1 Normative References.....	1
1.2.2 Other References	2
1.2.3 Contact Information	4
1.3 Terms	4
1.4 Abbreviations and Acronyms	6
1.5 SSM Object Tree.....	7
Section 2 CONCEPT OF OPERATIONS [NORMATIVE]	8
2.1 Tutorial [Informative]	8
2.2 Current Situation and Problem Statement [Informative]	11
2.3 Reference Physical Architecture.....	12
2.3.1 Remote Signal System.....	13
2.3.2 Hierarchical Distributed Signal System	14
2.3.3 Operational Policies and Assumptions.....	14
2.4 Architectural Needs.....	14
2.4.1 Provide Live Data	15
2.4.2 Provide Off-Line Logged Data.....	15
2.4.3 Connect Communications Networks	15
2.4.4 Support Legacy Communications Networks	15
2.5 Features	16
2.5.1 Manage SSM.....	16
2.5.2 Manage SSLs.....	21
2.6 Security	22
2.7 Relationship of User Needs to National ITS Architecture Flows [Informative].....	22
2.8 Operational Scenarios [Informative].....	23
2.8.1 Remote Signal System, Low-Speed Communications.....	23
2.8.2 Hierarchical Distributed Signal System on Low-Speed Infrastructure	24
2.8.3 Hierarchical Distributed Signal System with High-Speed Communications.....	24
Section 3 FUNCTIONAL REQUIREMENTS [NORMATIVE]	25
3.1 Tutorial	25
3.2 Protocol Requirements List.....	25
3.2.1 User Needs Column	26
3.2.2 Requirements Column.....	26
3.2.3 Conformance Column	26
3.2.4 Support Column	27
3.2.5 Instructions for Completing the PRL	27
3.2.6 Protocol Requirements List (PRL) Table.....	28
3.3 Operational Environment Requirements.....	35
3.3.1 Support Basic Communications	35
3.3.2 Support Logged Event Data	36
3.3.3 Manage Access.....	36
3.4 Data Exchange Requirements.....	36
3.4.1 Collect System Detector Data	37
3.4.2 Manage the SSM Configuration	37
3.4.3 Manage the System Timing Plans.....	38
3.4.4 Monitor the SSM Operation.....	41

Section 4 DIALOG SPECIFICATIONS [NORMATIVE]	43
4.1 Simple Network Management Protocol (SNMP)	43
4.1.1 Generic SNMP Get Interface	43
4.1.2 Generic SNMP Get Next Interface	44
4.1.3 Generic SNMP Set Interface	44
4.1.4 Variable Binding List Structure	45
4.1.5 Additional Requirements	46
4.2 Dialogs	47
4.2.1 Configure Sensor Source and Volume/Occupancy Period	48
4.2.2 Configure Section and Intersection Information in SSM	48
4.2.3 Timing Plans	49
4.2.4 Configure SSM Timekeeping	49
4.2.5 Configure Schedule Plan Selection	49
4.2.6 Configure Traffic Responsive Plan Selection	50
4.2.7 Engage Plan Selection	53
4.2.8 Synchronize the SSL Time-of-Day Clocks	53
4.2.9 Synchronize the SSL Coordination by SSM Direct Command	54
4.2.10 Set Block Data	54
4.2.11 Get Block Data	54
4.2.12 Monitor the SSM Operation	54
4.2.13 Pass-Through Interface Dialog	56
4.2.14 Configure SSM to SSL Command and Polling Interface	56
4.2.15 Determine Current Configuration and Capabilities of Event Logging Service	57
4.2.16 Configure Event Logging Service	57
4.2.17 Retrieve Event Logged Data	58
4.2.18 Clear Event Log	58
4.2.19 Determine Security Configuration	58
4.2.20 Security Configuration	59
4.2.21 Engage Timing Plan in the SSL by SSM Direct Command	59
4.2.22 TMS Plan Selection Override For Each Section	59
Section 5 SIGNAL SYSTEM MASTER OBJECT DEFINITIONS [NORMATIVE]	60
5.1 Section Setup	62
5.1.1 Maximum Sections	62
5.1.2 Section Setup Table	62
5.2 Intersection Setup	64
5.2.1 Maximum Number of Intersections	65
5.2.2 Intersection Setup Table	65
5.3 Command Setup	67
5.3.1 Maximum Commands	67
5.3.2 Command Table	67
5.4 Message Object Identifiers	71
5.4.1 Max Message OID Pairs	71
5.4.2 SSM Message OID Table	72
5.5 TMP Message Setup	75
5.5.1 TMP Maximum Messages	76
5.5.2 TMP Maximum Message Variables	76
5.5.3 TMP Message Setup Table	76
5.6 TMP Message Configuration	84
5.6.1 TMP Message Configuration Table	84
5.7 PMPP Routing	85
5.7.1 Maximum Messages Routed	86
5.7.2 SSL Message Routed Table	86
5.8 Intersection Status	90
5.8.1 Intersection Status Table	90

5.9	Control Mode.....	95
5.9.1	Control Mode Table.....	96
5.10	System Re-Sync.....	106
5.10.1	System Re-Sync Control.....	107
5.10.2	Max SSM Patterns.....	107
5.10.3	Pattern Cycle Length Table.....	107
5.11	SSM TimeBase.....	108
5.11.1	Maximum Timebase SSM Actions.....	108
5.11.2	Maximum Timebase SSM Action Tasks.....	109
5.11.3	Timebase SSM Action Table.....	109
5.12	Sensor Source.....	112
5.12.1	Maximum Sensor Sources.....	113
5.12.2	Sensor Data Table.....	113
5.13	SSM Volume Occupancy Configuration.....	119
5.13.1	SSM Volume Occupancy Table.....	119
5.14	Detector Group Configuration.....	120
5.14.1	Detector Group Configuration Table.....	121
5.14.2	Detector Group Output Table.....	124
5.15	Detector Configuration.....	125
5.15.1	Maximum Detectors Per Group.....	125
5.15.2	Detector Configuration Table.....	126
5.16	Computational Channel Detector Group.....	127
5.16.1	Computational Channel Detector Group Configuration Table.....	127
5.16.2	Threshold Comparator Channel Input Output Table.....	129
5.17	Threshold COS Matrix.....	133
5.17.1	Maximum Levels Cycle.....	133
5.17.2	Maximum Levels Split.....	133
5.17.3	Maximum Levels Offset.....	134
5.17.4	Levels To Output Table.....	134
5.18	Auxiliary Channels Output.....	136
5.18.1	Auxiliary Queue, Occupancy, and Non-Arterial Levels.....	136
5.18.2	Auxiliary Queue Output Matrix Table.....	137
5.18.3	Auxiliary Occupancy Output Matrix Table.....	139
5.18.4	Auxiliary Non-Arterial Output Matrix Table.....	141
5.19	Transfer Threshold Levels.....	142
5.19.1	Transfer Thresholds Table.....	143
5.20	Signature Configuration.....	149
5.20.1	Maximum Signatures.....	149
5.20.2	Maximum Signature Detectors.....	150
5.20.3	Signature Configuration Table.....	150
5.21	Signature Historical Data.....	153
5.21.1	Signature Historical Data Table.....	153
5.22	Signature Sample.....	155
5.22.1	Signature Sample Configuration Table.....	155
5.22.2	Signature Match Table.....	156
5.22.3	Signature Weighting Configuration Table.....	157
5.23	Unit Parameters.....	158
5.23.1	Algorithm Support.....	158
5.23.2	Backup Time Parameter.....	159
5.24	Algorithm Update and Control.....	159
5.24.1	Algorithm Update and Control Table.....	159
5.25	SSM Block Objects.....	161
5.25.1	SSM Block Get Control.....	161
5.25.2	SSM Block Data.....	162
5.25.3	SSM Block Error Status.....	163

Section 6 SSM BLOCK OBJECT DEFINITIONS [NORMATIVE]	164
6.1 Block Data Type & ID	164
6.2 SSM Section Setup Block	165
6.2.1 SSM Section Setup Block Example	166
6.3 SSM Intersection Setup Block	166
6.3.1 SSM Intersection Setup Block Example	166
6.4 SSM Command Sequence Block	167
6.4.1 SSM Command Sequence Block Example	168
6.5 SSM Message Object Identifier Block	168
6.5.1 SSM Message Object Identifier Block Example	169
6.6 SSM TMP Message Setup Block	169
6.6.1 TMP Message Setup Block Example	170
6.7 TMP Message Configuration Block	170
6.7.1 TMP Message Configuration Block Example	171
6.8 TMP Message Configuration Status Block	171
6.8.1 TMP Message Configuration Status Block Example	172
6.9 SSM Control Mode Block	172
6.9.1 SSM Control Mode Block Example	173
6.10 SSM Pattern Cycle Length Block	173
6.10.1 SSM Pattern Cycle Length Block Example	174
6.11 SSM Timebase Schedule Block	174
6.11.1 SSM Timebase Schedule Block Example	175
6.12 SSM Timebase Day Plan Block	175
6.12.1 Day Plan Block Example	176
6.13 SSM Timebase Action Block	177
6.13.1 SSM Timebase Action Block Example	177
6.14 SSM Sensor Source Block	178
6.14.1 SSM Sensor Source Block Example	179
6.15 SSM Volume Occupancy Configuration Block	179
6.15.1 SSM Volume Occupancy Configuration Block Example	179
6.16 SSM Detector Group Configuration Block	180
6.16.1 SSM Detector Group Configuration Block Example	180
6.17 SSM Detector Configuration Block	181
6.17.1 SSM Detector Configuration Block Example	182
6.18 SSM Comp Chan Detector Group Configuration Block	183
6.18.1 SSM Comp Chan Detector Group Configuration Block Example	183
6.19 SSM Threshold COS Matrix Block	184
6.19.1 SSM Threshold COS Matrix Block Example	185
6.20 SSM Aux Queue Channel Override Block	186
6.20.1 SSM Aux Queue Channel Override Block Example	187
6.21 SSM Aux Occup Channel Override Block	187
6.21.1 SSM Aux Occup Channel Override Block Example	188
6.22 SSM Aux Non-Arterial Channel Override Block	188
6.22.1 SSM Aux Non-Arterial Channel Override Block Example	189
6.23 SSM Transfer Thresholds Block	190
6.23.1 SSM Transfer Thresholds Block Example	190
6.24 SSM Algorithm Control Block	191
6.24.1 SSM Algorithm Control Block Example	192
6.25 SSM Signature Configuration Block	192
6.25.1 SSM Signature Configuration Block Example	193
6.26 SSM Signature Historical Block	193
6.26.1 SSM Signature Historical Block Example	194
6.27 SSM Signature Sample Block	195
6.27.1 SSM Signature Sample Block Example	195

6.28	SSM Signature Weighting Block	196
6.28.1	SSM Signature Weighting Block Example	197
6.29	SSM Miscellaneous Data Block	197
6.29.1	SSM Miscellaneous Data Block Example	198
6.30	SSM Event Class Block	198
6.30.1	SSM Event Class Block Example	199
6.31	SSM Event Config Block	199
6.31.1	SSM Event Config Block Example	200
6.32	SSM Dynamic Object Config Block	200
6.32.1	SSM Dynamic Object Config Block Example	201
6.33	SSM Dynamic Object Owner Block	202
6.33.1	SSM Dynamic Object Owner Block Example	202
6.34	SSM Dynamic Object Status Block	202
6.34.1	SSM Dynamic Object Status Block Example	203
6.35	SSM Watch Object Definition Block	203
6.36	SSM Watch Object Status Block	203
6.37	SSM Watch Block Definition Block	203
6.38	SSM Watch Block Status Block	204
6.39	SSM Report Object Configuration Block	204
6.40	SSM Report Object Status Block	204
6.41	SSM Report Block Definition Block	204
6.42	SSM Report Block Status Block	204
6.43	SSM Trap Management Block	204
6.44	SSM Trap Management Status Block	204
6.45	SSM Daylight Saving Block	204
6.45.1	SSM Daylight Saving Block Example	205

**ANNEX A REQUIREMENTS TRACEABILITY MATRIX, SSM DEVICE AND INFORMATION PROFILE
REQUIREMENTS LIST 207**

ANNEX B SSM DEVICE AND INFORMATION PROFILE 221

B.1	Introduction	221
B.2	NOTATION	221
B.2.1	TYPE SYMBOLS	221
B.3	Section Setup Group	221
B.4	Intersection Setup Group	222
B.5	Command Setup Group	222
B.6	Message Group	223
B.6.1	Message Object Identifier Group	223
B.6.2	TMP Message Setup Group	223
B.6.3	TMP Message Configuration Group	223
B.7	PMPP Routing Group	224
B.8	Intersection Status Group	224
B.9	Control Mode Group	225
B.10	System Resync Group	226
B.11	Timebase Group	226
B.11.1	Global Timebase Group	226
B.11.2	SSM Timebase Group	227
B.12	Threshold Algorithm Group	227
B.12.1	Sensor Source Group	228
B.12.2	Volume Occupancy Configuration Group	228
B.12.3	Detector Group Configuration Group	228
B.12.4	Detector Configuration Group	229
B.12.5	Computational Channel Detector Group	229
B.12.6	Threshold COS Matrix Group	230

B.12.7	Auxiliary Channels Output Group	230
B.12.8	Transfer Threshold Levels Group	230
B.12.9	Algorithm Update and Control Group	231
B.13	Signature Algorithm Group	231
B.13.1	Signature Configuration Group	231
B.13.2	Signature Historical Data Group	232
B.13.3	Signature Sample Group	232
B.14	Unit Parameters Group	232
B.15	Block Object Group	232
B.16	Global Configuration Group	233
B.17	Database Management Group	234
B.18	Report Group	234
B.19	PMPP Group	235
B.20	SNMP Group	235
B.21	System Group	236
B.22	SFMP Group	236
B.23	STMP Group	236
B.24	Logical Name Group	237
B.25	Security Group	237
B.26	RS232 Group	238
B.27	HDLC Group	238
B.28	Interfaces Group	239
B.29	IP Group	240
B.30	ICMP Group	241
B.31	TCP Group	241
B.32	UDP Group	242
B.33	Ethernet Group	242
B.34	PPP Table	243
B.35	Dialog Table	243
ANNEX C - SSM CONTROL HIERARCHY		245
C.1	SSM Section Pattern Control Hierarchy	245
C.2	SSM Section Special Function Control Hierarchy	246

Section 1 GENERAL [INFORMATIVE]

1.1 Scope

This document defines requirements related to the Information Level communications interface between a management station and a signal system master (SSM). This is achieved through the presentation of the user needs for such an interface in Section 2 with detailed functional requirements presented in Section 3.

This standard includes references to the communications interface between the SSM and a Signal System Local (SSL). However, the standardized definition of that interface is provided in other standards such as NTCIP 1202 v02.

This standard only addresses a subset of the requirements required for procurement. It does not address requirements related to the accuracy of readings, hardware components, mounting details, etc.

This standard standardizes the communications interface by identifying the various operational needs of the users and subsequently identifying the requirements that must be supported for each need. A summary of the conformance requirements are provided in Annex A through a traceability matrix.

1.2 References

For approved amendments, contact:

NTCIP Coordinator
National Electrical Manufacturers Association
1300 North 17th Street, Suite 1752
Rosslyn, VA 22209-3801
fax: (703) 841-3331
e-mail: ntcip@nema.org

Draft amendments, which are under discussion by the relevant NTCIP Working Group, and amendments recommended by the NTCIP Joint Committee are available on the World Wide Web at <http://www.ntcip.org>.

1.2.1 Normative References

The following standards contain provisions, which, through references in this text, constitute provisions of NTCIP 1210. By reference herein, these standards are adopted, in whole or in part as indicated, in this publication. At the time of publication, the editions indicated were valid. All standards are subject to revision, and parties to agreements based on NTCIP 1210 are encouraged to investigate the possibility of applying the most recent editions of the standards listed below.

Identifier	Title	Summary
IAB STD 17	(RFC 1213) <i>Management Information Base for Network Management of TCP/IP-based internets: MIB-II</i> , March 1991	RFC 1213 defines the second version of the Management Information Base (MIB-II) for use with network management protocols in TCP/IP-based internets.

Identifier	Title	Summary
NTCIP 1103 v02.17	<i>Transportation Management Protocols</i> Jointly Approved in June 2010; published in July 2010	NTCIP 1103 v02 defines the protocols used to exchange information between management systems and most field devices. NOTE—NTCIP 1103 v02 is a normative reference in NTCIP 2301 v02, which is also an Other Reference in this NTCIP 1210 v01 standard.
NTCIP 1201 v03.13a	<i>NTCIP Global Object Definitions</i> Recommended Standard submitted for balloting and approval in May 2010	NTCIP 1201 v03 defines data elements that are used by multiple types of devices (e.g., signs, sensor stations, signals, etc.). Many of these objects, such as time and scheduling objects, are referenced by this NTCIP 1210 v01 standard in order to satisfy user needs.
NTCIP 1202 v02.19	<i>NTCIP Object Definitions for Actuated Traffic Signal Controller Units</i> November 2005 edition	NTCIP 1202 v02 defines data elements that are used for the management of a traffic signal controller.

1.2.2 Other References

The following documents and standards may provide the reader with a more complete understanding of the entire protocol and the relations between all parts of the protocol. However, these documents do not contain direct provisions that are required by NTCIP 1210. At the time of publication, the editions indicated were valid. All standards are subject to revision, and parties to agreements based on NTCIP 1210 are encouraged to investigate the possibility of applying the most recent editions of the standard listed below.

Identifier	Title	Summary
IAB STD 16	(RFC 1155) <i>Structure and Identification of Management Information for TCP/IP based Internets</i> , M. Rose, K. McCloghrie, May 1990, (RFC 1212) <i>Concise MIB Definitions</i> , M. Rose and K. McCloghrie, March 1991	IAB STD 16 defines the generic format for defining an SNMP Management Information Base (MIB). The NTCIP standards have further refined this in NTCIP 8004.
RFC 1157	(RFC 1157) <i>Simple Network Management Protocol (SNMP)</i> . JD Case, M. Fedor, ML Schoffstall, C. Davin, May 1990.	RFC 1157 defines the protocol by which management information for a network element may be inspected or altered by logically remote users.
NEMA TS 2–2003	<i>Traffic Controller Assemblies with NTCIP Requirements</i> reaffirmed (R2008)	NEMA TS 2 provides a definition of the hardware and functional requirements of a traffic signal controller.

Identifier	Title	Summary
NTCIP 2101 v01.20	<i>Communications for ITS Protocol Point to Multi-Point Protocol Using RS-232 Subnetwork</i>	NTCIP 2101 is in the subnetwork level of the NTCIP communications framework. The subnetwork level standards define rules and procedures for exchanging data between two entities over particular communications media and interface with the plant level or physical communications infrastructure. This subnetwork standard defines the point-to-multi-point protocol using RS-232.
NTCIP 2102 v01.10	<i>Communications for ITS Protocol Point to Multi-Point Protocol Using FSK Modem Subnetwork</i>	NTCIP 2102 is in the subnetwork level of the NTCIP communications framework. The subnetwork level standards define rules and procedures for exchanging data between two entities over particular communications media and interface with the plant level or physical communications infrastructure. This subnetwork standard defines the point-to-multi-point protocol using FSK Modem communications media.
NTCIP 2103 v02.06	<i>Communications for ITS Protocol Point to Point Protocol Over RS-232 Subnetwork Profile</i>	NTCIP 2103 is in the subnetwork level of the NTCIP communications framework. The subnetwork level standards define rules and procedures for exchanging data between two entities over particular communications media and interface with the plant level or physical communications infrastructure. This subnetwork standard defines the point-to-point protocol using RS-232,
NTCIP 2201 v01.14	<i>Transportation Transport Profile (T2)</i>	NTCIP 2201 defines a specialized, low-bandwidth transport mechanism for exchanging data.
NTCIP 2202 v01.05b	<i>Transport Profile for Internet (TCP/IP and UDP/IP)</i>	NTCIP 2202 defines how the NTCIP community uses the TCP/IP and UDP/IP standards.
NTCIP 2301 v02.12	<i>NTCIP – Simple Transportation Management Framework (STMF) Application Profile</i>	NTCIP 2301, as restricted by NTCIP 1210, defines the mechanisms by which the data defined in NTCIP 1210 is exchanged.
NTCIP 8004 v02.04a	<i>Structure and Identification of Management Information</i>	NTCIP 8004 defines and explains the structure used by the NTCIP effort to document data definitions.
OMG Unified Modeling Language Specification, Version 1.5	OMG Unified Modeling Language Specification, Object Management Group, 2003	The standard that formally defines the meaning of each symbol used in the UML diagrams contained in this standard. However, as these diagrams are informational, this standard is not normative.
FHWA-SA-95-032	<i>Traffic Control Systems Handbook</i> , FHWA, 1995.	This book describes the overall concepts related to the operation of traffic signals, among other devices.

1.2.3 Contact Information

1.2.3.1 NEMA Standards

Copies of NEMA standards may be obtained from:

National Electrical Manufacturers Association
1300 North 17th Street, Suite 1752
Rosslyn, VA 22209

1.2.3.2 NTCIP Standards

Copies of NTCIP standards may be obtained from:

NTCIP Coordinator
National Electrical Manufacturers Association
1300 North 17th Street, Suite 1752
Rosslyn, Virginia 22209-3801
fax: (703) 841-3331
e-mail: ntcip@nema.org

1.2.3.3 Internet Documents

Electronic copies of RFC documents may be obtained electronically from:

Internet Architecture Board
<http://www.rfc-editor.org/>
<http://www.ietf.org/rfc.html>
<http://www.rfc-editor.org/repositories.html>

1.3 Terms

For the purposes of this standard, the following terms, definitions, acronyms, and abbreviations apply. Electrical and electronic terms not defined in this clause are used in accordance with their definitions in IEEE Std 100-2000. English words not defined in this clause or in IEEE Std 100-2000 are used in accordance with their definitions in *Webster's New Collegiate Dictionary*.

TERM	DEFINITION
Application Profile	A standard that defines subsets or combinations of base standards used to provide specific functions and services covering the application, presentation, and session layers of the OSI Basic Reference Model.
Controller Assembly	A complete electrical device mounted in a cabinet for controlling the operation of a traffic control signal display(s).
Controller Unit	A portion of a controller assembly that is devoted to the selection and timing of signal displays.
Coordination	The control of controller units in a manner to provide a relationship between specific green indications at adjacent intersections in accordance with a time schedule to permit continuous operation of groups of vehicles along the street at a planned speed.
Data Element	A single unit of data, such as a name or a serial number.
Database	The assemblage of data constraints and parameters used by computer algorithms in the execution of the traffic control function. Normally included are timing parameters, adjustment coefficients, algorithm coefficients, limit parameters, etc.

TERM	DEFINITION
Field Computer	A host computing platform that is used to temporarily manage one SSM and its SSLs. This is typically a laptop computer used by maintenance personnel.
Information Profile	A standard that defines subsets or combinations of base standards used to provide the definition of information that are related to specific functions and services.
Interchangeability	A condition which exists when two or more items possess such functional and physical characteristics as to be equivalent in performance and durability, and are capable of being exchanged one for the other without alteration of the items themselves, or adjoining items, except for adjustment, and without selection for fit and performance (National Telecommunications and Information Administration, U.S. Department of Commerce).
Internet	A large collection of connected networks running the Internet suite of protocols.
Interoperability	The ability of two or more systems or components to exchange information and use the information that has been exchanged (IEEE Std. 610.12-1990: IEEE Standard Glossary of Software Engineering Terminology).
Level Selection	See Threshold Selection
Network	A collection of communications capable devices that are logically connected through more than one subnetwork.
Network Layer	That portion of an OSI Basic Reference Model (Layer 3) responsible for data transfer across the network, independent of both the media comprising the underlying subnetworks and the topology of those subnetworks.
Occupancy	A measurement of vehicle presence within a zone of detection, expressed in percent of time, a given point, or area is occupied by a vehicle. In this standard, the text “normalized occupancy” and “weighted occupancy” are used to indicate modified values of the collected occupancy the SSM calculates using fixed or variable factors defined herein.
Pattern	See Timing Pattern.
Pattern-Recognition	See Signature Selection.
Plan	See Timing Plan.
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.
Section	A group of SSLs under the same logical control and on the same physical channel.
Signal System Local	A device that is being controlled and monitored by a SSM. A Signal System Local (SSL) could be an Actuated Signal Controller, Pre-timed Controller, Ramp Meter Controller, or other device that is part of the signal system.
Signal System Master	That portion of a field management station dealing with SSL coordination.
Signature Selection	Also known as Pattern-Recognition, Signature Selection is a traffic responsive plan selection method based on a user-determined detection signature or pattern. This signature is based on the sum of weighted volumes and weighted occupancy for a series of system detectors.
Special Function	An unassigned SSL circuit that is controlled primarily by a SSM or Traffic Management Center.
System Owner	The owner or operator of the signal system being managed.

TERM	DEFINITION
Threshold Selection	Also known as Level Selection, Threshold Selection is a traffic responsive plan selection method based on a comparison of weighted system detector readings to user-defined thresholds.
Timing Pattern	A unique set of coordination parameters that define how a traffic signal controller will operate in order to provide coordinated operation with other traffic signal controllers. Each timing pattern includes a cycle length, which is typically the same as the section cycle length; a split defining the amount of time allocated to each phase; an offset indicating when the first coordinated phase green occurs in relation to the section zero point; and an indication of the sequence of phases within the cycle.
Timing Plan	A specific set of rules that define how a section of SSLs operate together. The section timing plan is associated with a specific timing pattern for each SSL. The section timing plan may also be associated with a nominal cycle length, although individual SSLs may use different cycle lengths (e.g., SSLs may double cycle). A timing plan may also activate special functions within specific SSLs in order to activate special features, such as no left turn signs.
Traffic Management System	A computer system used by the system owner to manage the SSM. In this standard, the Traffic Management System may be a host computing platform in a Traffic Management Center, or a Field Computer.
Transport Profile	A standard that defines subsets or combinations of base standards used to provide specific functions and services covering the transport and network layers of the OSI Basic Reference Model.
Volume	The number of vehicles passing a given point in a specific period of time. In this standard, the text “normalized volume” and “weighted volume” are used to indicate modified values of the collected volume the SSM calculates using fixed or variable factors defined herein.

1.4 Abbreviations and Acronyms

The abbreviations and acronyms used in this Standard Publication are defined as follows:

AASHTO	American Association of State Highway and Transportation Officials
IAB STD	Internet Architecture Board Standard
IEEE	Institute of Electrical and Electronics Engineers
IP	Internet Protocol
ISO	International Organization for Standardization
ITE	Institute of Transportation Engineers
ITS	Intelligent Transportation Systems
MIB	Management Information Base
NEMA	National Electrical Manufacturers Association
NTCIP	National Transportation Communications for ITS Protocol
OSI	Open Systems Interconnection
PICS	Protocol Implementation Conformance Statement

PRL	Profile Requirements List
RFC	Request for Comments
RS	Roadway Subsystem
SNMP	Simple Network Management Protocol
SSL	Signal System Local
SSM	Signal System Master
STMF	Simple Transportation Management Framework
STMP	Simple Transportation Management Protocol
T2	Transportation Transport Profile
TCP	Transmission Control Protocol
TMC	Traffic Management Center
TMS	Traffic Management System or Traffic Management Subsystem
TOD	Time-Of-Day
UDP	User Datagram Protocol
WG	Working Group

1.5 SSM Object Tree

The *Object Definitions for Signal System Master* uses the International Organization for Standardization (ISO) global naming tree to uniquely identify all management information (object definitions). It also references numerous objects in the Actuated Traffic Signal Controller (ASC) and Global subtrees of the global naming tree. SSM objects definitions are registered under the ssm node in the ISO naming tree. The relevant organization of the SSM node is as follows:

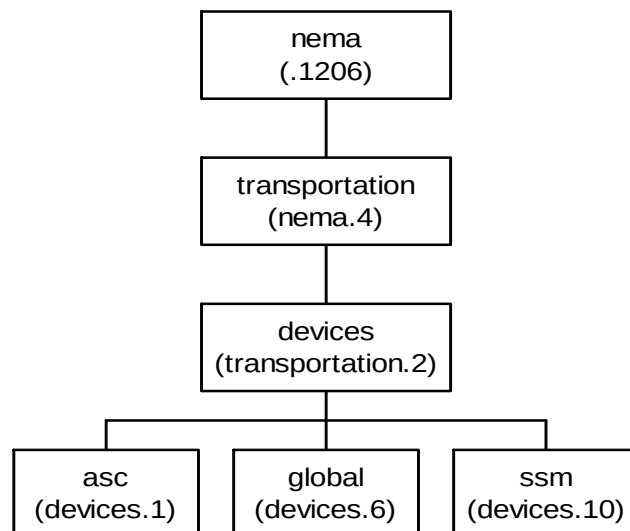


Figure 1 Naming Tree

Section 2 **CONCEPT OF OPERATIONS** **[NORMATIVE]**

Section 2 defines the user needs that are used to derive the functional requirements presented in Section 3. Accepted system engineering processes detail that requirements should only be developed to satisfy well-defined user needs. The first stage in this process is to identify the ways in which the system will be used. In the case of NTCIP 1210, this entails identifying the various architectural needs that are typically associated with SSMs and the features that are frequently desired.

This concept of operations provides the reader with:

- a) A detailed description of the scope of NTCIP 1210;
- b) An explanation of how a SSM is expected to fit into the larger context of an ITS network;
- c) A starting point in the procurement process; and
- d) An understanding of the perspective of the designers of the standard.

This document section is intended for all readers of the document, including:

- a) Transportation operations managers
- b) Transportation operations personnel
- c) Transportation engineers
- d) System integrators
- e) Device manufacturers

The first three categories of readers will find this document section useful in order to understand the standard services potentially offered by a SSM. For this audience, this document section serves as the starting point in the procurement process. They will be able to become familiar with each feature covered by the standard and determine whether that feature is appropriate for their implementation. If it is, then their procurement specification will need to require support for the feature and all of the mandatory requirements related to that feature.

The last two categories of readers will find this document section useful in order to gain a more thorough understanding as to why the more detailed requirements and design elements exist and how they relate to each other through traceability.

2.1 Tutorial [Informative]

A concept of operations describes a proposed system from the users' perspective. Typically, a concept of operations is used on a project to ensure that the system developers understand the users' needs. Within the context of NTCIP standards it is used to document the intent of each feature for which the standard supports a communications interface. It also serves as the starting point for users to select which features may be appropriate for their project.

The concept of operations starts with a discussion of the current situation and problems that have led to the need to deploy systems covered by the scope of the standard and to the development of the standard itself. This discussion should be presented in layman's terms such that both the potential users of the system and the system developers can understand and appreciate the situation.

The concept of operations then documents key aspects about the proposed system, including the:

- a) Reference architecture – The reference architecture defines the overall context of the proposed system and defines which specific interface is addressed by this standard. The reference architecture may be supplemented with one or more sample physical architectures that describe how the reference architecture may be realized in an actual deployment.
- b) Organizational policies that should be considered.
- c) Architectural Needs – The operational environment defines how data may be exchanged across the communications interface.

- d) Features – The features identify and describe the various functions that users may want the device to perform. These features are derived from the high level user needs identified in the problem statement but are refined and organized into a more manageable structure that form the basis of the traceability tables contained in Section 3.

The operational environment and features are collectively called the *user needs*. Section 3 uses these user needs in the analysis of the system in order to define the various functional requirements of a SSM. A conformant device may support other user needs, as long as they are conformant with the requirements of this standard and the standards it references (i.e., NTCIP 2301 and NTCIP 8004). For example, a device may support data that has not been defined by this standard; however, when exchanged via one of the NTCIP 2301 protocols, the data must be properly registered with a valid OBJECT IDENTIFIER under the Global ISO Naming Tree.

NOTE: Off-the-shelf interoperability and interchangeability can only be obtained by using well documented user needs, along with their corresponding requirements and design that are broadly supported by the industry as a whole. Designing a system that uses environments or features not defined in a standard or not typically deployed in combination with one another will inhibit the goals of interoperability and interchangeability, especially if the documentation of these user needs is not available for distribution to system integrators. The standards allow implementations to support additional user needs in order to support innovation, which is constantly needed within the industry; but users should be aware of the risks involved with using such environments or features.

The user needs are presented in a hierarchical fashion, starting out with high level concepts and then becoming more specific. In some cases, the specific user need may be fairly obvious, but in other cases, the reason a user need may exist may be less obvious. As a result, the presentation of user needs is accompanied with a UML activity diagram that depicts under what conditions a user need may be required. The diagram itself is informational, but the text explaining the diagram is normative. An example activity diagram is provided in Figure 2.

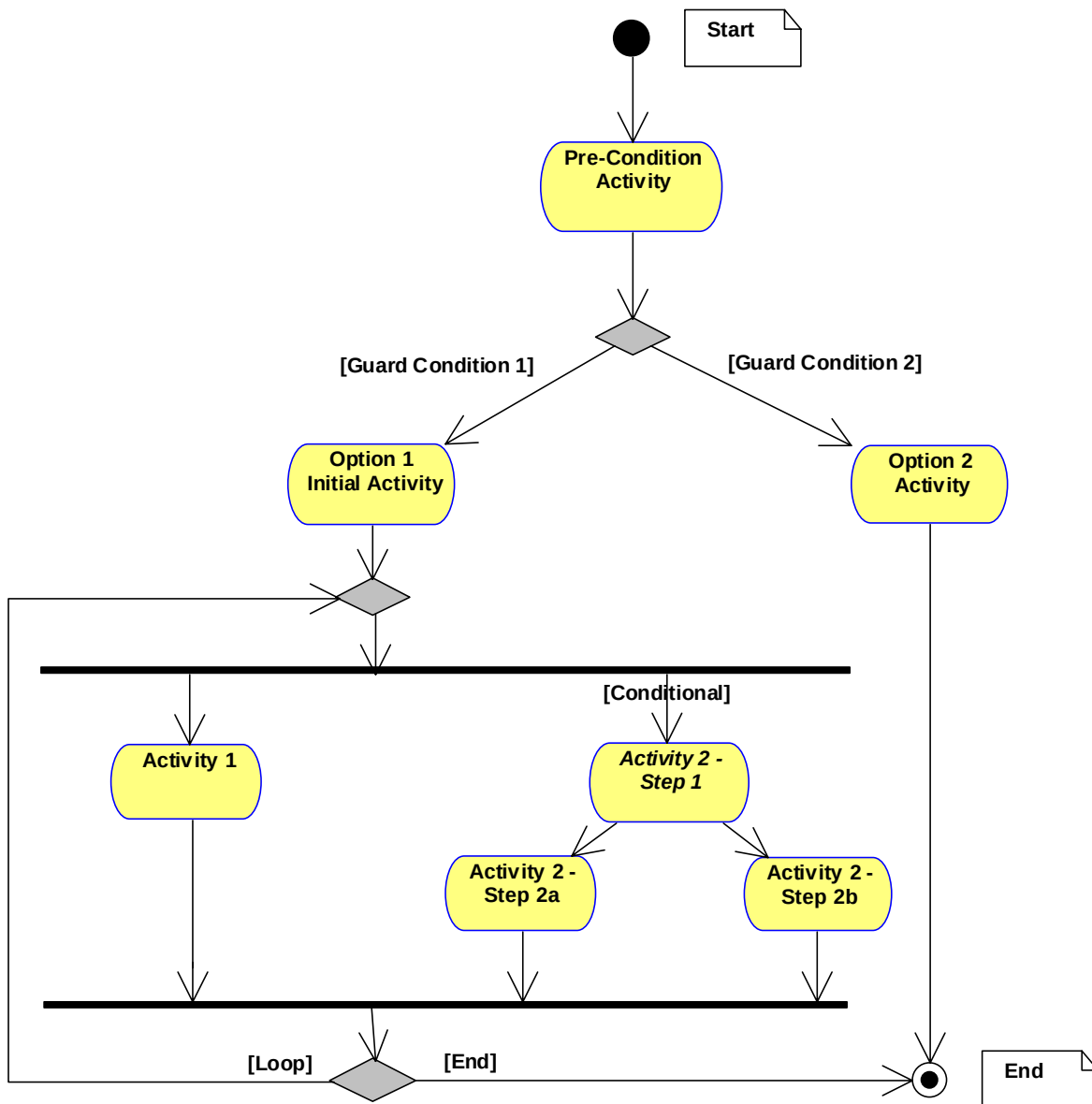


Figure 2 Sample Activity Diagram

The diagram depicts elements that are frequently used by the NTCIP. The diagram starts with the solid black circle at the top. In this case, next to the circle is a note explaining that it is the start point. Notes may be placed anywhere on a diagram next to any set of elements in the figure. The black circle always indicates the starting point (even without this note), but the note is provided to introduce the reader to the concept. The starting point also has a line leading from it to the "Pre-Condition Activity." The line is called a transition. The "Pre-Condition Activity" is a sample of an action that may be performed. Real activities should always start with a verb or in some cases an adverb preceding a verb. They describe the actions that may be performed within the "system". Within the context of the Concept of Operations, the "system" is the entire ITS network that allows the operator to perform his/her duties, including interacting with the traveling public through monitoring conditions and controlling devices. For example, the activities shown in these diagrams may include actions that are performed by the Traffic Management System or Subsystem (TMS) software and/or actions that are performed by the device that do not require any

communications with the TMS. The intent of the figure is to provide the overall context of the actions that must be performed and to convey to the reader the logic that the standard is based on.

The "Pre-Condition Activity" is also attached to a transition that leads to a diamond. The diamond represents a decision point where one of multiple transitions is chosen. The diamond may be associated with a question, although most diagrams will simply annotate each transition option with a guard condition (e.g., in this case, "Guard Condition 1" and "Guard Condition 2"; real guard conditions would state the condition that must apply in order for the path to be followed) within square brackets. The intent is to simplify the diagram for easy reading, while providing the full definition within the associated text describing the diagram. The presence of the decision point implies that the "Option 1 Initial Activity" (and its subsequent activities) is mutually exclusive from the "Option 2 Activity"; thus, the guard conditions should be formed such that they are mutually exclusive as well. For any pass through the process, only one of the two paths is chosen.

If "Guard Condition 2" applies, then "Option Activity 2" will be performed and the process then ends. The symbol used to designate the end of the process is a solid black circle inside of a larger empty circle, in this case with a note describing it.

If "Guard Condition 1" applies, the diagram depicts an initial activity, "Option 1 Initial Activity", followed by a decision point. In this case, the decision point only acts to join multiple paths; paths can be joined by decision points and activities. In this case, there is only one transition leading from the decision point and it goes to a synchronization bar.

Synchronization bars always occur in pairs and indicate that the various paths shown between the bars may be logically performed simultaneously. Note, however, within the context of this standard that not all paths have to be performed. For example, one path may have a conditional guard condition that prevents it from being performed unless the condition is true, another path may relate to a feature that is optional and may not be implemented in a given device. Thus, the logic being conveyed in the sample diagram is that the path with "Activity 1" may be performed simultaneously with the path containing the various "Activity 2" activities. The "Activity 2" path includes an initial step, "Step 1", and 2 additional steps that may be performed simultaneously. These lead to the synchronization bar and indicate that before proceeding, all of "Activity 1" and "Activity 2" must be completed. Once this becomes true, the logic passes to a decision point that allows the logic to loop back to a previous point in the process or allows the process to end. This sort of loop appears in many diagrams indicating the ability for devices to constantly operate (e.g. monitor conditions). Finally, if the end path is chosen, the process ends using the same end point previously referenced for "Option 2 Activity".

Finally, note that Activity 2 - Step 1 is shown in italics, which this standard uses to indicate that it is an activity that the system operator needs, but is outside of the scope of this standard. Such activities are shown in order to provide the full context of how various needs relate to one another, but such user needs do not trace to subsequent document sections of the standard.

Readers should be aware that the diagrams contained in the Concept of Operations are intended to be conceptual in nature and are not intended to be precise. They are intended to provide an organization of all of the various needs that are defined so that readers can gain a better understanding as to why specific activities may be included while also describing some of the possible scenarios that may occur between activities.

The concept of operations concludes by describing the degree to which security issues have been addressed by the standard and by providing a description of how this standard relates to the National ITS Architecture.

2.2 Current Situation and Problem Statement [Informative]

One of the primary responsibilities of Departments of Transportation (DOTs) is to provide for the safe and efficient movement of goods and people. Of course with millions of people moving about, there are constant conflicts created by people wanting to cross paths. DOTs use traffic signals to assign right of way at intersections when less restrictive means of doing so (e.g. stop signs) are ineffective. They assign

right of way by displaying red signals to motorists who are required to wait, providing an opportunity to use the intersection to other motorists who receive green signals. When signals are in close proximity to one another, they can interact. For example, if the signals are not properly coordinated, motorists who receive a green may reach the next signal just in time for it to go red. Another example is an intersection that causes a queue of traffic to extend back through another signal. As the number of signals in close proximity increase, they form a network.

A large number of strategies have emerged in an attempt to optimize any of a number of network performance objectives. Signal-operating agencies have evolved practices that are tailored to their local public expectations. These expectations vary regionally at both the local and national scales, by driver demographic, and even by time of day. Thus, agencies are accustomed to using a varying mix of objective functions in determining their optimal operation. These objectives include:

- Delay minimization
- Capacity maximization
- Emissions minimization
- Minimizing number of stops
- Maximizing the succession of green signals along a route (progression)
- Minimizing cycle failures (queue not fully served by green signals)
- Priority operation for transit vehicles
- Emergency alteration to accommodate emergency vehicles or nearby trains
- Minimize variability to provide predictable operation for safety
- Minimize onset of clearance intervals at unsafe times
- Minimize queue formation, or management of where queues are allowed to form

Many of these objectives compete, and no particular combination of objectives is suited to all applications. Agencies have implemented systems that coordinate traffic signals to meet a locally appropriate combination of these objectives.

The signal system functions are organized in different ways depending on the needs of the system. Some control functions require reliable, full-time communications with SSLs, and other control and surveillance functions can be performed using ad-hoc communications. In cases where it is inconvenient or infeasible to provide reliable, full-time communications from the SSLs all the way to the system owner's office or control location, those functions that require reliable, full-time communications are distributed to a field device that is installed in convenient proximity to the SSLs being controlled. An SSM is a field device that communicates with one or more nearby SSLs for the purpose of coordinated control and monitoring of those SSLs. The SSM also communicates with a TMS operated by the system owner. In the past, the SSM has often been referred to as a "field master" in a "closed loop system".

Additional information regarding signal systems can be found in the "Traffic Control Systems Handbook".

2.3 Reference Physical Architecture

The scale of coordinated signal systems varies considerably, from as few as two intersections to 10,000 intersections as in New York City. Some agencies manage coordinated signal systems at fringe locations in metro areas, or in rural locations, and others manage systems concentrated around a central control point. For example, state agencies frequently manage signals in unincorporated areas and in town below a certain size, and larger towns and cities usually manage signals within their jurisdiction. Some state agencies manage traffic control signals on state numbered routes only, while adjacent traffic control signals not on a state route are managed by local agencies. This wide variation of physical arrangement imposes a wide variation in communications and system architectures. Consequently, a key need is to accommodate a wide range of potential system architectures. Nonetheless, in order to standardize an interface, one must make certain assumptions about the architecture. This standard defines a reference architecture for this purpose, as depicted in Figure 3.

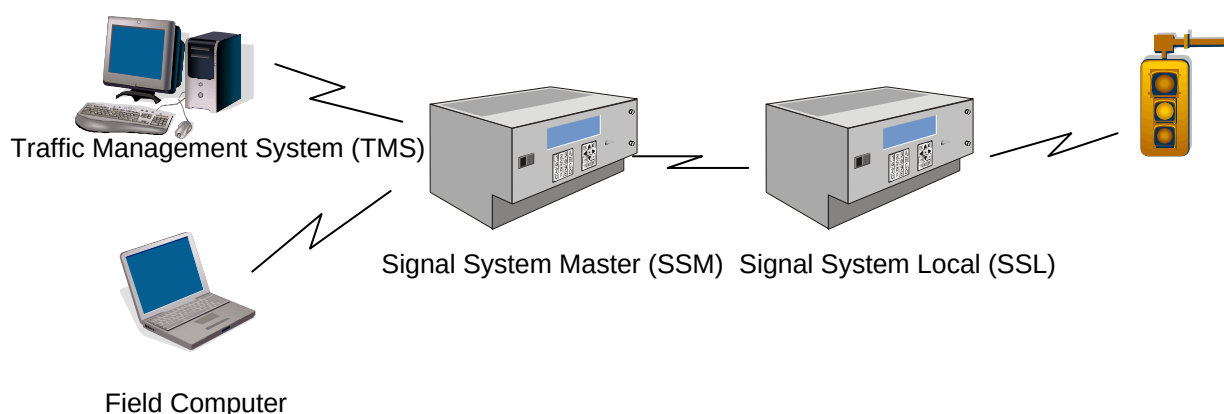


Figure 3 Sample Activity Diagram

The major components of the system are as follows:

- **Traffic Management System (TMS)** – One or more host computing platforms that manage one or more SSM and SSLs. TMSs are typically located in a Transportation Management Center (TMC), which may be a considerable distance from the SSM and its connected SSLs.
- **Field Computer** – A host computing platform that is used to temporarily manage one SSM and its SSLs. All of the operations that can be performed from a TMS can also be performed through a local connection via a field computer. This is typically performed by maintenance personnel using a laptop in the field. Frequently SSMs include connectors such that both a TMS and a field computer can be connected simultaneously. All of the further references to the TMS in this document apply to both the Traffic Management System and the Field Computer.
- **Signal System Master (SSM)** – A host computing platform that is used to manage a small set of SSLs (e.g., 2 to 40) and is typically located in a field cabinet relatively close to the SSLs it manages. It may be controlled by either the TMS or the Field Computer. SSMs also typically include a simple display and a keypad that allow a technician to control the device locally without a field computer.

NOTE: Some architectures do not use SSMs; however, since this standard defines the communications interface between a TMS (and/or Field Computer) and a SSM, systems that do not include SSMs are outside of the scope of this standard.

- **Signal System Local (SSL)** – A host computing platform that controls the operation of the green, yellow, and red indications of a traffic signal installation. This component is typically located in a field cabinet within a hundred meters of the traffic signal indications. It may be managed by a TMS, a Field Computer, or a SSM.

The connection between the TMS and the SSM and the connection between the SSM and the various SSLs run over telecommunications networks, however, the communications technology may change between the two networks. The following provide sample physical architectures that fit within this reference architecture.

2.3.1 Remote Signal System

In some cases, it is not feasible or appropriate to install a centralized signal system that brings surveillance, communication and control of traffic signals back to a TMS. In these cases, a SSM can be installed in the proximity of the SSLs being controlled, to act as a remote surrogate for a TMS. In these situations, system owners might desire to make ad-hoc contact (typically using dial-up communications) with the SSM and a remote signal system master for managing the devices.

2.3.2 Hierarchical Distributed Signal System

Another architectural construct is a hierarchical distributed system. The distributed system uses three levels of processors within the architecture: a SSL, a SSM, and a TMS. Typically, the architecture uses low-capacity but high-reliability links between signal controllers and the field-located SSM, and lower reliability between the TMS and the SSM to save cost. Thus, the SSM is used to maintain system operation without having to communicate that control over unreliable communications links.

The capacity and sub-network layer protocols of the communications links between the SSMs and the SSLs, and between the SSMs and the TMS vary from low-speed asynchronous serial using multi-drop addressing communications at 1200 baud to the fastest fully routed protocol-driven high-speed networks.

2.3.3 Operational Policies and Assumptions

Operational policies are agency-specific and need to be determined and implemented by the agency operating the NTCIP equipment. This standard does not cover this topic, but instead provides a set of common functions that can support an agency's operational policies.

If assumptions pertaining to the operations of a device have been made, they have been stated clearly at the locations where they apply.

2.4 Architectural Needs

This standard addresses the interface between a SSM and one or more management stations (e.g., TMS, field computers, etc.). In order to enable communications between these components, the transportation system manager will need to establish a communication system that links the SSM with a management station. For some systems, the cost of communications may be minimal and as such the system may be designed for constant polling; other systems may encounter significant costs for communicating with the SSM and as such the system may be designed to minimize data exchanges. When deploying a SSM, the system designer must determine the architectural needs that apply to the given system. Standardized needs include:

- a) Providing live data;
- b) Providing off-line, logged data;
- c) Connecting communication networks; and
- d) Support legacy communication networks.

As depicted in Figure 3, each of these can be provided simultaneously by the SSM. Each of these needs is further described in the following.

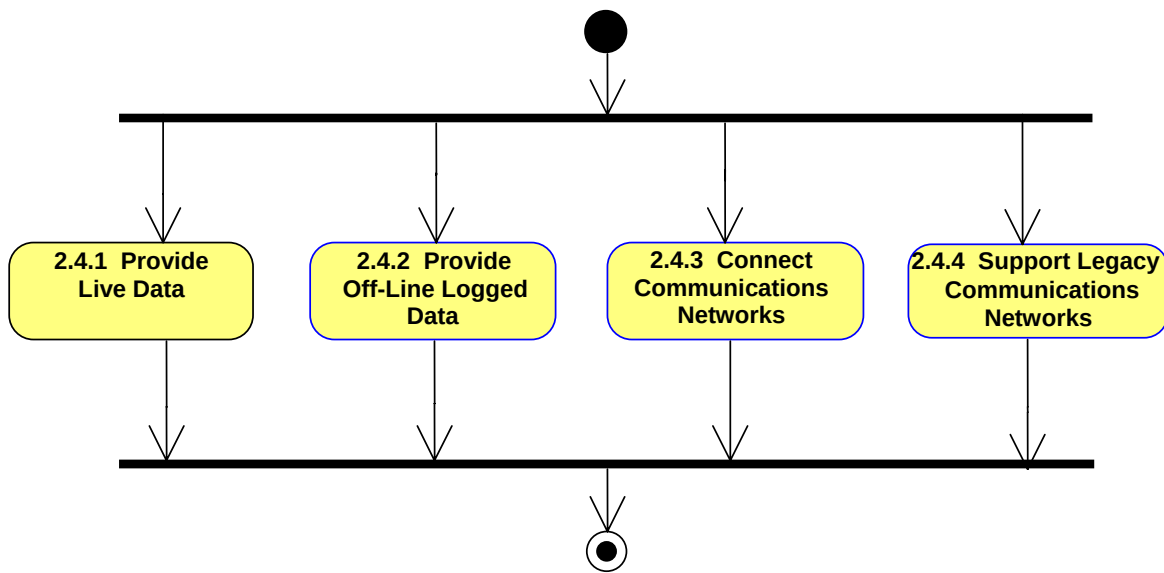


Figure 3 Architectural Needs

2.4.1 Provide Live Data

The typical operational environment allows the TMS to monitor and control the SSM by issuing requests (e.g., requests to explore information, access information, alter information, or control the device). In this environment, the SSM responds to requests from the TMS immediately (e.g., through the provision of live data, success/failure notice of information alteration, or success/failure of the command).

2.4.2 Provide Off-Line Logged Data

Some operational environments do not have always-on connections (e.g., dial-up links). In such environments, a TMS operator may wish to define conditions under which data will be placed into a log, which can then be uploaded at a later time. For example, the operator may wish to maintain a log of when the cabinet door is opened.

2.4.3 Connect Communications Networks

Owners of signal systems need to be able to manage all operational aspects of their SSLs. However, in a system that uses a SSM, the communications path used to connect the TMS to the SSL goes through the SSM. Thus, the SSM needs to provide the ability to connect communication networks such that NTCIP components on one communications circuit are able to exchange information with NTCIP components on another communications circuit.

NOTE: This architectural need is sometimes referred to as bridging or routing, however, these terms actually refer to precise mechanisms used to achieve the desired goal as stated here.

2.4.4 Support Legacy Communications Networks

Associated with the previous need is that agencies may need to use SSM's within existing communications networks. Therefore, the SSM needs to provide for the efficiencies needed by old low-speed communications, and to support those same efficiencies used by SSLs.

2.5 Features

The system owner uses a SSM to manage a set of SSLs, either directly or indirectly. These two activities can be performed simultaneously as depicted in Figure 4. Both of these activities are further defined in the following.

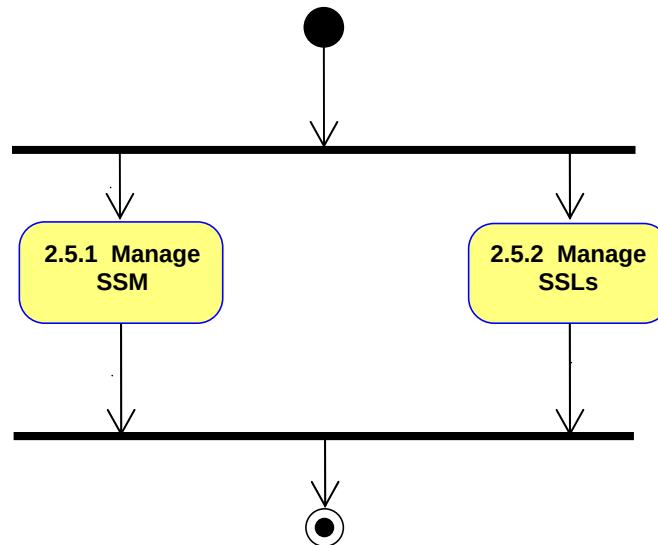


Figure 4 Features

2.5.1 Manage SSM

The system owner needs to be able to manage the operation of the SSM. This includes the ability to:

- a) Configure Cycle Timers and Unit Backup Time;
- b) Manage System Timing Plans; and
- c) Monitor System Operation.

All three of these activities can be performed simultaneously, as depicted in Figure 5. Each activity is further defined in the following.

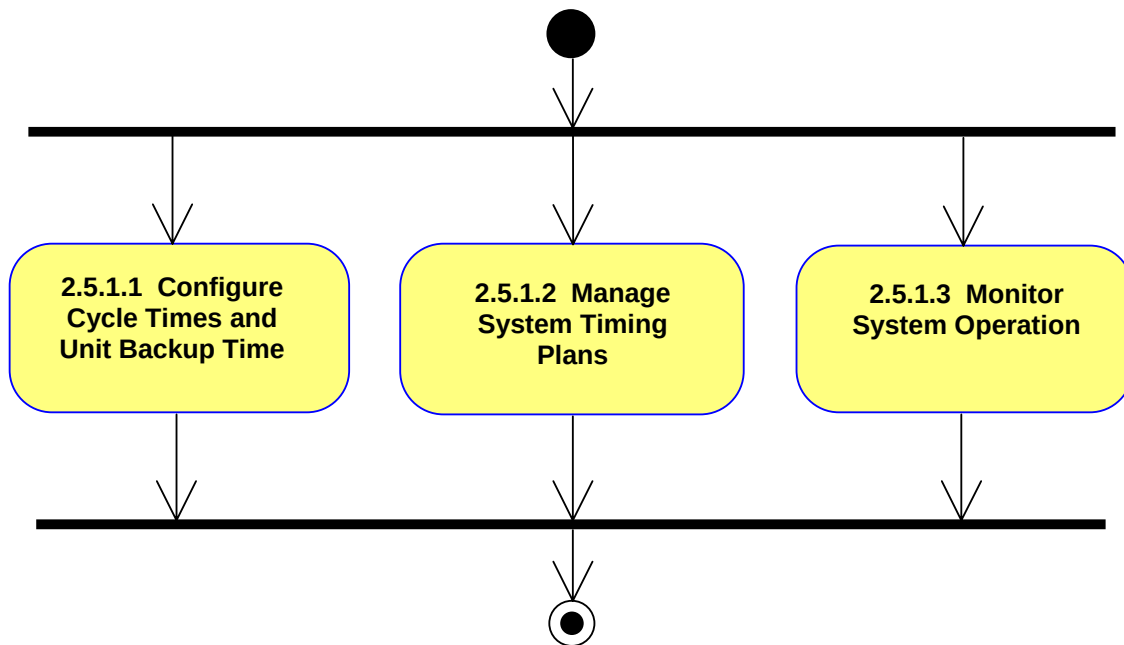


Figure 5 Manage SSM

2.5.1.1 Configure Cycle Timers and Unit Backup Time

The system owner needs to be able to determine the capabilities of the SSM. The system owner may need to configure the SSM to operate cycle timers for synchronizing the SSLs directly using a sync pulse.

2.5.1.2 Manage System Timing Plans

The system owner may want to manage the selection of timing plans for the various sections controlled by the SSM. This is a complex feature, which entails several distinct functions.

The SSM must determine the section boundaries (SSLs belonging to the section). For each section, the SSM determines the appropriate timing plan to use according to one or more methods. There are four major methods in which the plan selection can be made. It can be determined:

- a) Through manual selection at SSM;
- b) By the receipt of a command from the TMS;
- c) According to a schedule; or
- d) In response to current traffic conditions.

The SSM must provide a system reference point for the SSLs in each section. There are two means to determine the system reference point for each section. The first method requires all the SSLs to have the same Time-of-Day (TOD) and the second requires the SSM to know the Cycle Length of each Timing Plan. To accomplish this, the SSM must:

- a) Synchronize Clocks of SSLs; and
- b) Assign Cycle Length By Plan.

The SSM allows the system owner to configure which of these methods should be used and finally implements the selected plan based on an override hierarchy.

Each of these activities is further defined as follows and depicted in Figure 6.

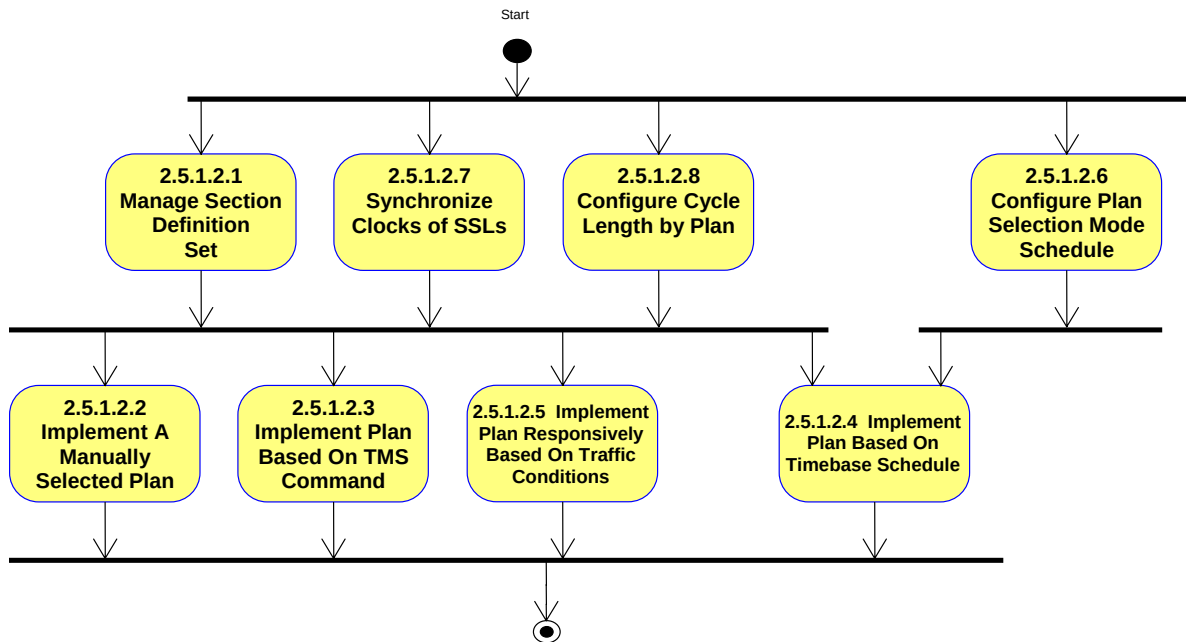


Figure 6 Manage System Timing Plans

2.5.1.2.1 Manage Section Definition Set

The system owner needs to be able to assign an SSL to a signal group, also called a section, or change that assignment.

2.5.1.2.2 Implement A Manually Selected Plan

A TMS operator needs to be able to override the SSM timing plan selection and implement a manually selected plan for a specified section. This might be done in response to a special event or incident. Manual selection takes priority over TMS, traffic-responsive, or timebase selection.

2.5.1.2.3 Implement Plan Based On TMS Command

A TMS operator needs to be able to override the internal SSM timing plan selection and implement a selected plan for a specified section from a TMS. This might be done in response to a TMS schedule. To allow recovery from TMS failure, the SSM needs to revert from TMS control if it has not received a TMS command during a user-defined period of time.

2.5.1.2.4 Implement Plan Based On Timebase Schedule

A TMS operator needs to be able to command the SSM to select a timing plan for a section based on a timebase schedule in the SSM. Perhaps the most common approach to select a timing plan for a given section is to use a timebase schedule, which is useful when daily traffic patterns are highly predictable. The timebase scheduling function typically needs to accommodate variations on a time-of-day, day-of-week and holiday basis.

2.5.1.2.5 Implement Plan Responsively Based On Traffic Conditions

In other environments, traffic patterns may be more variable. In such cases, the system owner may want the SSM's selection of timing plans to be responsive to current traffic conditions. In this traffic responsive mode, the SSM reviews the data obtained from groups of user-defined system detectors, smoothes the

data, checks it for sufficient data availability and sums the data at a user-specified interval. This process is usually refined by experimentation.

2.5.1.2.5.1 Configure Traffic Responsive Mode

To operate in an traffic responsive mode, a system owner needs to configure the SSM to assign which system detectors to obtain data from, configure the pattern selection frequency, and to select which traffic-responsive algorithm (Threshold or Signature) to use. Once these selections are made, the SSM directs the SSL to engage the plan that contains these elements.

2.5.1.2.5.2 Configure Threshold Selection

A system owner needs to be able to configure the SSM to select a timing plan for a section based on the Threshold method. The SSM sums the data from the defined system detectors to first determine if traffic is predominantly inbound, outbound, or balanced (known as offset selection). The SSM sums data from a (possibly) different selection of detectors to determine cycle length, and still a potentially different set of detectors to select the splits. The SSM then optionally evaluates special queue, occupancy and non-arterial system detectors to determine if special conditions require overriding the previous cycle, offset and split selections. Detectors may be weighted separately to allow some detectors greater influence in the selection. The system owner needs to configure failure conditions under which the SSM reverts to timebase operation.

The Threshold method compares the weighted system detector readings to two user-designed thresholds per level. The first threshold (up transition point) directs the SSM when to transition into a level from a lower level. The second threshold (down transition point) directs the SSM to transition to a lower level from that level or a higher level. This separation (up transition point being greater than the down transition point) prevents a system from rapidly switching back and forth between two plans, and is called hysteresis.

2.5.1.2.5.3 Configure Signature Selection

A system owner needs to be able to command the SSM to select a timing plan for a section based on the Signature method. The Signature method depends on each plan defined in the SSM having a user-determined detection signature or pattern. This signature is the sum of weighted volume and weighted occupancy for a series of detectors, each of which are separately weighted. The SSM takes the current detector data and applies the same weightings, and then calculates the difference between the observed weighted values and the values stored in the signature. The SSM then calculates an error or cost function, which is the sum of the absolute values of those differences, or the sum of the squared values of those differences, or least squares analysis. The plan or pattern showing the lowest evaluated error or cost function is selected, and the SSM selects that plan.

Each plan may use a different combination and weighting of detectors within its signature, so the SSM must calculate the observed values separately for each plan that is available.

2.5.1.2.6 Configure Plan Selection Mode Schedule

System owners may wish to use different types of plan selection logic based on the unique characteristics of their system and/or current conditions. Thus, the system owner needs to be able to configure an SSM schedule to select the method (timebase schedule or traffic responsive) for selecting timing plans for each section.

NOTE: The operational mode may be different for each section. The TMS may override the plan selection mode schedule using either TMS schedule or manual modes.

2.5.1.2.7 Synchronize Clocks of SSLs

The user may synchronize SSLs by one of two methods. In the first method, the SSM may provide a sync command directly to the SSL, based on the SSM's section cycle timer. In the second method, the SSL will

derive a section cycle timer reference based on TOD. In this second method, the SSM maintains synchronization by updating the SSL TOD clocks, either at a user-defined period or by direct command from the TMS operator.

2.5.1.2.8 Configure Cycle Length by Plan

The system owner needs to be able to configure the cycle length for each plan so that the SSM can support direct control of the SSL coordination section cycle timer (system reference point).

2.5.1.3 Monitor System Operation

The system owner needs to be able to monitor system operation in order to ensure that it is operating as intended. This includes the ability to simultaneously:

- a) Manage alerts;
- b) Manage system display data; and
- c) Monitor traffic conditions.

This is depicted in Figure 7 and explained in more detail in the following.

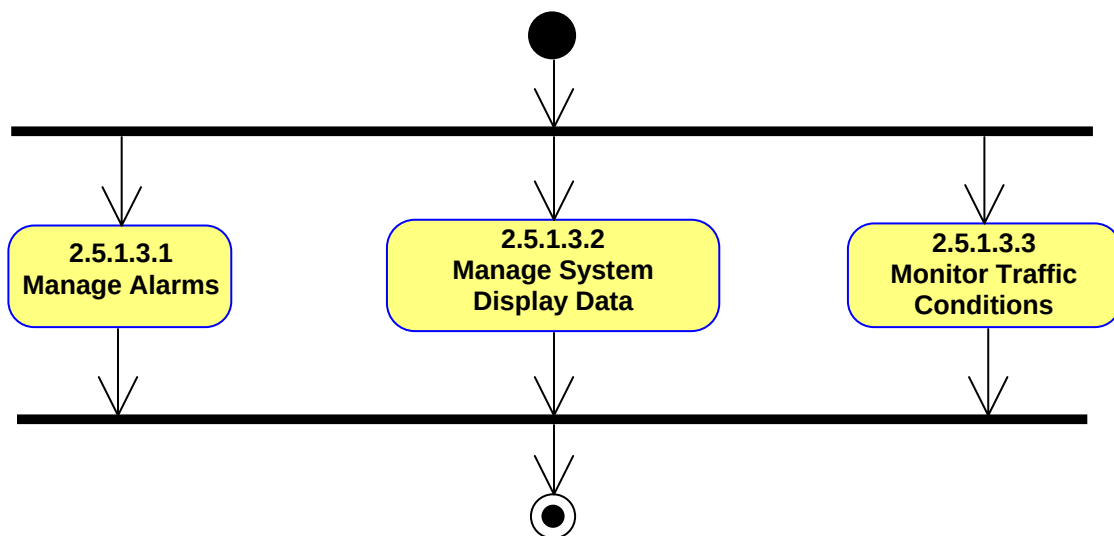


Figure 7 Monitor System Operation

2.5.1.3.1 Manage Alarms

The SSM needs to monitor itself as well as the connected SSLs by reporting any errors and alarms to the appropriate TMS managing arterial operations involving the SSM. Errors and alarms requiring action by the SSM include:

2.5.1.3.1.1 Loss of Control of SSLs

The system owner will configure the SSM for the minimum number of active SSLs in each section below which the SSM should give up control of the remaining SSLs, so that partial control will not cause more disruption of traffic flow than it resolves. The system owner will configure the period of time that an SSL is unresponsive to an SSM beyond which the SSL will be considered inactive by the SSM. The system owner will need to retrieve the number of inactive SSLs from the SSM.

2.5.1.3.1.2 Failed System Detectors

The user needs to be able to set a minimum number of non-failed system detectors in order to maintain traffic responsive operation.

2.5.1.3.1.3 Other Alarms Within a SSL

The SSM does not act on all other alarms from a SSL. The SSM stores and reports SSL alarms to the TMS.

2.5.1.3.1.4 Forward SSM Alarms and Events

The SSM stores events involving the SSM and the SSM reports alarms involving the SSM to the TMS. The SSM stores and reports alarms to the TMS based on user-selected alarm types.

2.5.1.3.2 Manage System Display Data

The system operator is responsible for ensuring the proper, efficient operation of the system and may need to respond to citizen complaints, requests from elected officials, and legal inquiries with little notice. In order to fulfill these responsibilities, the system owner needs to be able to visually monitor the following information about the operation of the system, in a near-real-time manner:

- a) Fault information for the SSM (e.g., loss of communication)
- b) For each section:
 - i) The SSLs currently associated with the section
 - ii) The selected timing plan
 - iii) The nominal cycle length, if available
 - iv) Section cycle timer
 - v) The traffic responsive algorithm data and criteria (relevant system detector sample totals and thresholds or signatures)
- c) For each SSL:
 - i) The difference between the SSL and SSM clocks
 - ii) SSL cycle timer
 - iii) An indication of the current status of the SSL (e.g., detectors, etc.)
 - iv) * The pattern number that the signal is running
 - v) * Current fault information.
 - vi) * Status of coordinator (e.g., coordination, transition, offset error, traffic responsive system detector comparisons, etc.)
 - vii) * Mode of Operation (e.g., timebase, traffic responsive, etc.)
 - viii) * Status of Pre-emption and Priority
- d) Detector faults for SSLs

Many of the items in Part C of the above list are needed by the TMS and not by the SSM. Those items also needed as part of SSM operation are marked with an asterisk.

2.5.1.3.3 Monitor Traffic Conditions

The system owner may wish to monitor traffic conditions throughout the system in order to apply various traffic management techniques, monitor the operation of the system and/or identify problem areas. The data collected can also be stored at the TMS in order to provide valuable information in the development of new timing plans when deemed necessary. In fact, some systems even use this data to detect long-term changes in traffic conditions in order to warn system owners when new timing plans may be needed.

When performing this activity, the system owner is interested in summary traffic data that is collected from system detectors over the data collection period used for traffic responsive operation (i.e., rather than the more detailed data that is available directly from the SSLs). The data of interest includes volume and occupancy. The traffic conditions of interest to the TMS that would be derived from the collected data include travel time, speed, density and vehicles per hour.

2.5.2 Manage SSLs

A system owner needs to be able to manage the various parameters that are stored in the SSLs. The management of this data includes the ability for uploading parameters and data for verification,

downloading modified parameters to implement improvements, and retrieving data from the SSL. The detailed user needs for the SSL are dependent upon the type of device and are defined in other standards (e.g., NTCIP 1202 v02).

2.6 Security

This standard does not address any security issues. Any security pertaining to protecting the communications with a SSM should be implemented either physically by protecting the communications access points, or logically by enabling security features associated with the underlying communications protocols.

2.7 Relationship of User Needs to National ITS Architecture Flows [Informative]

The National ITS Architecture does not explicitly call out an individual subsystem that solely maps to a SSM. In order to leverage the content in the National ITS Architecture, the SSM needs to be characterized as both a TMS (Traffic Management Subsystem) and a RS (Roadway Subsystem) depending on the viewpoint of the role of the SSM. In addition, there are cases where the SSM is transparent to the communications between the TMS and the SSLs at the roadway. There are three National ITS Architecture Flows associated with the operation of a SSM. These are:

- a) signal control data
- b) signal control status
- c) traffic control coordination

The Traffic Management Subsystem (TMS) or System represents the central computer or field computer that communicates to and from the Roadway Subsystem (RS). In the National ITS Architecture, the SSL is represented by the RS. The main user needs (features), as identified above, are related to the National ITS Architecture flows in the following manner:

Main User Needs	Source	Architecture Flow	Destination
Provide Live Data (SSM is part of the RS)	TMS	signal control data	RS (SSM)
	RS (SSM)	signal control status	TMS
Provide Off-Line Logged Data (SSM is part of the TMS)	TMS	traffic control coordination	Other TMS (SSM)
Monitor Exceptional Conditions (SSM is part of the RS)	TMS	signal control data	RS (SSM)
	RS (SSM)	signal control status	TMS
Connect Communications Networks (SSM is transparent)	TMS	signal control data	RS (SSL)
	RS (SSL)	signal control status	TMS
Manage SSM (SSM is part of the TMS)	TMS	traffic control coordination	Other TMS (SSM)
Manage SSLs (SSM is transparent)	TMS	signal control data	RS (SSL)
	RS (SSL)	signal control status	TMS

2.8 Operational Scenarios [Informative]

2.8.1 Remote Signal System, Low-Speed Communications

In this scenario, the SSM is installed in a field location in the vicinity of the SSLs being controlled. The SSLs are in a limited geographical area along a suburban arterial street, and comprise 12 actuated signal controllers. Each of these actuated signal controllers includes coordination ability.

The SSLs are connected to the SSM using an existing system of multi-drop twisted-pair copper wire cable. The physical connection is two twisted pairs of 19-gauge copper wire. Each SSL is equipped with a modem that communicates at 1200 baud using frequency shift keying. The modem converts asynchronous serial digital communications to modulated signaling, with one pair devoted to transmitting and the other to receiving. Because the pairs are multi-dropped, all local devices are party to all SSM transmitted communications. Devices within the system, including the SSM and the SSLs, acquire use of their outgoing transmit wire pair by first sensing if a carrier is present. If no carrier is present, the modem establishes a carrier and begins transmitting, releasing the carrier when the transmission is complete.

The TMS operator gains access to the system through the use of software running on a PC, communicating over a standard dial-up telephone link to the SSM. There is no prospect of full-time communications to the SSM, nor does the agency have a need for a full-time centralized monitoring and operation of the system.

Each of the 12 SSLs operates the traffic signals at their respective intersection. They use detectors on the approaches to provide actuated control, and have some detectors designated as system detectors for use by the SSM.

The TMS operator designs coordinated signal timing plans, which include intersection offsets, cycle lengths, splits, and zonal boundaries. The TMS operator then downloads these timings to the SSLs. The TMS operator designs the system to operate responsively to traffic. The operator assigns certain SSL detectors to operate as system detectors. The TMS operator designs thresholds and weightings for system detector readings, using the threshold traffic-responsive plan selection technique.

In operation, the SSM polls the SSLs to collect information about their status. It also collects volume and occupancy data for the SSL system detectors. It applies the relevant weightings to the volume and occupancy, combines them, and then weights each detector that has been assigned to be used for the plan selection step. It compares the sum of the weighted and combined measurements to the thresholds for offset level, cycle length, and split, and determines which plan should be selected. The SSM then sends a command to the SSLs to implement the selected plan.

The detector volume and occupancy is summed into 15-second totals by the SSL, and further summed into five-minute totals by the SSM.

The SSM performs this operation every three minutes, in accordance with the TMS operator's design. After a year of operation, the TMS operator changes the system to select plans at 12-minute intervals.

The TMS operator monitors the operation of the system by dialing into it using a remote computer. He monitors the actions of the SSM, and also observes real-time displays of several individual SSLs. He reviews alarm conditions that may have occurred, and he uploads and downloads SSL data.

Citizens complain about the operation by calling the TMS operator and making requests. The TMS operator determines if the complaint concerns a fault condition, an operational design, or a misperception on the part of citizen. The TMS operator looks at the relevant intersection operation in real time, perhaps while the citizen is on the phone, monitoring detections and SSL operation. If a fault condition is apparent, the TMS operator dispatches a maintenance crew with the information needed to effect a repair. If the operation of the system is accomplishing the design objective, then the TMS operator will explain that objective to the citizen. If the observed condition is not within the intention of the traffic engineer, then the TMS operator will make further observation and then, in consultation with the traffic engineer, will make revisions to the operation and implement those changes by downloading a new signal timing database (or portion thereof) to the relevant SSL or by downloading new pattern selection parameters to the SSM.

2.8.2 Hierarchical Distributed Signal System on Low-Speed Infrastructure

In this scenario, a municipal agency is replacing an outdated and unreliable TMS on a series of arterial streets surrounding the core of the city. The system covers 250 intersections in 40 corridors, which range in size from four intersections to 28 intersections. The agency is constrained by budget and must use the existing infrastructure, which provides twisted-pair copper wire from a central location to a series of local interface cabinets. The TMC is in a location adjacent to a large urban-renewal project, and thus the communications infrastructure surrounding the TMC is frequently interrupted by construction activities. These construction activities are expected to continue for a period of years, and thus the new TMS will have to operate reliably despite these activities.

The designers of the new TMS have decided to use a series of SSMs as a boundary between the reliable portions of the communications network between the interface cabinets and the SSLs and the unreliable long trunk lines surrounding the TMC. These SSMs will be installed in the existing interface cabinets at the junction between trunk lines and distribution lines. This distributes the system operation, including pattern selection for traffic responsive operation, to field processors outside the area affected by long-term construction projects. In so doing, on-the-ground reliability can exceed the reliability of the communications trunk lines.

The TMS operators develop signal timing databases and also pattern-selection parameters. Some of the SSMs select traffic patterns based on measured traffic performance, and others select patterns by time of day, based on the expected variation in traffic and motorist expectations on those facilities. The TMS operators upload stored detector data from the SSLs and SSMs to use as the basis for developing pattern selection parameters.

After developing the signal timing and pattern selection parameters, the TMS operators will download these parameters to SSLs. As they fine-tune and maintain these timings and parameters, they will download revised settings to both the SSLs and SSMs on an ad hoc basis.

On occasion, the operators will direct the SSM(s) to implement a timing pattern manually, perhaps to respond to traffic diversion away from a freeway incident.

The TMS supports a scalable map display that the operators use to monitor three things:

- a) Communications status (online, offline, etc.)
- b) Main-street green
- c) Intersection status (manual plan, time of day, traffic responsive, etc.)

Additionally, the TMS operators use a real-time display of intersections (singly or in groups of up to several) to monitor traffic movement status (i.e. the signal colors being displayed), detector calls, SSL time clock, pattern running, transitions, and so on.

The map and intersection displays are used for ad-hoc monitoring and responding to citizen requests, and the agency considers it acceptable that these features are not available when the trunk lines are interrupted by construction activities.

(Note, in this scenario, the loss of reliability of trunk lines is presented as a specific example, but it could be caused by any of a number of circumstances. For example, the trunk lines might be communicated at long distance over low-reliability wireless media, or even over high-latency networks such as the Internet. The point to be illustrated by this scenario is the use of SSMs in large-scale systems as a boundary between high-reliability and low-reliability network portions, to make sure that the real-time control elements are on the same side of that boundary as the SSLs.)

2.8.3 Hierarchical Distributed Signal System with High-Speed Communications

This scenario is identical to Scenario 2, except that the budget for TMS implementation is large enough to provide high-capacity communications from the TMC to the SSLs. The only difference lies in the ability to use high-overhead communications protocols to manage the communications architecture. Thus, in its communications brokering role, the SSM acts solely as a router.

Section 3

FUNCTIONAL REQUIREMENTS

[NORMATIVE]

Section 3 defines the Functional Requirements based on the user needs identified in the Concept of Operations (See Section 2). This section includes:

- a) A tutorial
- b) The Protocol Requirements List – A Functional Requirement is a requirement of a given function and therefore is only required to be implemented if the associated functionality (e.g., user need) is selected through the use of the Protocol Requirements List (PRL). The PRL also indicates which of the items are mandatory, conditional, or optional. The PRL can be used by procurement personnel to specify the desired features of a SSM or can be used by a manufacturer to document the features supported by their implementation.
- c) Operational Environment Requirements – These are requirements related to the Operational Environment (Architectural) Needs defined in Section 2.4.
- d) Data Exchange Requirements – These are requirements related to the Features identified in Section 2.5 that can be realized through a data exchange. For example, this includes the requirement for a SSM to be able to manage SSLs.

This section is intended for all readers of the document, including:

- a) Transportation operations managers
- b) Transportation operations personnel
- c) Transportation engineers
- d) System integrators
- e) Device manufacturers

The first three categories of readers will find this document section useful in order to understand the details of what the standard requires of a SSM. This audience will find Section 3.2.6 to be particularly useful in preparing procurement specifications and will be able to map the various rows of this table to the more detailed text contained within the other clauses.

The last two categories of readers will find this document section useful in order to fully understand what is required of equipment meeting this interface standard. They will also be able to use the table in Section 3.2.6 and the Tables in Annex B to document the capabilities of their implementations.

3.1 Tutorial

Requirements are based on the user needs. An implementation only needs to support the requirements corresponding to the user needs that a particular procurement addresses. However, a user need may be associated with several requirements. The PRL in Section 3.2.6 maps the user needs identified in Section 2 with the functional requirements defined in Section 3 along with an indication as to whether each item is mandatory or optional for conformance to this standard. Additionally, some requirements need project specific details in order to be completely defined. A user will need to provide this additional information, as identified in the PRL, in order to fully specify the desired SSM.

3.2 Protocol Requirements List

The PRL, provided in Section 3.2.6, maps the user needs defined in Section 2 to the requirements defined in Section 3. The table can be used by:

- a) A user or specification writer to indicate which requirements are to be implemented in a project specific implementation;
- b) The protocol implementer, as a checklist to reduce the risk of failure to conform to the standard through oversight;

- c) The supplier and user, as a detailed indication of the capabilities of the implementation; and
- d) The user, as a basis for initially checking the potential interoperability with another implementation.

3.2.1 User Needs Column

The user needs are defined within Section 2 and the PRL is based upon the user needs within that section. The section number (User Need ID) and user need name are indicated within these columns.

3.2.2 Requirements Column

The requirements are defined within Section 3 and the PRL references the traces from user needs to these requirements. The section number (Functional Requirement ID) and functional requirements name are indicated within these columns.

3.2.3 Conformance Column

The following notations and symbols are used to indicate status and conditional status in the PRL within all NTCIP standards. Not all of these notations and symbols may be used within this standard.

3.2.3.1 Status Symbols

The following symbols are used to indicate status:

M	Mandatory
M.#	Support of every item of the group labeled by the same numeral # required, but only one is active at a time
O	Optional
O.# (range)	Part of an option group. Support of the number of items indicated by the '(range)' is required from all options labeled with the same numeral #
C	Conditional
N/A	Not-applicable (i.e. logically impossible in the scope of the standard)
X	Excluded or prohibited

The O.# (range) notation is used to show a set of selectable options (e.g., O.2 (1..*) would indicate that one or more of the option group 2 options must be implemented). Two character combinations are used for dynamic requirements. In this case, the first character refers to the static (implementation) status, and the second refers to the dynamic (use); thus "MO" means "mandatory to be implemented, optional to be used."

3.2.3.2 Conditional Status Notation

The following predicate notations may be used:

<predicate>: This notation introduces a single item that is conditional on the <predicate>.

The <predicate>: notation means that the status following it applies only when the PRL states that the feature or features identified by the predicate are supported. In the simplest case, <predicate> is the identifying tag of a single PRL item.

The symbol <predicate> also may be a Boolean expression composed of several indices. "AND", "OR", and "NOT" shall be used to indicate the Boolean logical operations.

The predicates used in this standard map to the following:

Predicate	Section
SyncPulse	2.5.1.2.8
Threshold	2.5.1.2.5.1
Signature	2.5.1.2.5.2

3.2.4 Support Column

The support column can be used by a procurement specification to identify the required features for the given procurement or by an implementer to identify which features have been implemented. In either case, the user circles the appropriate answer (Yes, No, or N/A) in the support column:

Yes	Supported by the implementation.
No	Not supported by the implementation.
N/A	Not applicable

3.2.5 Instructions for Completing the PRL

In the 'project requirements' column, each response shall be selected either from the indicated set of responses (for example: Yes / No / NA), or it shall reference additional items that are to be attached. If a conditional requirement is inapplicable, use the Not Applicable (NA) choice. If a mandatory requirement is not satisfied, exception information must be supplied by entering a reference Xi, where i is a unique identifier, to an accompanying rationale for the non-conformance. When the status is expressed as a two-character combination, the response shall address each element of the requirement; e.g., for the requirement "mo," the possible compliant responses are "yy" or "yn."

To claim conformance with this standard, an implementation shall fulfill the mandatory and selected optional requirements as identified in the PRL.

Everything in the PRL can apply to an FMS in both a Closed Loop System and a Hierarchical Distributed System. The architectures are different however the functionality of the SSM is the same.

3.2.6 Protocol Requirements List (PRL) Table

User Need ID	User Need	Functional Requirement ID	Functional Requirement	Conformance	Support	Additional Specifications
2.4	Architectural Needs					
2.4.1	Provide Live Data			M	Yes	
		3.3.1.1	Accept Data from the TMS	M	Yes	
		3.3.1.2	Deliver Data to the TMS	M	Yes	The Response Start Time for all requests shall be not greater than ____ milliseconds (Default=2000).
		3.3.1.3	Explore SSM Data by the TMS	M	Yes	The Response Start Time for all requests shall be not greater than ____ milliseconds (Default=2000).
		3.3.3.1	Determine Current Access Settings	M	Yes	
		3.3.3.2	Configure Access	M	Yes	
2.4.2	Provide Off-Line Logged Data			M	Yes	
		3.3.2.1	Determine Current Configuration of Event Logging Service	M	Yes	
		3.3.2.2	Configure Event Logging Service	M	Yes	
		3.3.2.3	Retrieve Event Logged Data	M	Yes	
		3.3.2.4	Clear Event Log	M	Yes	
		3.3.2.5	Determine Capabilities of Event Logging Service	M	Yes	
2.4.3	Connect Communications Networks			M	Yes	
		3.3.1.4	Accept Data from the SSLs	M	Yes	

User Need ID	User Need	Functional Requirement ID	Functional Requirement	Conformance	Support	Additional Specifications
		3.3.1.5	Deliver Data to the SSLs	M	Yes	
		3.3.1.6	Explore SSL Data by the TMS	M	Yes	
		3.3.1.7	TMS Acceptance of Data from the SSL	M	Yes	
		3.3.1.8	TMS Delivery of Data to the SSL	M	Yes	
		3.3.3.1	Determine Current Access Settings	M	Yes	
		3.3.3.2	Configure Access	M	Yes	
2.4.4	Support Legacy Communications Networks			O	Yes / No	
		3.3.1.9.1	Configure Using Block Objects	M	Yes	
		3.3.1.9.2	Retrieve Block Objects	M	Yes	
		3.3.1.9.3	Retrieve Block Status	M	Yes	
		3.3.1.9.4	Support STMP	O	Yes / No	
2.5	Features					
2.5.1	Manage SSM					
2.5.1.1	Configure Cycle Timers and Unit Backup Time			M	Yes	
		3.4.2.2.1	Determine SSLs Currently Connected	M	Yes	
		3.4.2.2.2	Determine Pattern Selection Capabilities	M	Yes	
		3.4.2.2.3	Determine SSM Section Characteristics	M	Yes	
		3.4.2.2.4.1	Configure Cycle Timer Reference	O	Yes / No	
		3.4.2.2.4.2	Determine Cycle Timer Capability	O	Yes / No	
		3.4.2.2.5	Determine SSM Software Version	M	Yes	
		3.4.3.7.4	Sync SSL by Direct Command	O	Yes / No	
2.5.1.2	Manage System Timing Plans			M	Yes	
2.5.1.2.1	Manage Section Definition Set			M	Yes	

User Need ID	User Need	Functional Requirement ID	Functional Requirement	Conformance	Support	Additional Specifications
		3.4.3.1.1	Configure Section Assignment	M	Yes	
		3.4.3.1.2	Retrieve Section Assignment	M	Yes	
		3.4.3.1.3	Configure Section Characteristics	M	Yes	
2.5.1.2.2	Implement A Manually Selected Plan			M	Yes	“Manual” means user-directed ad-hoc from TMS, vs. TMS automatically directed
		3.4.3.3	TMS Override of Plan Selection	M	Yes	
2.5.1.2.3	Implement Plan Based On TMS Command			M	Yes	
		3.4.3.6.1	TMS Override of SSM Algorithm or Timebase Timing Plan	M	Yes	
		3.4.3.6.2	SSM Instruct SSLs to Engage TMS Timing Plan	M	Yes	
		3.4.3.6.3	Set Maximum Time Without TMS Control	M	Yes	
2.5.1.2.4	Implement Plan Based On Timebase Schedule			M	Yes	
		3.4.2.1	Synchronize SSM Clock with TMS	M	Yes	
		3.4.3.4	Configure SSM Schedule	M	Yes	
		3.4.3.6.2	SSM Instruct SSLs to Engage TMS Timing Plan	M	Yes	
2.5.1.2.5	Implement Plan Responsively Based On Traffic Conditions					
2.5.1.2.5.1	Configure Traffic Responsive Mode			M	Yes	Either Threshold Selection or Signature Selection, or both, must be supported

User Need ID	User Need	Functional Requirement ID	Functional Requirement	Conformance	Support	Additional Specifications
		3.4.1.1	Assign System Detectors	M	Yes	
		3.4.3.5.1	Select Algorithm	M	Yes	
		3.4.3.5.2	Accept Pattern Selection Frequency	M	Yes	
		3.4.3.5.3.8	Instruct SSLs to Engage Threshold Timing Plan	M	Yes	
2.5.1.2.5.2	Configure Threshold Selection			O.1 (1..*)	Yes / No	
		3.4.1.2	Configure Detector Grouping	M	Yes	
		3.4.1.3	Configure System Detector Group Smoothing	M	Yes	
		3.4.1.4	Configure Override System Detector Group Smoothing	M	Yes	
		3.4.1.5	Configure Minimum Valid Detector Samples	M	Yes	
		3.4.1.6	Configure Average or Highest Value	M	Yes	
		3.4.3.5.3.1	Configure Traffic Directional Characteristic Thresholds	M	Yes	
		3.4.3.5.3.2	Configure Cycle Thresholds	M	Yes	
		3.4.3.5.3.3	Configure Split Thresholds	M	Yes	
		3.4.3.5.3.4	Configure User-Defined Minimum Number of Operational Detectors	M	Yes	
		3.4.3.5.3.5	Configure Queue Detector Override Thresholds	O	Yes / No	
		3.4.3.5.3.6	Configure Occupancy Detector Override Thresholds	O	Yes / No	
		3.4.3.5.3.7	Configure Non-Arterial Detector Override Thresholds	O	Yes / No	
		3.4.3.5.3.8	Instruct SSLs to Engage Threshold Timing Plan	M	Yes	
2.5.1.2.5.3	Configure Signature Selection			O.1 (1..*)	Yes / No	

User Need ID	User Need	Functional Requirement ID	Functional Requirement	Conformance	Support	Additional Specifications
		3.4.3.5.4.1	Configure Signature Parameters	M	Yes	
		3.4.3.5.4.2	Instruct SSLs to Engage Signature Timing Plan	M	Yes	
2.5.1.2.6	Configure Plan Selection Mode Schedule			M	Yes	
		3.4.3.2	Configure Plan Selection Mode Schedule	M	Yes	
2.5.1.2.7	Synchronize Clocks of SSLs			M	Yes	
		3.4.3.7.1	Accept User-Defined Period for SSL Clock Synchronization	M	Yes	
		3.4.3.7.2	Periodically Set Clocks of SSLs	M	Yes	
		3.4.3.7.3	Instruct SSM to Set Clocks of SSLs	M	Yes	
2.5.1.2.8	Configure Cycle Length by Plan			SyncPulse:M	Yes / No	
		3.4.2.2.6	Accept Cycle Length by Plan	M	Yes	
2.5.1.3	Monitor System Operation					
2.5.1.3.1	Manage Alarms			M	Yes	
		3.4.4.1.1	Configure Critical Alarms and Events to Monitor	M	Yes	
		3.4.4.1.2	Provide Critical Alarms and Events Logging Requirements to SSM	M	Yes	
		3.4.4.1.3	Critical Alarms and Events Reporting Requirements	M	Yes	
2.5.1.3.1.1	Loss of Control of SSLs			M	Yes	
		3.4.4.1.4.1	Lost Communications to a SSL	M	Yes	
		3.4.4.1.5	Configure Intersection Non-Responsive Time to Constitute Failure	M	Yes	

User Need ID	User Need	Functional Requirement ID	Functional Requirement	Conformance	Support	Additional Specifications
		3.4.4.1.6	Coordination Failure Caused by Loss of Control	M	Yes	
2.5.1.3.1.2	Failed System Detectors			M	Yes	
		3.4.4.1.4.2	Failed System Detectors for Threshold Selection of Timing Plans	Threshold:M	Yes / No	
		3.4.4.1.4.3	Failed System Detectors for Signature Selection of Timing Plans	Signature:M	Yes / No	
2.5.1.3.1.3	Other Alarms Within a SSL			M	Yes	
		3.4.4.1.4.4	SSL Alarms and Events	M	Yes	
2.5.1.3.1.4	Forward SSM Alarms and Events			M	Yes	
		3.3.2.2	Configure Event Logging Service	M	Yes	
		3.3.2.3	Retrieve Event Logged Data	M	Yes	
2.5.1.3.2	Manage System Display Data			M	Yes	The Response Start Time for all requests shall be not greater than ____ milliseconds (Default=2000).
		3.4.3.1.2	Retrieve Section Assignment	M	Yes	
		3.4.4.2.1	Provide Timing Plan for Each Section	M	Yes	
		3.4.4.2.2	Provide the Nominal Cycle Length for Each Section	M	Yes	
		3.4.4.2.3	Provide Current Status of the Signal Displays for Each SSL	M	Yes	
		3.4.4.2.4	Provide Current Traffic Responsive Comparison	O	Yes / No	

User Need ID	User Need	Functional Requirement ID	Functional Requirement	Conformance	Support	Additional Specifications
		3.4.4.2.5	Provide Mode of Operation and Pattern Number for Each SSL	M	Yes	
		3.4.4.2.6	Provide Status Information for Each SSL	M	Yes	
		3.4.4.2.7	Provide Detector Status Information for Each System Detector	M	Yes	
2.5.1.3.3	Monitor Traffic Conditions			M	Yes	
		3.4.1.7	SSM Collect Volume and Occupancy Data	M	Yes	
		3.4.1.8	TMS Collect Volume and Occupancy Data	M	Yes	
2.5.2	Manage SSLs			O	Yes / No	
		3.3.1.6	Explore SSL Data by the TMS	M	Yes	
		3.3.1.7	TMS Acceptance of Data from the SSL	M	Yes	
		3.3.1.8	TMS Delivery of Data to the SSL	M	Yes	
		3.4.2.3	Configure Connected SSLs	M	Yes	